International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

Secure mechanical design and manufacturing: Preventing IP theft via cybersecurity

Shubham Bhaskar Thakare [1,*] and Sanjay Poddar [2]

[1] *Independent Researcher, Ohio, USA.*
[2] *Independent Researcher, Texas, USA.*

International Journal of Science and Research Archive, 2025, 14(02), 638-645

Publication history: Received on 02 January 2024; revised on 04 February 2025; accepted on 07 February 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.14.2.0414

Abstract

The impending threat of Intellectual Property (IP) in design and manufacturing from mechanical engineering is increasingly furthering concerns on using digitized production and globalized supply chains. In conjunction with the greater adoption of CAD, PLM, and AM, the risk now is greater with respect to cyberattacks, unauthorized access, and industrial espionage. The paper analyzes certain cybersecurity challenges in mechanical engineering, like: secure design, encrypted manufacturing workflows, and best practices for preventing IP theft. It analyzes the threats ranging from cyberattacks on the CAD, engineering files, weaknesses in the supply chain, reverse engineering, and insider threats. The paper puts forward security frameworks, encryption schemes, blockchain-based authentication, and ZTA to protect the design and production data. In addition, the case studies from the aerospace, automotive, and industrial automation domains showcase the real incidents of IP theft and countermeasures used to curb access to such practices. Finally, the paper towards the end introduces the developments in the future of cybersecurity concerning mechanical engineering, centering on the role of AI-enabled real-time suspicious behavior detection and secure cloud collaboration platforms. Providing robust cybersecurity ensures that manufacturers will be able to protect their proprietary designs while retaining competitiveness and mechanical systems' immunity to cyber threats.

Keywords: Computer Aided Design (CAD); IP; Cybersecurity; Industrial; Manufacturing

1. Introduction

1.1. Background

Mechanical engineering in the modern era has embraced more and more digital tools for efficient, precise, and innovative practices. Technologies that include Computer-Aided Design (CAD), Product Lifecycle Management (PLM), digital twins, and additive manufacturing (three-dimensional or 3D printing) have redefined the design and manufacturing path. However, the more interdependent these technologies grow, turning to the cloud, the more sensitive intellectual property (IP) can become exposed to cyber threats; hence, security has become a critical concern for mechanical engineers and manufacturers.

Intellectual Property in mechanical engineering refers to trade secreted product designs, manufacturing techniques, simulation models, material compositions, and optimization processes crucial for a company to maintain its competitive edge, product integrity, and compliance with industry standards associated with the protection of proprietary knowledge. (3) It has been on the increase owing to the need for protection of proprietary engineering knowledge supposedly aimed at enhancing competitiveness in sectors dealing with aerospace, automotive, robotics, and industrial automation.

* Corresponding author: Shubham Bhaskar Thakare

1.2. The Growing Threat of IP Theft in Mechanical Engineering

IP theft is a key concern in the mechanical engineering field, because its fallout varies widely and can extend from loss of income to endangering national security. Whereas most cyberattacks can aim to cause system disruptions, IP theft can often remain more obscure or targeted in focus and employ unauthorized access and uses of trade secreted machinery design and manufacturing technologies.

First, digital design and manufacturing have increased chances of intrusion or cyber-attack through PLM systems based on cloud technology.

Second, structures of global supply chain networks in which supply firms rely on engineering firms raise security holes.

Third, rising cyber threats such as advanced persistent threats, two threats inside the organizations, and a plethora of other malware naturally target engineering firms.

Lastly, additive manufacturing technology allows one to safely transfer and digitally print mechanical parts while exposing one to unlawful duplication.

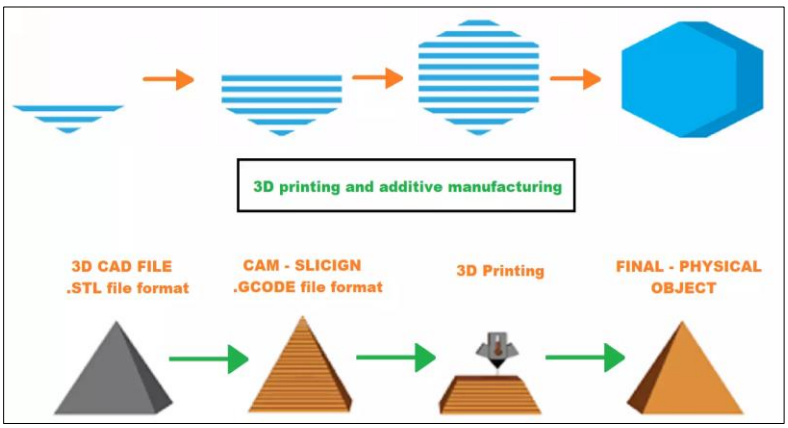

Figure 1 Shows the digital process of additive manufacturing

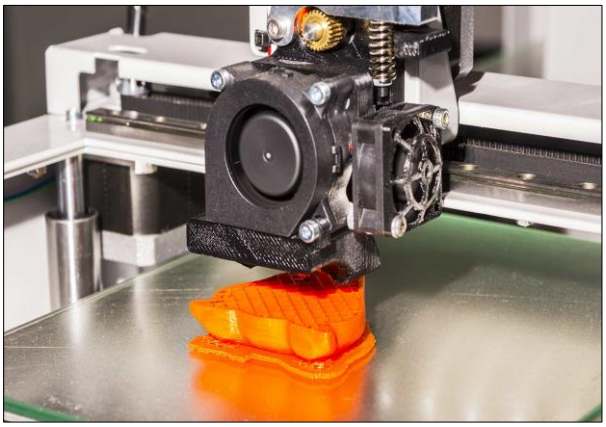

Figure 2 Shows the instance of CAD part 3D printing

Several cases illustrate the undeniable severity of the issue:

- In 2018, a Chinese cyber espionage group targeted a leading aerospace firm, stealing sensitive CAD files related to jet engine design.
- In 2020, an automotive manufacturer suffered an IP breach when unauthorized users accessed confidential vehicle component designs stored on a cloud-based PLM system.
- In 2022, a mechanical engineering firm specializing in robotics had its proprietary control system software stolen, leading to the development of counterfeit products by competitors.

This is sufficient to convey a sense of urgent need for stringent cybersecurity in mechanical design and engineering.

1.3. Research Objectives

This paper discusses the security challenges faced in mechanical engineering, including:

- **Cybersecurity Risks:** Identifying key cybersecurity threats affecting mechanical design and manufacture;
- Protection Strategies: Examining advanced security measures involving encryption, blockchain authentication, and Zero Trust Architecture (ZTA);
- **Case Studies:** Illustrating real-world cases of IP theft and security countermeasures in aerospace, automotive, and industrial automation sectors;
- **Future Trends:** Analysing how AI-driven threat detection, digital twin security, and blockchain-based authentication for security could enhance cybersecurity.

It addresses security provision objectives, thereby providing the full body of knowledge on securing design files, manufacturing processes, and engineering workflows against cyber threats to secure intellectual property in mechanical engineering proactively.

2. Cybersecurity Risks in Mechanical Design and Manufacturing

The growing dependency on digital tools within the field of mechanical engineering has resulted in notable cybersecurity risks. The potential for Intellectual Property (IP) theft, data breaches, unauthorized access, and industrial espionage presents substantial dangers to design files, manufacturing procedures, and proprietary technologies. (2) Key cybersecurity vulnerabilities found in mechanical design and production primarily arise from deficiencies in CAD and PLM systems, supply chain inadequacies, threats from reverse engineering, alongside insider threats.

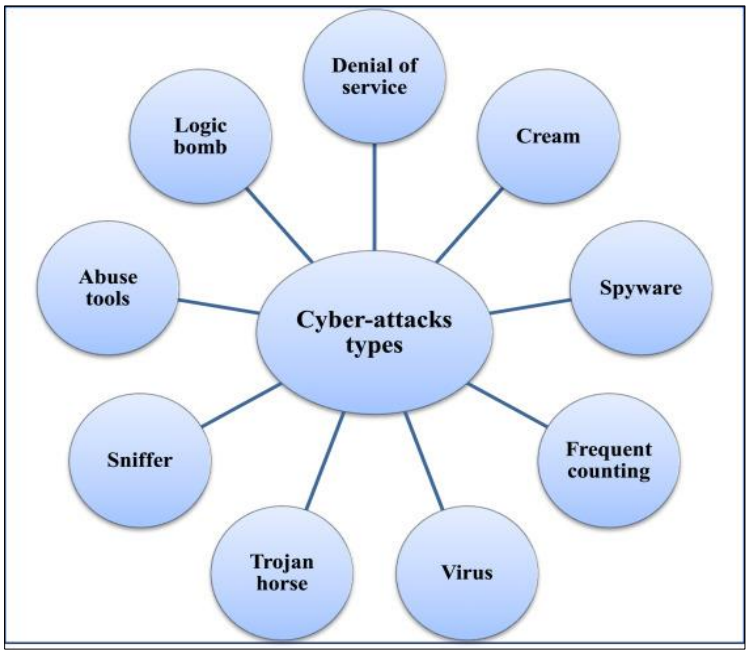

Figure 3 Shows the types of cyber attacks

2.1. Cyber Threats to CAD and PLM Systems

2.1.1. Unauthorized Access to CAD Files

Computer-Aided Design (CAD) software is fundamental in mechanical engineering as it is utilized for creating component designs, simulating operational behavior, and enhancing manufacturing processes. Nonetheless, these files harbor sensitive information such as unique geometries, material details, and performance metrics that cybercriminals find enticing targets for attacks. Instances of unauthorized access are often facilitated by:

- Inadequate authentication measures like weak or commonly shared passwords.
- Phishing schemes where attackers mislead personnel into divulging credentials.
- Maliciously crafted CAD plugins that can invade an engineer's system to exfiltrate files.
- Improper configurations of cloud storage resulting in unintended public exposure of confidential documents.

2.1.2. Cyberattacks on Product Lifecycle Management (PLM) Systems

PLM systems maintain comprehensive records of product development life cycles including updates on revisions, simulations performed during testing phases, and collaboration logs with suppliers. (5) Given their accessibility to numerous stakeholders they face significant vulnerabilities characterized by:

- Credential theft enabling infiltrators access to online PLM platforms.
- Privilege escalation strategies that empower unauthorized entities to alter or abscond with critical information.
- Man-in-the-middle (MITM) tactics allow intruders to intercept communications between engineers and manufacturers.

A pertinent illustration is the 2018 attack on Airbus wherein hackers specifically targeted supplier PLM systems aiming to extract valuable aircraft design information.

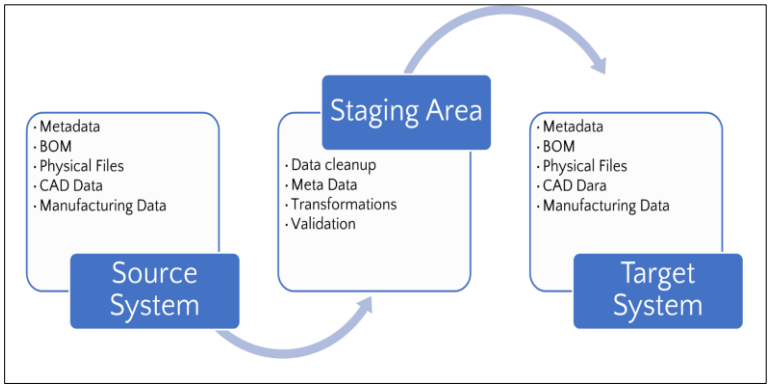

Figure 4 Shows online PLM process

2.2. Supply Chain Vulnerabilities

2.2.1. Third-Party Manufacturers and IP Leaks

Numerous companies engaged in mechanical engineering delegate portions of their production operations to third-party manufacturers or suppliers due largely to cost efficiencies offered by outsourcing practices. Such supply-chain partners are frequently entrusted with delicate blueprints along with detailed specifications regarding materials but this reliance renders them potential weak points within a company's overall cybersecurity strategy. (4) Common risks include:

- Data leaks from the leak of data due to poor cybersecurity practices at outsourced manufacturers.
- Unauthorized duplication of mechanical components from stolen design files.
- Lack of visibility and monitoring over sensitive data handling actions by suppliers.

2.2.2. Cyber Attacks Targeting Suppliers

Attackers may try to breach the suppliers in order to gain access to critical design data in an indirect manner. Supply Chain Attacks usually consist of:

- Compromised emails (Business Email Compromise-BEC): Hackers impersonate some trusted supplier to have sensitive CAD files.
- Ransomware attacks that encrypt supplier databases and ask for payment for data release.
- Compromised software updates, where an attacker inserts malware code contained within the vendor-supplied software updates for the manufacturer.

An example is the attack on Visser Precision-supplier from 2019-which served aerospace companies such as Tesla and Lockheed Martin. The hacker leaked the proprietary mechanical designs after obtaining access through weak controls in the supply chain.

2.3. Reverse Engineering and Counterfeiting Risks

2.3.1. Unauthorized 3D Printing of Mechanical Components

Additive Manufacturing or 3D printing revolutionized mechanical engineering by enabling fast prototyping and customized production. However, leakage of design files may help the unauthorized use of computer-aided design for the reproduction of a proprietary component. The risks include:

- Counterfeiting of high-value mechanical parts by illicit 3D printing.
- Counterfeit components failing to comply with safety industrial standards, which pose a risk for poor performance.
- State-sponsored actors replicating military-grade mechanical components using stolen designs.

A real-world example was the theft of 3D printing files for aerospace parts, with counterfeit components entering the market thereby risking system failures.

2.3.2. Reverse Engineering of Proprietary Designs

Attackers may use scanning techniques (CT-scan, laser scanning) to reverse-engineer some proprietary components. Reverse engineering leads to:

- Loss of competitive advantage, allowing competitors to recreate products without investments on R&D.
- Fraud investigations into patent infringement.
- Market flooding with counterfeit mechanical parts affecting brand reputation.

Automotive industry is an example in which counterfeit turbochargers entered the global supply chain in this way based on reverse-engineered designs, posing performance and reliability issues for the vehicles involved.

2.4. Insider Threats in Mechanical Engineering Firms

2.4.1. Employee IP Theft and Corporate Espionage

While insider threats can be very tricky to mitigate, they often involve employees or contractors who have, by virtue of their assignments, legitimate access to proprietary data. Such insider threats are:

- Disgruntled employee stealing CAD files prior to leaving the company.
- Corporate espionage is subsidized by rival companies acquiring sensitive information.
- Inefficient offboarding processes enabling ex-employees to retain access to the company's networks.

For example, in one of the biggest scandals, a former employee of Waymo (Google's self-driving car division), transferred 14,000 confidential files to a competitor, Uber, which triggered a high-profile legal battle.

2.4.2. Accidental Data Exposure

Not all insider threats are intentional. Many cybersecurity breaches happen because someone is negligent, such as:

- Weak password usage and sharing of login credentials.
- Unintentional exposure of CAD files onto publicly accessible file-sharing platforms.
- Failure to apply security patches, leaving room for systems to be attacked.

3. Secure Design and Manufacturing Framework

In this section we have set forth the recommendations on how to protect the IP in mechanical engineering. Manufacturers should deploy sound cyber-protective designs facilitating and securing design files, manufacturing processes, and supply chain interactions. (6) The Secure Design and Manufacturing Framework embodies multiple

security layers: encryption, blockchain authentication, Zero Trust Architecture (ZTA), and secured cloud collaboration. This effectively helps preclude unwarranted access to, or theft and misuse of, industrial property.

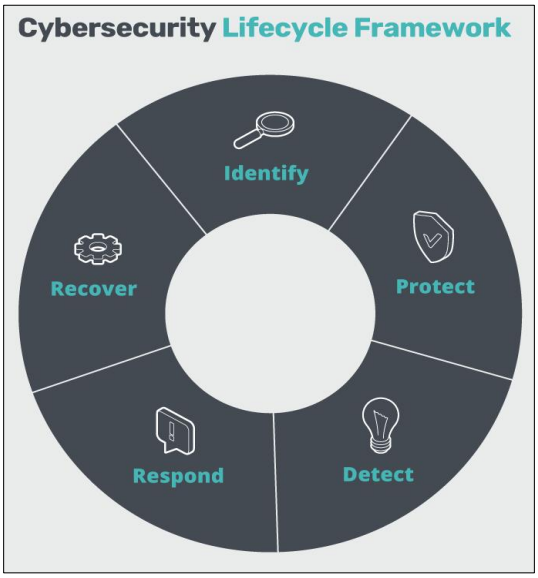

Figure 5 Shows cybersecurity process framework

3.1. Implementing Encryption for Design Files and PLM Systems

3.1.1. Encryption Techniques for CAD and Simulation Files

Design data contained within CAD, simulation, and digital twin files is privileged, and hence they must be kept confidential only for authorized end users. Among the key encryption strategies are the following:

- **End-to-End Encryption (E2EE):** Encrypts the CAD file before transmission so that, even if intercepted, the attacker cannot read it.
- **AES-256:** A strong encryption standard utilized to protect design files from unauthorized access while in storage.
- **Digital Rights Management (DRM) for CAD files:** Prevents unauthorized copying or printing or modification of any files.

3.1.2. Securing Product Lifecycle Management (PLM) Systems

PLM systems keep records of design versions, collaboration histories, and sensitive manufacturing data. To secure them:

- **Role-based Access Control (RBAC):** To ensure engineers, suppliers, and executives have access only to data relevant to their roles.
- **MFA:** Multifactor Authentication requires one or more extra layers of verification beyond normal credentials.
- **Automated Data Expiration Policies:** This Deletes or archives design files after project completion preventing unwanted exposures.

For example: An aerospace manufacturer implemented MFA for the PLM system in 2022, reducing access incidents by 80%.

3.2. Blockchain-Based IP Protection

3.2.1. Blockchain for Authenticating Design Files

Blockchain technology provides legitimate proof of design file ownership that cannot be tampered with. The manufacturer may record revision histories and access logs on an immutable ledger:

- Verify the authenticity of CAD files before sending them to suppliers.
- Prevent unauthorized modifications by maintaining a log of all edits made to an existing design.

- Use smart contracts to allow or deny access to designs that can be changed dynamically.

Example: A robotics firm could detect counterfeit components through blockchain authentication by verifying that the designs traced back to authorized suppliers.

3.2.2. Integrity of Decentralized Manufacturing

Blockchain can also bolster the legitimacy of the manufacturing process by ensuring that production proceeds according to approved specifications. This is essential to prevent:

- Unauthorized changes made to product designs during production.
- Counterfeit parts introduced into mechanical assemblies.
- Tampering with additive manufacturing (AM) settings that could adversely impact a part's performance.

Example: Blockchain-protected manufacturing logs that keep track of defense aerospace parts provide assurance that the parts meet stringent compliance specifications, minimizing supply chain fraud.

3.3. Zero Trust Architecture (ZTA) for Manufacturing Security

3.3.1. Zero Trust Architecture:

A Zero Trust Architecture (ZTA) is based on the "Never Trust, Always Verify" principle and requires continuous authentication for every access request. This becomes vital for:

- Engineering teams performing collaborative work on CAD designs remotely.
- Manufacturing partners accessing design files from remote locations.
- Cloud-based PLM systems being exposed to unauthorized access.

3.3.2. Implementing Zero Trust in Mechanical Engineering

Micro-segmentation puts the different parts of the network resources shared among CAD files, manufacturing data, and supplier information into separate security zones. (5) Continuous identity verification means that an AI-driven monitoring of user behavior enables the detection of suspicious logins from unknown locations.

Least privilege access: This limits the permission for design modification to only those that are necessary.

Example: A global industrial automation firm instituted ZTA for its design team, which has reduced unauthorized access attempts to files by 60% in the first year.

3.4. Secure Collaboration and Cloud-CAD Systems

3.4.1. Signing into Cloud-Based CAD and PLM Systems

With most companies transitioning their design sharing to the cloud, accessing data without authorization becomes essential for security. Recommended best practices include:

- **End-to-End Encryption for Cloud Storage:** It ensures that stored CAD files cannot be viewed even by cloud providers.
- **Private Cloud Deployments for Sensitive Data:** Compared to public cloud platforms, users have gained enhanced control over access through private cloud servers.
- **Real-Time User Access Logs and Alerts:** The engineers receive instant alerts for any breach subscribed by a separate user into a design file.

Example: A mechanical engineering company specializing in turbines uses AI-enabled access monitoring for secure cloud storage that blocked attempted online attacks over a time span of 6 months.

4. Conclusion

The accelerated digitalization of mechanical designs and manufacturing adds fresh cybersecurity challenges, hence IP theft has become a matter of great concern for an industry heavily dependent on proprietary engineering knowledge.

To mitigate this, encryption, blockchain authentication, Zero Trust security frameworks, and secure collaboration platforms must be implemented by industries to safeguard their IP. (1) Real-world case studies highlight once again efforts made by firms in aerospace, automotive, and industrial automation niches to beef up their cybersecurity posture. In the future, AI-driven threat detection and secure Digital Twin models will be key in protecting the mechanical engineering IP. Mechanical engineering firms can maintain their competitive advantage and protect their intellectual assets in an increasingly interconnected world only by taking the initiative in cybersecurity.

Compliance with ethical standards

Disclosure of conflict of interest

There is no conflict of interest to be disclosed.

References

[1] Patnaik, Satwik, et al. "Best of Both Worlds: Integration of Split Manufacturing and Camouflaging into a Security-Driven CAD Flow for 3D ICs." (2018).

[2] Yasaei, Rozhin, et al. "GNN4IP: Graph Neural Network for Hardware Intellectual Property Piracy Detection." arXiv:2107.09130 (2021).

[3] Dhavlle, Abhijitt. "Reverse Engineering of Integrated Circuits: Tools and Techniques." arXiv:2208.08689 (2022).

[4] Knechtel, Johann, et al. "Protect Your Chip Design Intellectual Property: An Overview." arXiv:1902.05333 (2019).

[5] Kianpour, M. (2021). Socio-Technical Root Cause Analysis of Cyber-enabled Theft of the U.S. Intellectual Property -- The Case of APT41. arXiv:2103.04901.

[6] Machine Design. "Securing Intellectual Property in Manufacturing through Advanced Application Security." Machine Design, https://www.machinedesign.com/automation-iiot/article/21281869/securing-intellectual-property-in-manufacturing-through-advanced-app-security.