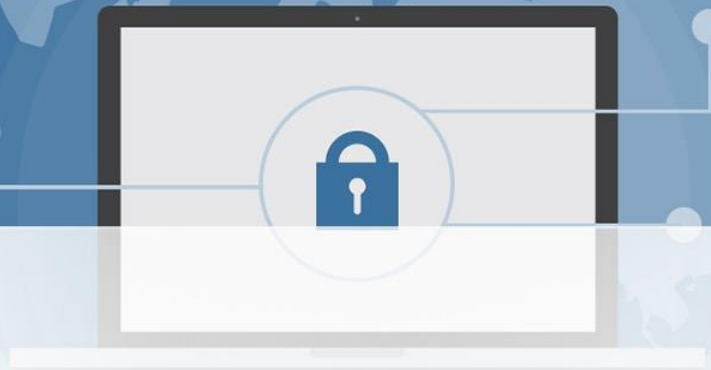
Tauheed Waheed

The Impact of IoT Cybersecurity in Industry 4.0

Introduction



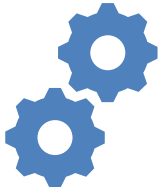
IoT (Internet of Things) and Industry 4.0 are continuously providing opportunities and challenges in various domains

Especially for better and more productive autonomous systems.

The growth of their hardware and software complexity is opening more critical security and privacy threats.

Related Work

The violations that may raise serious consequences for financial loss and society's trustworthiness (Corallo and Lazoi, 2020)

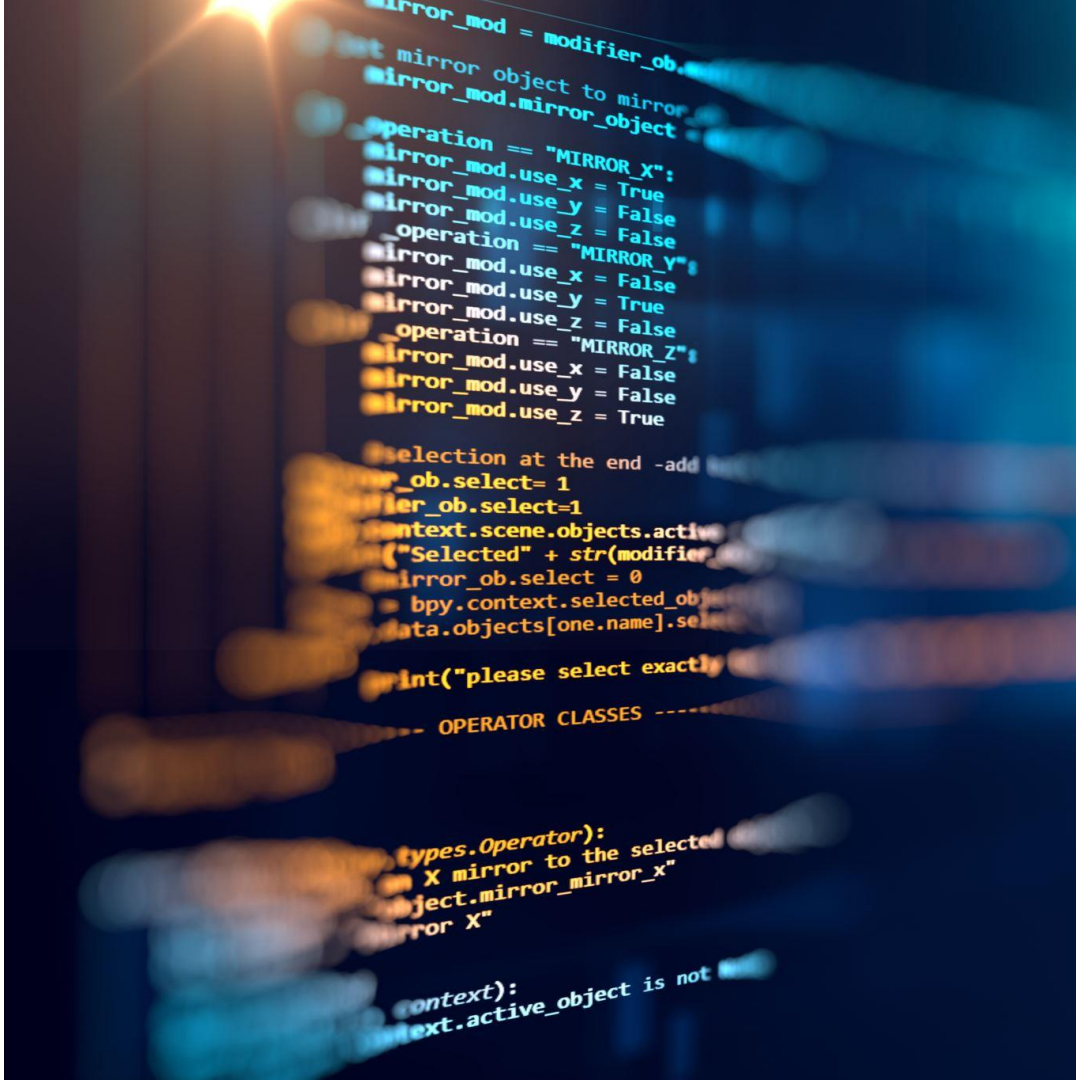


The guidelines, methodologies and specific tool for integrating Cybersecurity into the entire life cycle of software development.

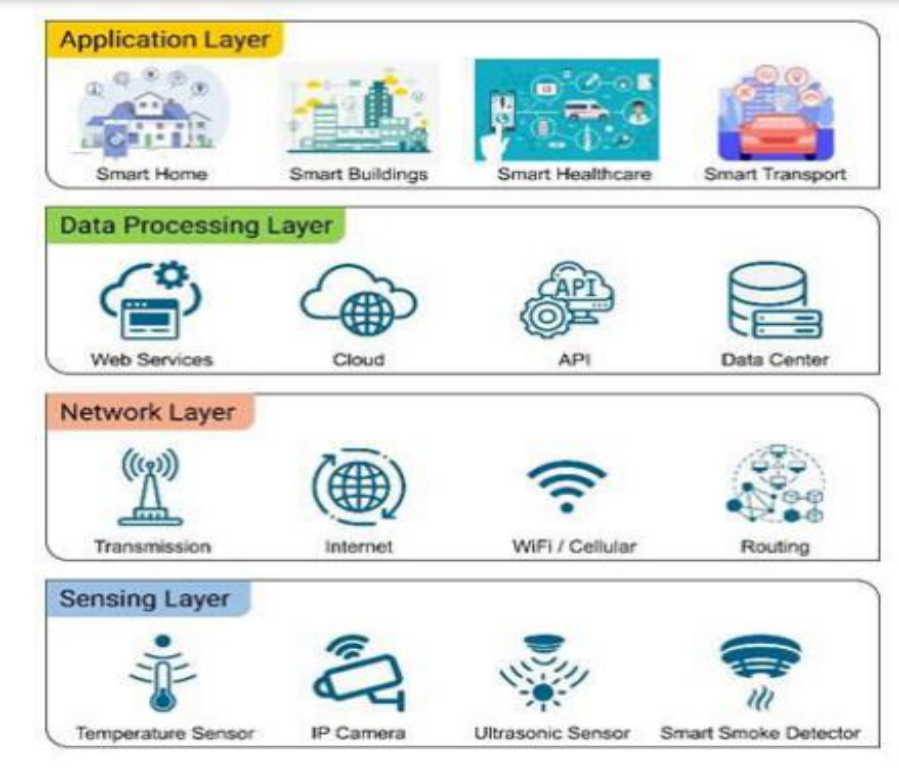
It has been the focus of the last year's research activity (Tahaei and Vaniea, 2022)

Cybersecurity Challenges

- Privacy and Data theft
- Security for IoT systems
- Preventive Testing



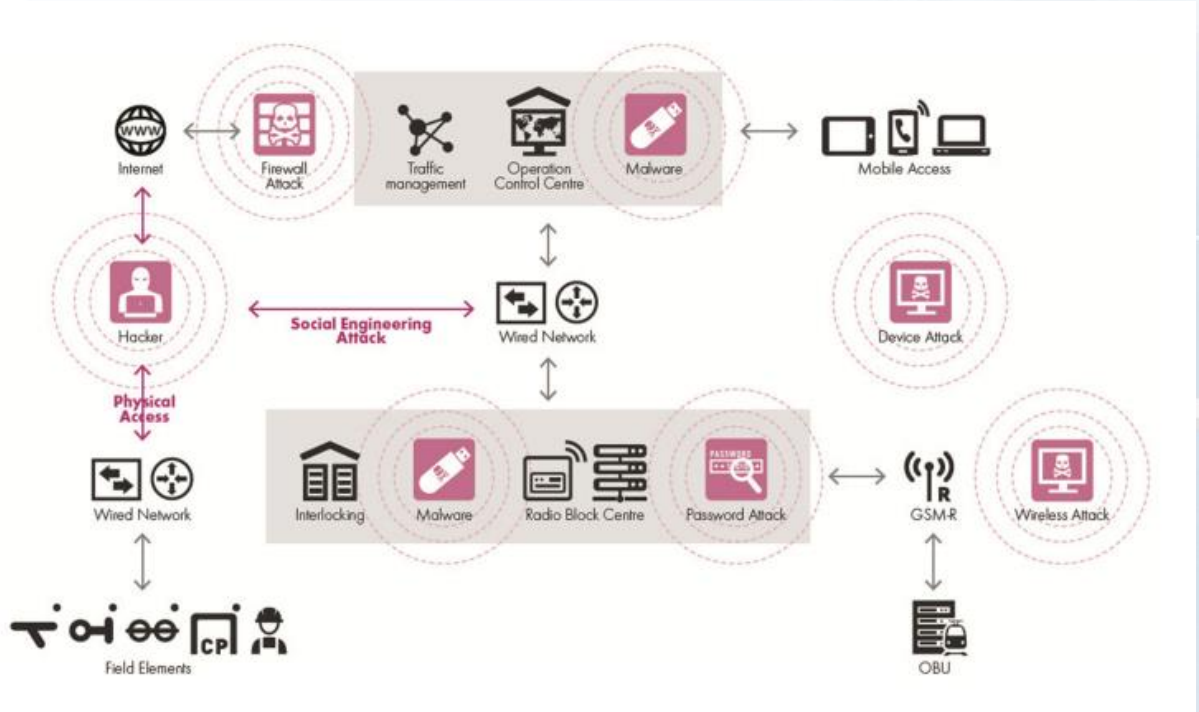
Layered Architecture of IoT



Industry 5.0

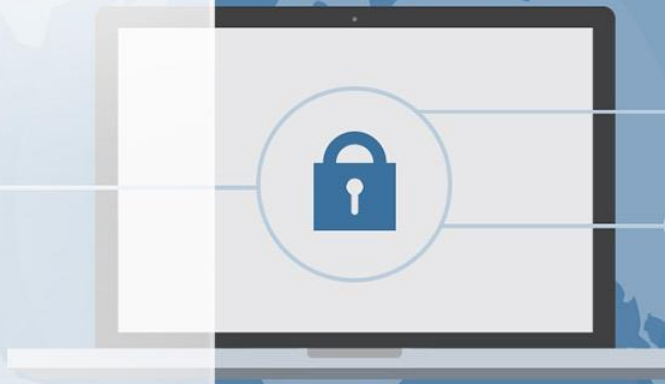
- The revolution of industry 5.0 defines that humans and machines must collaborate.
- The productivity of manufacturing industry will boost by universal robots and human workers (Garg and Jain, 2021).
- It is evident that Industry 5.0 is changing paradigm.

Transformation from Industry 4.0 to Industry 5.0



Present Solutions

- Quality 4.0 and Quality 5.0
- Automotive Cybersecurity Testing
- Penetration Testing
- Human-Centric Cybersecurity

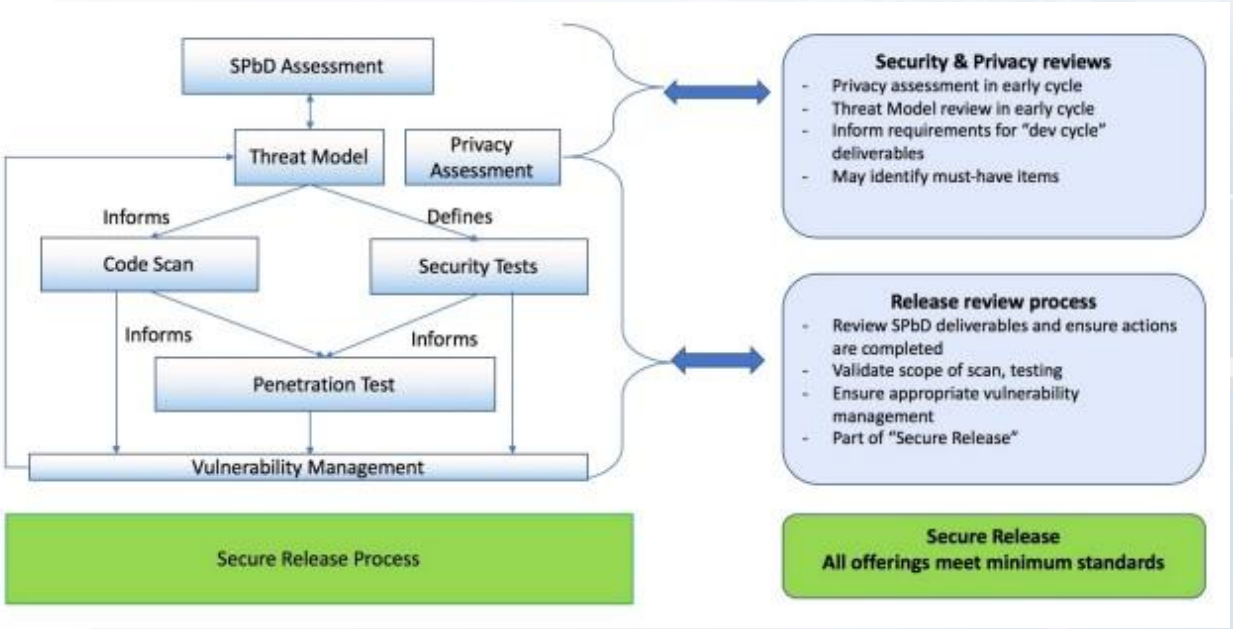


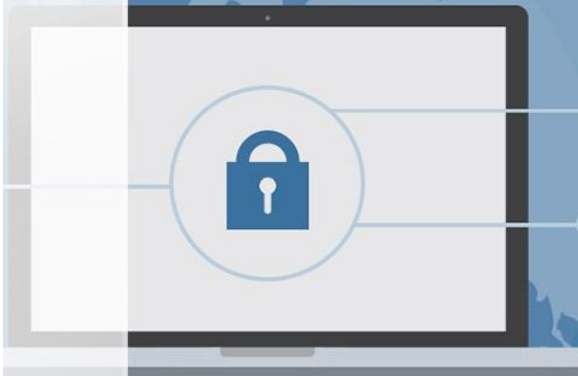
Security and Privacy by design

- The purpose of the Threat Model is to basically identify, communicate, mitigate and comprehend threats.

- The security tests are a vital component of the overall testing cycle and are intended to ensure that the overall development process results in secure code.

Security and Privacy by design





Security and Privacy by design

- Security testing helps to validate that the information system under test protects functions and data as intended.

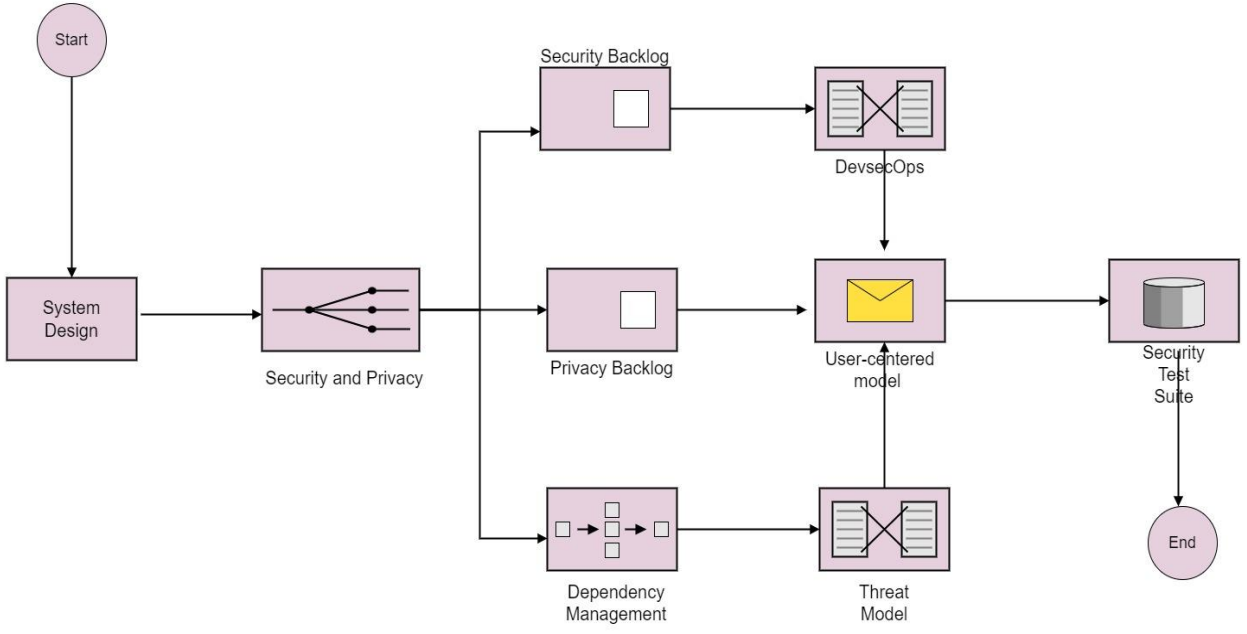
- The penetration is an authorized simulated attack on a system or application.

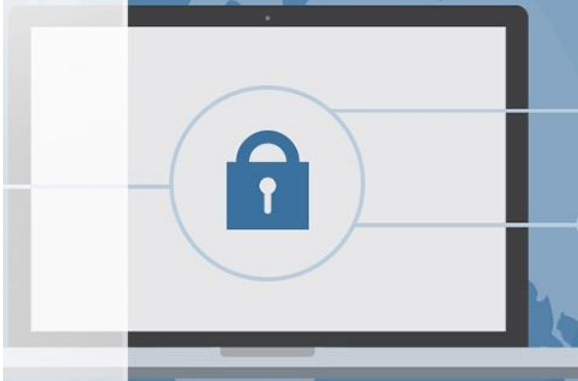
Security and Privacy by design

- The pen testers pretend as hackers to conduct cyber-attacks on the system under test.

- It usually involves automated tools and must involve a spirit of ethical hacking.

Proposed Framework





Proposed Framework

- The User-Centric testing model prioritizes users at every step of the testing process and focuses on their requirements and overall working of the system.

- Consumers or Users are not aware of specific functions that are designed and developed to ensure their security.

Proposed Framework

- The user-centric testing is promoted to make sure that their products are used in a safe and secure way, while their users are aware of different functions.

- Mostly, this User-Centric testing approach is implemented by continuous evaluation of user needs and behavior.

Questions and Future Directions