PROTECTING URBAN MOBILITY: CYBERSECURITY FOR ESCALATOR SYSTEMS

Mahesh Wakchaure, Shubham Jambhe
R&D, Schindler India Pvt. Ltd., India

KEYWORDS: Cyber-Security, Escalator, SDL, Threats, Urban Mobility

1 ABSTRACT

In today's interconnected world, the cybersecurity of critical infrastructure, such as escalators, is paramount. Escalators, often overlooked as potential cyber-attack targets, are integral components of urban transportation systems. A cyber-attack on an escalator can lead to severe consequences, including operational disruptions, safety hazards, and public panic. This research paper explores the vulnerabilities of escalator systems to cyber-attacks and the potential impact of such breaches. By analysing threat models and reviewing past incidents, the paper highlights the importance of implementing robust cybersecurity measures. The Secure Development Lifecycle (SDL) approach ensures that security is integrated into every phase of the product development process, from first design to deployment and maintenance. This comprehensive method is crucial in finding and mitigating potential vulnerabilities before they can be exploited by malicious actors.

The paper also discusses the role of advanced technologies, such as cloud connectivity and predictive maintenance, in enhancing the security and reliability of escalator systems. Cloud connectivity allows for real-time monitoring and data analysis, enabling quick detection and response to any irregularities or potential threats. Predictive maintenance uses data analytics to foresee and address maintenance issues before they lead to system failures, thereby reducing the risk of cyber-induced malfunctions. Additionally, the research underscores the importance of continuous monitoring, employee training, and collaboration with cybersecurity experts to safeguard escalators against evolving cyber threats. Continuous monitoring ensures that any suspicious activities are detected promptly, while regular employee training keeps staff informed about the latest security practices and potential threats. Collaboration with cybersecurity experts provides access to specialized knowledge and resources, enhancing the overall security posture of escalator systems. The findings of this paper emphasize that a multi-faceted approach, combining advanced technologies, rigorous security practices, and continuous vigilance, is essential to protect escalators from cyber-attacks and ensure the safety and reliability of urban transportation systems.

2 INTRODUCTIONS

In urban mobility, escalators are essential components of daily transportation, quietly supporting the flow of millions of people in subways, airports, shopping malls, and metro stations. Often regarded as simple mechanical systems, modern escalators have evolved into complex cyber-physical infrastructures that rely heavily on digital technologies for control, monitoring, and maintenance. However, this digital transformation has also introduced new vulnerabilities, making escalator systems potential targets for cyber-attacks.

The cybersecurity of critical infrastructure has become a growing concern as more operational technologies are integrated with networked systems. Escalators, though traditionally overlooked in cybersecurity discussions, play a vital role in ensuring the smooth functioning of urban mobility. A successful cyber-attack on these systems could result in operational disruptions, safety hazards, economic losses, and widespread public panic. Malicious actors exploiting security gaps in escalator control systems could cause malfunctions, shutdowns, or even accidents, underscoring the need for proactive risk management. (Man, 2025)This paper investigates the cyber vulnerabilities of escalator systems by analysing threat models, reviewing incidents from analogous industries, and identifying gaps in current security practices. A key focus is the implementation of the Secure Development Lifecycle (SDL) a framework that embeds security considerations throughout the product design, development, and operational phases. By adopting SDL, organizations can find and mitigate vulnerabilities before they can be exploited.

Furthermore, the research explores how emerging technologies such as cloud connectivity and predictive maintenance can enhance the security and resilience of escalator systems. Cloud-based solutions enable real-time monitoring and rapid response to anomalies, while predictive maintenance uses data analytics to detect potential issues before they escalate into failures. In addition, continuous system monitoring, employee training, and collaboration with cybersecurity experts are emphasized as essential components of a robust defence strategy. As escalators become smarter and more connected, safeguarding them from cyber threats is critical to keeping public safety, service continuity, and confidence in urban infrastructure. This paper presents a comprehensive approach to securing escalator systems against evolving cyber-physical risks.

3 INDUSTRIAL CYBERSECURITY INCIDENTS

Cybersecurity failures in industries have led to devastating consequences, from monetary loss to reputational damage. The 2021 Colonial Pipeline attack demonstrated the fragility of national infrastructure; a weak VPN password and lack of multi-factor authentication enabled ransomware to shut down fuel supply, causing shortages and panic across the U.S. East Coast (Beerman, 2023). Similarly, Maersk’s 2017 NotPetya malware attack disrupted global shipping due to poor network segmentation, costing up to $300 million.

Figure 1: *Industrial Cybersecurity Incidents (AI Created)*

Retail giant Target was compromised in 2013 when attackers exploited a third-party HVAC vendor to access POS systems, affecting millions of customers and costing over $162 million (Shu, 2017). In 2012, Saudi Aramco suffered a major disruption from the Shamoon virus, which wiped data on 35,000 devices, forcing manual operations. The attack highlighted endpoint vulnerabilities and spear-phishing risks (Alsaeed, 2021).

Equifax's 2017 breach exposed sensitive data of 147 million Americans due to an unpatched software flaw, resulting in legal penalties exceeding $575 million and irreparable brand damage.

Common factors across these incidents include poor patch management, weak access controls, inadequate third-party risk oversight, and human error. These failures prove that cybersecurity is not just a technical issue, it's a business-critical imperative requiring vigilant policies, layered defences, and continual employee training.

3.1 Significance of Securing Escalator Systems

Pervasiveness in urban transport: With millions using escalators daily, any disruption cyber-induced or otherwise will quickly escalate into public safety concerns and infrastructural overload.

Cyber-physical risk: A successful cyber-intrusion could cause abrupt stops, erratic speeds, control malfunction or emergency braking - all leading to injury, panic, or crowd crushes.

Interdependence with IoT: Modern escalators often rely on remote diagnostics and cloud connectivity for operational monitoring, firmware management, and predictive maintenance. This integration is efficient—but also increases attack surfaces.

Precedent in analogous systems: Incidents like the 2021 Oldsmar water treatment hack where attackers briefly altered chemical doses via remote access highlight how OT compromise in public infrastructure yields physical danger.

Public trust & managerial transparency: Escalator failure impacts confidence in transit systems and can mirror the societal impact of large-scale attacks such as Colonial Pipeline (2021) or Ukraine's power grid disruptions.

4 CYBERSECURITY THREATS AND LIMITATIONS

4.1 Threats

Unauthorized Remote Access and Control

One of the primary cybersecurity threats to escalator systems is the risk of unauthorized access to control systems, particularly when remote monitoring or diagnostics are in place. Escalator manufacturers and service providers offer remote access capabilities to check system health and receive real-time alerts. If this remote access is not properly secured through multi-factor authentication (MFA), strong passwords, and encrypted communication, attackers could gain control over the escalator's operation. Malicious actors could issue commands to stop, reverse, or accelerate the escalator in ways that the system was never designed to manage. Such actions could result in passenger falls, injuries, panic situations, or complete operational shutdowns. Beyond physical harm, the organization responsible could face lawsuits, regulatory penalties, and brand reputation damage. (Ahsan, 2022)

Malware and Ransomware Attacks

Escalator systems, especially those connected to larger smart building platforms, may be vulnerable to malware or ransomware infections. These attacks can enter through infected devices (such as laptops used by maintenance teams), unprotected USB ports, or even via vulnerable software updates. A ransomware attack could lock down the escalator control software, making it inoperable until a ransom is paid. In the case of a large public venue such as a shopping mall, airport, or metro station, this could lead to significant public safety risks, crowding, and logistical nightmares. In addition to the potential for injury, the cost of system recovery, downtime, and ransom payments could be large. (Abdelgawad, 2021)

Denial of Service (DoS) Attacks

Escalator systems that are network-connected can also be targeted by Denial of Service (DoS) attacks, where cybercriminals flood the system or its connected servers with excessive traffic, causing them to slow down or crash. Though escalators might seem like unlikely targets, attackers could use a DoS attack as part of broader disruption efforts such as during protests, political events, or coordinated attacks on public infrastructure. The result could be escalator outages in high-traffic areas, leading to inconvenience, possible safety issues (such as crowding on emergency stairways), and damage to public confidence in facility safety. (Shen Y, 2017)

Sensor Spoofing or Manipulation

Modern escalators rely on various sensors such as load sensors, motion detectors, and safety triggers to run safely and efficiently. If an attacker gains access to the system's communication layer, they could alter or spoof sensor data. For example, false readings could make the escalator ignore overload conditions or do not stop when obstructions are detected. This could directly result in passenger injuries, mechanical damage, or emergency shutdowns. Sensor manipulation may also remain undetected until a real accident occurs, making it a subtle but highly dangerous form of cyberattack. (Yasser Shoukry, 2015)

Physical Interface Tampering (Insider or External Threats)

Escalator systems have physical diagnostic ports or programmable logic controllers (PLCs) used by maintenance teams to update software, change settings, or troubleshoot issues. If these physical access points are left unsecured or if service laptops/devices are compromised, attackers (including insiders) could physically reprogram the escalator. Potential consequences could include unexpected speed changes, failure of safety interlocks, or even mechanical stress leading to long-term wear and tear or sudden breakdowns. Tampering could be difficult to detect if adequate audit logging and change management controls are not in place.

Supply Chain Attacks

A less visible but equally dangerous cybersecurity threat comes from the supply chain. If the software or hardware components used in the escalator system are compromised before installation through malicious firmware, counterfeit components, or vulnerabilities in third-party software an attacker could embed malicious code that activates after deployment. This type of attack could lead to mass deployment of vulnerable escalators across multiple sites, making it possible for attackers to launch coordinated, simultaneous disruptions or failures. Such attacks could have nationwide consequences if affecting transportation hubs, commercial centres, or critical infrastructure. (Beerman, 2023)

Data Breaches and Privacy Risks

Escalators in smart buildings are now part of integrated platforms that collect and send usage statistics, maintenance logs, and sometimes video or occupancy data. If this information is not properly secured, attackers could breach these systems and exfiltrate sensitive data. This could expose patterns of building occupancy, maintenance schedules, or even personal information of staff or contractors, leading to privacy violations and regulatory penalties under data protection laws such as GDPR or local cybersecurity regulations. While the escalator itself may not directly store personal data, its integration into a larger system creates new risks.

4.2 Limitations

Legacy Mechanical Design

Most existing escalator systems were originally designed as purely mechanical and electrical devices, with no consideration for digital security. Their control systems often run on outdated software, minimal computing power, and proprietary hardware

that cannot easily support modern cybersecurity features such as encryption or authentication layers. Retrofitting old systems to meet today's cybersecurity standards can be technically difficult and prohibitively expensive, often requiring complete system overhauls. This leaves older escalators vulnerable to cyber threats with no easy solution.

Lack of Cybersecurity Awareness and Skills

The escalator industry primarily consists of mechanical engineers, electrical engineers, and maintenance personnel who traditionally focus on physical safety and mechanical reliability. Cybersecurity is not yet a core part of their training or professional culture. As a result, there is often limited understanding of how cyber risks can affect the safety and functionality of escalators. This human factor lack of awareness can lead to poor configuration of security settings, weak password management, and failure to find potential cyber risks during installation or maintenance.

Cost Constraints

Implementing robust cybersecurity measures comes with added costs both in first investment and ongoing maintenance. This includes costs for secure remote monitoring systems, software updates, security audits, staff training, and incident response planning. In industries where budgets are tight or where escalators are viewed as low-priority infrastructure, there is often resistance to spending extra on cybersecurity. Decision-makers may underestimate the risks, choosing short-term savings over long-term security, until an incident forces them to act reactively.

Integration Challenges with Legacy Systems:

Even when cybersecurity is considered, escalators are often integrated into larger building systems such as Building Management Systems (BMS), fire alarms, or centralized SCADA systems that may themselves be running on outdated or insecure platforms. The challenge lies in ensuring compatibility between new security features and older networked systems without causing operational disruptions. In more cases, patching or upgrading these larger systems requires complex planning and can lead to temporary service interruptions that building managers are reluctant to authorize.

Absence of Industry-Specific Cybersecurity Standards:

Unlike critical infrastructure sectors such as energy, aviation, or finance, the escalator and vertical transportation industry lacks standardized cybersecurity regulations or guidelines. While general cybersecurity frameworks (such as ISO/IEC 27001 or NIST) exist, there are no tailored standards that directly address the unique risks and requirements of escalators. This results in inconsistent practices across manufacturers, service providers, and building operators, leaving systems inadequately protected. Without regulatory pressure or clear standards, cybersecurity often stays an afterthought rather than a design priority.

5 RISK MITIGATION

5.1 Secure Development Lifecycle (SDL)

The primary recommendation of this guideline is to implement a robust Secure Development Lifecycle (SDL). This lifecycle needs the manufacturer's dedication to providing adequate training, tools, resources, and processes to fortify and sustain escalators against cyber threats. It aligns with best practices across cybersecurity standards and methodologies (NEII, 2019). Figure 2. Shows the architecture of Cybersecurity process life cycle.

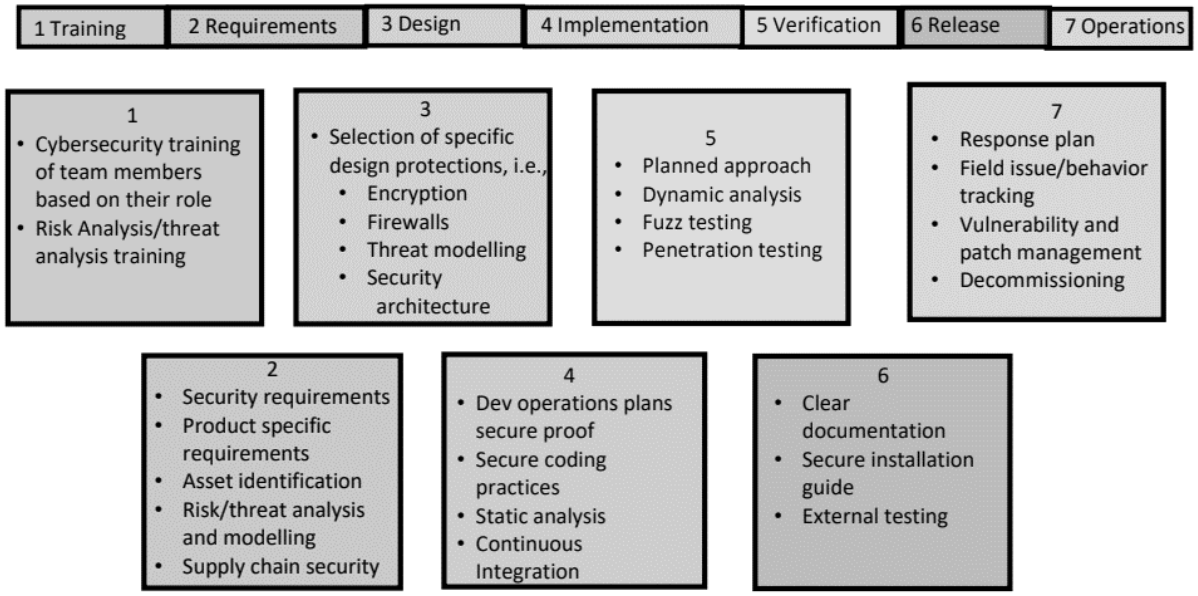


Figure 2: *Architecture of Cybersecurity process life cycle* (NEII, 2019)

Training-

Individual involved in the cybersecurity lifecycle need tailored training for their roles to ensure the security of escalators, incorporating general knowledge and role-specific ability.

Requirements-

Escalator cybersecurity management involves risk management, setting up measures and controls, asset identification, and risk assessment. Regular updates consider adversary capabilities and vulnerabilities, while prioritizing passenger safety. Requirements are categorized into baseline and system-specific for effective risk assessment and management.

Design-

The design phase aims to develop system architecture, making key design decisions and outlining product functionality. It’s prone to security vulnerabilities; early detection is crucial. Use best practices like least privilege, attack surface minimization, modular design, defines in depth, restricted access, proven components, and regular security reviews.

Secure Implementation-

Use secure coding guidelines, static analysis for high-risk code, and continuous analysis throughout development to find and mitigate security issues, ensuring robust protection against vulnerabilities.

Verification-

Implement a formalized cybersecurity verification process including dynamic analysis, fuzz and penetration testing, and third-party analysis to find and address security vulnerabilities effectively and ensure robust protection.

Release Documentation-

Comprehensive documentation before release includes threat modelling, security requirements, test reports, user manuals, and secure installation guides to ensure all security aspects are properly addressed and communicated.

Operations-

Track hardware/software inventory, check vulnerabilities, and address risks. Use a scoring system for prioritization and conduct engineering tests to ensure security levels and compliance with standards.

5.2 Industry standards compliance

When addressing cybersecurity threats related to escalators, it is essential to reference specific industry standards to ensure comprehensive protection. The relevant standards include ISO 8102-20:2022, which provides guidelines for cybersecurity in building automation systems; IEC 62443-3-3:2013, outlining system security requirements for industrial automation; and IEC 62443-4-2:2019, detailing technical security requirements for individual components. These standards collectively form a robust framework to effectively manage and mitigate potential cybersecurity risks within escalator systems, ensuring the safety and integrity of these critical infrastructures. These standards help organizations keep high security levels and protect against cyber threats. (F. Djebbar, 2023)

5.3 Advanced Technologies for Cybersecurity of Escalator Systems

5.3.1 Cloud Connectivity

Modern escalators are now equipped with Internet of Things (IoT) devices that send real-time operational data to cloud platforms (Ahmad, 2022). This cloud connectivity offers various cybersecurity benefits.

Centralised Monitoring: Escalator performance and security data can be collected and analysed centrally, allowing cybersecurity teams to detect anomalies or breaches across multiple locations.

Automated Software Updates: Cloud-connected escalator systems can receive regular security patches and firmware updates, reducing the risk of cyber-attacks that exploit outdated software.

Data Encryption & Access Control: Cloud platforms enable stronger encryption protocols and access management to protect sensitive data against interception or unauthorized access.

However, cloud connectivity also introduces risks such as data breaches, denial of service (DoS) attacks, and supply chain vulnerabilities, which must be mitigated using network segmentation, multi-factor authentication (MFA), and robust encryption.

5.3.2 Predictive Maintenance

Predictive maintenance (PM) involves using sensor data, historical maintenance records, and machine learning algorithms to predict equipment failures before they occur. In the context of cybersecurity, predictive maintenance offers the following advantage.

Anomaly Detection: Sudden irregularities in equipment behaviour such as abnormal vibration, speed, or power consumption can be early indicators of cyber tampering or malware.

Minimized Downtime from Cyber Incidents: By finding both mechanical and cyber-related issues early, predictive maintenance helps avoid sudden shutdowns that could be exploited by attackers.

Behavioural Baseline Monitoring: By continuously learning the “normal” behaviour of escalators, PM systems can detect deviations that may signal unauthorized software manipulation or cyber intrusions.

Predictive maintenance can also help ensure that security-critical components, such as safety brakes or emergency stop systems, are functioning correctly and have not been compromised. (M. Patel, 2023)

5.3.3 Digital Twins

A Digital Twin is a real-time virtual replica of a physical system that can simulate, check, and predict the performance of an escalator (Liu, 2023). In cybersecurity, digital twins play a crucial role:

Cyber-Physical Simulation: Digital twins allow for simulation of cyber-attacks on escalator systems in a safe, virtual environment. This helps security teams test defences without risking real-world operations.

Incident Response Planning: Operators can use digital twins to model different attack scenarios such as ransomware, system hijacking, or unauthorized access and develop optimized response strategies.

Real-Time Monitoring & Diagnostics: Any cyber-induced anomaly in the physical escalator is instantly reflected in the digital twin, enabling quick diagnosis and isolation of the problem. Digital twins can also support regulatory compliance by providing detailed logs and security audits for authorities.

5.3.4 AI-Based Monitoring

Artificial Intelligence (AI) and Machine Learning (ML) algorithms are transforming the way escalator systems are checked for cybersecurity threats (Ahsan, 2022). AI-based monitoring offers:

Threat Detection and Prediction: AI systems can analyse vast amounts of sensor and network data to find patterns indicative of cyber-attacks, including zero-day threats that traditional systems may miss.

Automated Response: If a detected cyber intrusion, AI algorithms can trigger automated safety measures such as halting escalator operation, isolating network segments, or alerting security teams.

Behavioural Analytics: AI can continuously learn from user behaviour and system performance, detecting subtle anomalies that could show insider threats or advanced persistent attacks (APTs).

Integration with Physical Safety: AI-driven cybersecurity is integrated with physical safety protocols. For example, if AI detects a cyber-attack aimed at disabling emergency brakes, the system can override digital commands and activate physical safety locks.

By using AI, escalator systems not only become more resilient to known threats but also better prepared for emerging, sophisticated cyber-attacks.

6 CONCLUSION

The cybersecurity of escalators within urban transportation systems is of paramount importance, given the severe consequences that cyber-attacks can pose. The potential for operational disruptions, safety hazards, and public panic needs a robust and comprehensive approach to securing these critical infrastructures.

The Secure Development Lifecycle (SDL) appears as a pivotal strategy, ensuring that security considerations are woven into every stage of the product development process. By finding and addressing vulnerabilities from the outset, SDL significantly reduces the risk of exploitation by malicious actors.

Advanced technologies such as cloud connectivity and predictive maintenance play crucial roles in bolstering escalator security. Cloud connectivity eases real-time monitoring and data analysis, enabling swift detection and response to anomalies or threats. Predictive maintenance, through data analytics, expects maintenance issues before they escalate into failures, thus mitigating the risk of cyber-induced malfunctions and ensuring operational continuity.

Continuous monitoring, employee training, and collaboration with cybersecurity experts are equally vital components of a robust security framework. Continuous monitoring ensures the prompt detection of suspicious activities, while regular training keeps employees abreast of the latest security practices and threats. Collaboration with experts provides access to specialized knowledge and resources, enhancing the security posture of escalator systems.

The research underscores the necessity of a multi-faceted approach, combining SDL, advanced technologies, and a culture of continuous vigilance. Such a holistic strategy not only safeguards against existing threats but also prepares escalator systems to adapt to future cybersecurity challenges.

By embracing these measures, organizations can protect escalator systems from cyber-attacks, ensuring the safety and reliability of urban transportation. This initiative-taking stance not only preserves public confidence but also contributes to the resilience and sustainability of critical urban infrastructure in an increasingly digital world.

Disclaimer: This paper presentation is by the authors and is intended for educational purposes without constituting any professional judgment. Statements of facts and opinions provided are those of the participants individually and do not purport to reflect the opinion or statements by the Company. The Company neither approves nor assumes responsibility for the content, accuracy, or completeness of the information provided in the paper presentation.

7 REFERENCES

Abdelgawad, M. (2021). Securing Hardware from Malicious Attacks., (p. 4).

Ahmad, W. (2022). Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey. *Electronics, 11*, 16.

Ahsan, M. (2022). Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning. *Journal of Cybersecurity and Privacy*.

Alsaeed, A. (2021). The Cyber Attack on Saudi Aramco in 2012. *Asian Journal of Engineering and Applied Technology*, 25-28.

Beerman, J. (2023). A Review of Colonial Pipeline Ransomware Attack. *IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops* .

F. Djebbar, K. N. (2023). A Comparative Analysis of Industrial Cybersecurity Standards. *IEEE, 11*, 85315-85332.

Jiao, Z. (2022). *Potential escalator-related injury identification and prevention based on multi-module integrated system for public health.* Hong Kong: Beihang University.

Liu, Z. (2023). The Digital Twin Modeling Method of the National Sliding Center for Intelligent Security. *Sustainability, 15(9)*, 7409.

M. Patel, J. V. (2023). Predictive Maintenance: A Comprehensive Analysis and Future Outlook. *International Conference on Futuristic Technologies (INCOFT)*, 1-7.

Man, P. K. (2025). Reliability and safety of elevators and escalators/ travelators: Past, present and future. *Results in Engineering, Volume 25*.

NEII. (2019). Elevator and Escalator Industry Cybersecurity Best Practices. *National Elevator Industry, Inc.* Retrieved from https://nationalelevatorindustry.org/wp-content/uploads/2024/07/NEII-Cybersecurity-Best-Practices-rev2-July-2024

Sándor, B. (2022). *Cyber Security Analysis of Smart Buildings from a Cyber Security Architecture Point of View.* Interdisciplinary Description of Complex Systems.

Shen Y, F. M. (2017). Cyber security study for power systems under denial of service attacks. *Transactions of the Institute of Measurement and Control., 41(6)*, 1600-1614.

Shu, X. (2017). Breaking the Target: An Analysis of Target Data Breach and Lessons Learned.

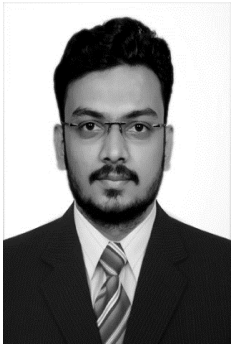
Vallabhaneni, R. (2024). Protecting the Cybersecurity Network Using Lotus Effect Optimization Algorithm Based SDL Model. *International Conference on Distributed Computing and Optimization Techniques (ICDCOT)* (pp. 1-7). Bengaluru, India: IEEE.

Wakchaure, M. (2016). Reconnaissance of Industrial Control System by deep packet inspection. *IEEE International Conference on Engineering and Technology (ICETECH).* Coimbatore, India: IEEE.

Yasser Shoukry, P. M. (2015). PyCRA: Physical Challenge-Response Authentication For Active Sensors Under Spoofing Attacks. *Computer and Communications Security*, (pp. 1004-1015).

8 BIOGRAPHICAL DETAILS

Mr. Mahesh Wakchaure holds a Master of Technology degree in Electrical (Control System) from VJTI Mumbai. He has professional experience as Design and development engineer at Tox Pressotechnik India Pvt Ltd. and is currently Assistant manager- Electrical R&D at Schindler India's Escalator Division



Mr. Shubham Jambhe is an R&D Design Engineer at Schindler India with over 7 years of experience in mechanical design engineering. Specializing in escalator system modernization and adaptation. He holds a Bachelor of Technology in Mechanical Engineering from Babasaheb Ambedkar Marathwada University, Aurangabad, and is currently pursuing a Master’s Degree in Mechanical and Materials Engineering from Savitribai Phule Pune University (SPPU), Pune. Passionate about innovation in urban transportation.