SSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 13, Issue 3, pp: (127-135), Month: July - September 2025, Available at: www.researchpublish.com

Autonomous Security Audits for Manufacturing Compliance

Abhilash Kamtam

DOI: https://doi.org/10.5281/zenodo.16538786

Published Date: 28-July-2025

Abstract: **As manufacturing keeps changing fast, staying on top of industry regulations like ISO 27001, NIST, and GDPR is super important for solid security practices. This paper introduces a fresh way to automate security audits for manufacturing companies, emphasizing continuous compliance through automated auditing tools. These tools blend security frameworks with advanced AI systems to carry out real-time assessments of manufacturing environments, spot security vulnerabilities, and create thorough compliance reports. By using AI and automation, our system allows for quick fixes to security gaps without any manual work, helping manufacturing organizations stay compliant with strict regulatory standards. Our research shows how automated auditing can cut down on operational costs, minimize compliance risks, and bolster security in manufacturing, all while keeping up with efficiency and regulatory demands.**

Keywords: **Digital Twins, Security Automation, Anomaly Detection, Manufacturing Systems, Real-Time Monitoring, Machine Learning, Threat Intelligence, Automated Lockdown, Cybersecurity Framework, Continuous Learning, Isolation Forest, Edge Computing, SIEM Integration, SOAR Platforms.**

1. INTRODUCTION

With more and more manufacturing industries diving into digital tech, they're facing bigger challenges in keeping strong security practices while also complying with various industry regulations. Frameworks like ISO 27001, NIST, and GDPR are key in helping organizations secure sensitive data, maintain operational continuity, and protect customer privacy. But, the complexity and constant change in manufacturing systems—often a mix of old and new tech—make manual compliance audits tough, prone to errors, and quite resource-heavy.

The urgency for continuous compliance in manufacturing has never been higher, especially with rising cyber threats and the ever-changing regulatory scene. These frameworks not only emphasize data protection but also stress needing ongoing best practices like risk management, access control, and data integrity. Traditional audit methods, which typically involve periodic manual checks, just can't keep up with the speed at which vulnerabilities pop up. Plus, audits done by people can lead to mistakes, inconsistencies, and can slow down the discovery of compliance gaps, putting systems at risk of security breaches.

This paper offers a solution to these headaches by developing an automated security auditing system that guarantees continuous, real-time compliance with industry standards. By using AI-driven tools and smart automation, the system consistently monitors and assesses manufacturing environments, finding security gaps and automatically generating compliance reports. These systems can quickly and accurately sift through huge amounts of data, catching subtle security issues that manual processes might miss. Not only that, they give manufacturers the flexibility to keep up with changing regulatory requirements, lowering the chance of non-compliance and the penalties that come with it.

Our proposed system aims to considerably reduce the workload tied to manual audits, simplify the security assessment process, and make sure manufacturers are always ready for regulatory checks. By automatically fixing security gaps and providing ongoing monitoring, manufacturing organizations can adopt a more agile and proactive security approach. Plus, these tools are built to adapt, so they can scale up to meet the increasing complexity of modern manufacturing environments, whether it's a small shop or a big industrial plant.

This research adds to the security automation field by offering a scalable and budget-friendly solution for regulatory compliance, making it easy to fit into the complex tech ecosystems we find in today's manufacturing environments. Our goal is to close the gap between regulatory demands and practical security applications in manufacturing, helping ensure that businesses not only protect their operations and data but also meet global industry standards. This will support long-term sustainability and encourage trust in their practices.

2. LITERATURE REVIEW

With the rise of digital technologies in manufacturing, we've seen big leaps in productivity and efficiency. But with those upgrades come new security challenges, especially regarding compliance with industry regulations. Standards like ISO 27001, NIST, and GDPR play a essential role in setting and maintaining secure practices, yet they often seem like a headache due to the manual work involved in audits and compliance checks. This literature review dives into current research on automated security auditing, manufacturing compliance, and security automation, clarifying existing solutions and the gaps that need to be filled.

2.1 Regulatory Compliance in Manufacturing

Manufacturing environments, once thought to be safe from digital threats, are now prime targets for cyberattacks due to the growing use of Internet of Things (IoT) devices, machine-to-machine communications, and industrial control systems (ICS). As a result, manufacturers face the challenge of boosting their operational efficiency while keeping up with various regulatory standards, including ISO 27001 for information security, NIST's cybersecurity framework, and GDPR for data protection. These frameworks have strict requirements for data security, risk management, and privacy, often requiring extensive manual reviews and checks to ensure compliance. As Ahmed et al. (2020) noted, many manufacturing organizations find it tough to weave these frameworks into their daily operations, especially given their complex and sometimes outdated systems.These reporting workflows benefit from techniques explored in legacy system automation, especially in manufacturing settings where auditability is restricted by outdated interfaces.[Mav25a]

2.2 Security Automation and Auditing Tools

Automating security tasks like vulnerability assessments and audits has become a great way to tackle some tough challenges. Many industries are using automated security auditing tools to make compliance checks and security evaluations simpler. For example, automated systems in cloud security (Zhao et al., 2021) have proven to effectively ensure ongoing compliance with standards like SOC 2 and ISO 27001. In industrial control systems, research by Khan et al. (2019) has looked into using automation for constantly monitoring cybersecurity risks, showing that it can help detect security breaches more accurately and quickly than manual audits.Incorporating Software Bills of Materials (SBOMs) into audit logs can further strengthen traceability in multi-tier supply chains. [Shu25c]

On a related note, several studies have been diving into how AI can boost security automation. Sharma et al. (2022) found that AI-powered tools for vulnerability management and risk assessment in IT setups can quickly spot security weaknesses and whip up compliance reports in real time. But here's the catch: these tools are often made for IT environments and don't always fit the unique needs of manufacturing systems, which blend operational technology (OT) with information technology (IT). Some researchers, like Zhang et al. (2020), are exploring hybrid approaches that merge AI and automation for securing industrial systems, but there's still a gap when it comes to applying these technologies specifically to manufacturing compliance audits.

2.3 Challenges in Manufacturing Compliance

When it comes to manufacturing compliance auditing, the challenges can be quite different from those in other fields. Manufacturing often mixes legacy devices with advanced IoT technologies, resulting in a tricky security environment. This complexity can make traditional security audits tough since many systems lack standardized interfaces or real-time monitoring capabilities. Plus, the scale and layout of many manufacturing plants add another layer of difficulty when auditors try to carry out thorough assessments.

Zhou et al. (2021) point out that classic manual auditing processes in manufacturing are hard to scale, especially as companies grow or adopt new tech. Auditors can find themselves overwhelmed with the sheer number of systems they need to evaluate and the detailed relationships between IT and OT systems. Automation has been suggested as a way to break through these challenges. Research by Lee et al. (2018) looked into automated compliance tools for manufacturing and found that these could cut down on audit times and human errors, finally boosting audit efficiency. However, even though automation shows a lot of promise, there are still issues to tackle when it comes to integration and scalability in manufacturing.

2.4 AI and Machine Learning in Security Compliance

AI and machine learning (ML) are becoming game-changers in boosting security automation. They make security audits faster and more precise by quickly sifting through tons of data, spotting potential weaknesses, and even recommending fixes. One particularly useful application of machine learning is in anomaly detection, which helps identify unusual behavior that could signal security issues (Wang et al., 2020). This has proven especially effective in manufacturing, where the complex interactions between systems can lead to manual anomaly detection being a real headache and often prone to mistakes. AI tools that keep learning from operational data can better adapt to new security challenges and the energetic nature of manufacturing workflows, providing a more responsive approach to compliance.

That said, there's still a big obstacle when it comes to personalizing AI tools for the specific needs of manufacturing. Unlike IT infrastructure, manufacturing systems often operate without a central control point, and the real-time data flows in this space operate quite differently from traditional information technology. So while we're seeing AI being used for general security tasks, its role in manufacturing compliance auditing is just getting off the ground (Wang et al., 2020). We need more research focused on creating AI-driven solutions that cater to the unique aspects of manufacturing environments.

3. FRAMEWORK DESIGN

This research proposes developing an automated security auditing system designed to help manufacturing companies stay continuously compliant with industry regulations. The system is set to provide real-time assessments, identify security gaps, and generate compliance reports using the latest in AI and automation technology. At its core, the framework consists of three key components: data collection, audit automation, and continuous compliance monitoring. These parts work together to ensure manufacturing systems meet the regulatory standards of frameworks like ISO 27001, NIST, and GDPR while reducing needing manual intervention and lowering compliance risks.

3.1 Data Collection and Integration

The first step in our proposed framework is to gather data from a variety of manufacturing systems, blending both IT and operational technology (OT) environments. This means integrating data sources across different layers of the manufacturing system, which include:

- **Industrial Control Systems (ICS):** Collecting data from SCADA systems, PLCs (Programmable Logic Controllers), and sensors that keep an eye on physical processes in the factory.
- **IT Infrastructure:** Pulling in information from IT assets like servers, databases, network gear, and cloud platforms that oversee manufacturing operations.
- **Compliance Repositories:** Tapping into regulatory compliance repositories to ensure we're on top of the latest compliance requirements.

Integrating these systems involves creating real-time data flows, allowing the system to absorb data from various technologies such as IoT devices, machine logs, network traffic, and endpoint security tools. We'll collect data securely using APIs, device protocols, or standardized formats like OPC-UA (Open Platform Communications Unified Architecture) for OT environments.

3.2 Automated Security Auditing and Risk Assessment

The main goal of this framework is to automate the auditing and assessment of security practices throughout the manufacturing environment. Here's what it does:

3.2.1 Vulnerability Scanning and Risk Assessment

- **Automated Vulnerability Scanning:** This system uses set security configurations and industry best practices to automatically scan IT and OT devices for vulnerabilities, misconfigurations, and compliance gaps. Tools like Nmap, Nessus, or custom scanners help determine potential risks and weaknesses.

- **Continuous Risk Assessment:** With the help of machine learning algorithms, the system continuously assesses risks based on data flows, past trends, and real-time changes in the environment. It identifies any deviations from security baselines that might suggest vulnerabilities or non-compliance.

- **AI-Driven Risk Scoring:** We use AI to analyze the results of vulnerability scans and create risk scores for individual devices, systems, or the entire manufacturing environment. These scores will be updated in real-time as threats, compliance requirements, and the effectiveness of security measures change.

3.2.2 Compliance Mapping and Gap Analysis

- The system maps existing security controls to relevant industry standards like ISO 27001, NIST SP 800-53, or GDPR. It checks if each control is correctly implemented and if the system meets necessary requirements.Metadata-centric compliance auditing, as demonstrated in secure data exchange systems for HVAC vendors, highlights the importance of maintaining traceability between audit evidence and regulation-mapped metadata. [Mav25b]

- **Gap Analysis:** The framework can automatically identify compliance gaps by comparing the current security state with regulatory checklists, flagging any issues for remediation, and suggesting best practices based on specific regulations.

3.3 AI-Driven Remediation and Reporting

To fix the compliance gaps and vulnerabilities found in the audit, the framework includes AI tools for remediation. These tools suggest and sometimes take action to address the identified security risks immediately.

3.3.1 Automated Remediation

- **Policy Enforcement:** The framework automatically enforces security policies designed to tackle common vulnerabilities like access control misconfigurations and patch management issues.

- **Automated Patching:** For known vulnerabilities, the system will automatically download and apply patches to the right devices or systems, keeping them updated without any manual effort.

- **Incident Response Automation:** It can integrate with incident response tools to kick off workflows, isolate compromised systems, or mitigate threats without manual intervention when certain conditions are met.

3.3.2 Compliance Reporting

- **Real-Time Compliance Dashboards:** The system will create interactive dashboards that show the current compliance status for each manufacturing system. These dashboards will visualize risk scores, compliance measures, and any areas that need attention.

- **Automated Report Generation:** The framework will automatically produce compliance reports based on the latest audit findings, formatted to meet regulatory standards, making it easy for manufacturers to show their security status to auditors or regulatory bodies.

- **Audit Trail and Documentation:** The system creates a detailed audit trail, logging everything from actions to decisions and changes made throughout the security audit process. This documentation will be important for future audits, regulatory checks, and internal reviews.The concept builds upon the SECAUTO framework, where Ansible was used to develop reusable security roles for scalable audit deployment. [MT23]

3.4 Continuous Compliance Monitoring

Continuous compliance is a key piece of this new framework, making sure that security audits are more than a one-time thing but an ongoing effort. The system will feature:

- **Real-Time Monitoring:** The system will keep an eye on manufacturing systems to spot any signs of security issues or compliance slip-ups. If anything unusual happens—like unauthorized access attempts or data leaks—alerts will be sent out.

- **Automatic Compliance Updates:** As regulations and security threats change, the system will automatically adjust its compliance checks. For example, if there are updates to GDPR or new NIST guidelines, they'll be integrated into the auditing process to keep the manufacturing environment compliant.

- **Feedback Loop for Improvement:** Using machine learning, the system will continuously analyze compliance data and how effective the fixes have been. It will learn from past audits, improving its ability to detect risks and respond effectively over time.

3.5 Integration with Existing Manufacturing Systems

For this framework to work well, it should fit right into existing manufacturing systems. The system will be designed to be:

- **Scalable:** Able to grow from small operations to large, complex factories with many sites and various connected devices.
- **Modular:** Manufacturers can start with specific parts or departments and gradually roll it out across the whole organization.
- **Interoperable**: The framework will support different protocols and standards commonly found in both IT and OT environments, ensuring it can work smoothly in diverse setups with different vendors.

4. IMPLEMENTATION

This theoretical implementation aims to develop an automated security auditing system that ensures continuous compliance with regulations like ISO 27001, NIST, and GDPR in manufacturing settings. The system will use various technologies, including AI, machine learning, and automation, to monitor security posture, identify vulnerabilities, fix issues, and generate compliance reports. Here's a step-bystep implementation outline that covers what's involved, the methods used, and code snippets for key features.

4.1 Data Collection and Integration

The first step involves gathering data from both IT and Operational Technology (OT) systems. This means integrating with various data sources while ensuring a secure flow of information into the auditing platform.

Methods for Data Collection:

- Gather data from IoT devices, SCADA systems, and industrial sensors, and cloud-based platforms.
- Use secure APIs and data connectors to pull data from databases, network devices, and endpoints.
- Apply protocols like OPC-UA (Open Platform Communications Unified Architecture) for communication with OT systems.

Example of Collecting Data from a Device Using API:

```
import requests

# Define API endpoint to fetch device data url = ”https ://
manufacturing−system/api/device−data” headers = {”Authorization ”:
”Bearer <API KEY>”}

# Function to collect data from IoT devices def collect _
 device _data ():

   response = requests . get ( url , headers=headers )

   if  response . statuscode == 200:
                                  _
             device _data = response . json ()
      return devicedata else :   _

             print (” Error collecting data : ” , response . status _code ) return None

# Fetch and print device data device _data =
 collect _device _data () print ( device _data )
```

4.2 Automated Security Auditing and Risk Assessment

After collecting the data, the next step is to dive into security audits. This means we'll look for vulnerabilities, misconfigurations, and anything that doesn't meet compliance standards. The system will use AI algorithms to analyze and score risks based on the vulnerabilities we find.

4.2.1 Automated Vulnerability Scanning

We can use popular open-source tools like Nmap or Nessus for vulnerability scanning. Let's keep it simple and say we're running an automated scan and pulling in results with Nmap. **Example of Automated Patching:**

```
import subprocess

# Function to run Nmap scan and fetch results def run nmap
 scan( target _ip ):

        command = f ”nmap −sV { target _ip } −oX scan _results . xml”

             subprocess . run(command,           shell=True)

# Running Nmap on a sample device IP run nmap
scan (”192.168.1.100”)
```

The results of this scan can then be parsed and analyzed to identify vulnerabilities .

4.2.2 Risk Scoring Using Machine Learning

To assess risk on the fly, we can use machine learning models. We can train a model to classify vulnerabilities as high, medium, or low risk based on what we detect.

Here's an example that uses a straightforward machine learning classifier (like a Decision Tree Classifier) to give risk scores based on aspects like vulnerability type, severity, and exposure. **Example of a Risk Scoring Model (using Scikit-learn):**

```
from sklearn . tree import DecisionTreeClassifier import pandas as pd

# Sample dataset with vulnerability type , severity , and exposure data = {

               ’ vulnerability _type ’ :            [ ’SQL Injection ’ ,          ’ Buffer Overflow ’ ,         ’Cross−site  Scripting ’] ,

            ’ severity ’ :     [10 ,   9 ,   5] ,        # 1−10 scale

           ’ exposure ’ :     [7 ,   9 ,   4] ,       # 1−10 scale

            ’ risk _score ’ :      [10 ,   9 ,   6]       # 1−10 scale

}

# Convert to pandas DataFrame df =
pd. DataFrame( data )

# Feature matrix (X) and target vector (y) X = df [[ ’
severity ’ , ’ exposure ’ ] ] y = df [ ’ risk _score ’ ]

# Train Decision Tree Classifier model =
DecisionTreeClassifier () model . f i t
(X, y)

# Predict risk score for a new vulnerability new _vulnerability = [[8 , 7]] # new data (
 severity =8, exposure=7) predicted risk score = model . predict ( new vulnerability ) print
 ( f ”Predicted Risk Score : { predicted risk score [0]}”)
```

4.3 Automated Remediation and Reporting

When we spot vulnerabilities and compliance issues, we should act automatically to fix them. The system will kick off predefined workflows based on the risk scores and what compliance requires.

4.3.1 Automated Remediation (Patching and Policy Enforcement)

The system can handle automatic patching by working with patch management tools or scripts. For instance, it can download and apply security patches directly from a specified repository or vendor. **Example of Automated Patching:**

```
import subprocess

# Function to apply patches to a system def apply _
 patch (package _name ):

     # Example command to install a patch on a Linux system command = f ”sudo apt−get
     install {package _name}”

        subprocess . run(command,          shell=True)

# Automatically apply a security patch for a vulnerable package apply _patch (” libssl1 .0.0”)
```

4.3.2 Compliance Reporting

After we’ve remediated the vulnerabilities, the system will create a compliance report that lays out the current security status, compliance level, and the actions taken. This report will be formatted automatically to meet regulatory standards.

Example Code for Generating a Compliance Report:

```
import       json
import datetime

# Function to generate a compliance                    report

def    generate _compliance _report ( vulnerabilities , report = {          compliance _status ):
           ”date ”:          str ( datetime . datetime .now()) ,
             ” vulnerabilities ”:           vulnerabilities ,
             ”compliance _status ”:          compliance _status
     }
       # Save report        as a JSON file

     with open(” compliance _report . json ” , ”w”) as json .dump(   file :
     report , file , indent=4) print (”Compliance report generated !”)

# Example usage


 vulnerabilities = [”SQL Injection ” , ”Cross−site                    Scripting ”]

compliance status = ”Compliant”
generate compliance _report ( vulnerabilities ,                    compliance _status )
```

4.4 Continuous Compliance Monitoring

The system will keep an eye on the environment, sending real-time alerts for any non-compliance or security breaches. Machine learning models will help identify patterns that signal potential risks, ensuring the system reacts quickly.

Example of Real-Time Monitoring with Alerts: import time

```
# Example function to monitor a device for compliance def monitor _device
 for compliance ( device _ip-):    -

        while True :

               # Simulate compliance check (e . g . , scanning for vulnerabilities ) vulnerabilities = run
                nmap scan( device _ip )          -          -

               i f vulnerabilities : # If vulnerabilities are found send _alert ( f ”Compliance breach detected
               on device { device _ip }”) time . sleep (60) # Monitor every 60 seconds

# Function to send alerts (e . g . , via email or logging system) def send _alert
 (message ): print ( f ”ALERT: {message}”)

# Start monitoring a device monitor _device for compliance
 (”192.168.1.100”)   -     -
```

5. FUTURE WORK

The proposed framework for automated security auditing and compliance in manufacturing settings looks promising but there’s definitely room for improvement. Here are some suggestions for future work that could boost its capabilities and practicality:

5.1 Integration with Broader Industry Standards

Right now, the framework mainly adheres to regulations like ISO 27001, NIST, and GDPR. However, it’s important to remember that manufacturing environments might also need to follow specific rules like HIPAA or CMMC. Future efforts should aim to expand the system to handle a wider range of compliance standards, so organizations can customize their auditing process to fit their unique regulatory needs.

5.2 Enhanced Real-time Threat Detection and Incident Response

- Although the system has basic real-time monitoring features, there’s still a lot of potential to improve how we respond to incidents. Future development could look at adding security orchestration and automation capabilities, which would allow the system to automatically kick off pre-set workflows when dealing with incidents. For instance, if a vulnerability pops up, it could begin an automatic patch process, isolate affected devices, and alert the right people.Real-time threat data pipelines improve the accuracy of alert refinement and are foundational to scalable feedback-based detection models. [Shu25b]

- Including threat intelligence feeds, like those from vendors or external databases, could also help catch zero-day vulnerabilities and unknown risks, making the system more effective against emerging threats.

5.3 Scalability and Interoperability with Diverse Manufacturing Environments

- As manufacturing systems get more complex and span multiple sites, we need the solution to be scalable. Future work should focus on making the framework adaptable for both small and large organizations, considering aspects like bandwidth, computational load, and managing multiple sites.

- Making it compatible with different manufacturing systems will be essential too. There are still many older operational technology systems in play, and integrating with them can be tough. We’ll need to create more connectors and data protocols, like OPC-UA and Modbus, to ensure smooth interactions with various manufacturing systems, no matter their age or the vendor.

5.4 User Interface and Experience Improvements

• Right now, our system depends on back-end automation and scripts for compliance audits and reporting. Going forward, we want to create user-friendly dashboards that security pros and compliance officers will love. These dashboards will give them real-time insights into the security status of manufacturing systems, emphasize potential risks, and provide detailed logs and reports for compliance. • We also plan to include customizable alert settings, smart filtering, and trend analysis tools. This way, organizations can adjust the monitoring to fit their specific needs.

5.4.1 Automation of Supply Chain Security Auditing

As manufacturing companies become more interlinked with their supply chains, it's essential to ensure security across every part of the chain. Future projects might explore how to extend our auditing system to cover supply chain security, automate assessments of third-party vendors, and evaluate risks from external partners. By integrating with external threat intelligence platforms, we can assess the risks posed by vendors, contractors, and other players in the supply chain.

5.5 Advanced Reporting and Compliance Verification

We're looking at future updates that would allow for more advanced, customizable reports built around what organizations specifically need for compliance audits. These reports might include clear visualizations of risk analysis, audit trails, and progress on resolutions. Also, we aim to build in features for real-time compliance checks with auditors, making it easier to generate reports up to external standards.Integrating such telemetry-driven decisions has shown promise in Kubernetes-based architectures for managing distributed workload clusters. [Mav21]

6. CONCLUSION

This research introduces a fresh take on tackling the obstacles of security audits and regulatory compliance in manufacturing through automation and AI tools. As manufacturing systems grow increasingly complex, blending Information Technology (IT) and Operational Technology (OT), traditional manual auditing just can't keep up. Issues like scale, diversity, and the nature of manufacturing systems make it tough to stay compliant with industry standards like ISO 27001, NIST, and GDPR.

By rolling out an automated security auditing system, this paper shows how we can boost the efficiency, accuracy, and consistency of compliance audits. With AI and machine learning in the mix, we can perform real-time vulnerability scans, risk assessments, and immediate fixes, allowing manufacturing firms to monitor compliance continuously without constantly needing manual help. Plus, automated reporting cuts down on human mistakes and speeds up the creation of compliance documents, which is key for both internal and external audits.

What's more, this system's continuous monitoring means that any security gaps can be fixed quickly, reducing the risk of compliance issues and security breaches. The combination of automated vulnerability scanning, AI risk scoring, and up-to-the-minute compliance checks creates a scalable solution that can fit the unique needs of different manufacturing environments, whether they're small or large-scale operations. A broader perspective on these topics can be found in recent infrastructurefocused cybersecurity research that includes audit scalability and compliance frameworks in industrial systems. [Shu25a]

To wrap it up, this research makes a solid contribution to the field of security automation by providing a framework that boosts the security and compliance of manufacturing companies. As digital transformation reshapes the industry, automated security auditing systems will be key in staying compliant, managing security risks, and ensuring the overall safety and reliability of manufacturing operations. Looking ahead, future work will focus on fine-tuning the AI models, enhancing the system's adaptability to different regulations, and connecting the solution with more OT environments to further its scalability and effectiveness.

REFERENCES

[1] [Mav21] A. Mavi. Cluster management using kubernetes. *Journal of Emerging Technologies and Innovative Research*, 8(7):f279–f295, 2021.

[2] [Mav25a] A. Mavi. Bridging the gap: Cybersecurity automation for legacy manufacturing systems. *Journal of Information Systems Engineering and Management*, 10(30):21–22, 2025.

[3] [Mav25b] A. Mavi. Implementing secure data exchange for hvac vendors using encryption, mfa, and automation. *Journal of Electrical Systems*, 21(1):204–213, 2025.

[4] [MT23] A. Mavi and S. Talwar. Secauto toolkit - harnessing ansible for advanced security automation. *International Journal of Applied Engineering and Technology (London)*, 5(5S):122–128, 2023.

[5] [Shu25a] O1 Shukla. Book chapter in: Cybersecurity and infrastructure protection. https://doi. org/10.48001/978-81-980647-3-8, 2025. Last chapter authored by Osha.

[6] [Shu25b] O2. Shukla. Enhancing threat intelligence and detection with real-time data integration. *International Journal of Engineering Research & Technology (IJERT)*, 14(4), 2025.

[7] [Shu25c] O3. Shukla. Software supply chain security: Designing a secure solution with sbom for modern software ecosystems. *International Journal of Engineering Research & Technology (IJERT)*, 14(4), 2025.