iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** I **Month of publication:** January 2024

DOI: https://doi.org/10.22214/ijraset.2024.57793

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue I Jan 2024- Available at www.ijraset.com

Cyber Security Challenges and Solutions

Kunal Pradeep Puri
Information Technology, Sinhgad Colleage of Engineering,Pune

Abstract: ***This article discusses the challenges and opportunities in the field of Cyber Physical Systems (CPSs). It highlights the integration of the physical and digital realms in CPSs and the increasing importance of security in this context. The article provides an overview of the challenges faced by CPSs and suggests potential solutions to address them. It emphasizes the need for preventive measures, coordination, lightweight solutions, and early-stage verification to enhance the security and effectiveness of CPSs.***

Keywords: Cyber Physical Systems, security, effectiveness

I. INTRODUCTION

Cyber Physical Systems (CPSs) are becoming more prevalent in our modern world, enabling smart living through the integration of the physical and digital realms. However, this integration poses several challenges, particularly in terms of security, privacy, and system vulnerabilities. The article explores these challenges and discusses potential solutions to overcome them. It emphasizes the importance of considering both the cyber and physical aspects of security in CPS design.

.

II. CHALLENGES

1) *Lack of Security by Design:* Many CPSs were not initially designed with security in mind, as they were not connected to external networks. This poses a challenge in ensuring the security of CPSs, as physical security measures alone are insufficient. The article suggests a shift in mindset to consider both the cyber and physical aspects of security in CPS design.
2) *Vulnerability of Industrial Control Systems (ICS) and Smart Grids:* ICSs often consist of old components that are difficult to replace with newer, more secure ones. Short-term solutions are needed to address potential problems in ICSs. Smart grids face challenges in change management and comprehensive security. Change management is crucial to handle the complexity of smart grids, while comprehensive security measures need to be implemented at all levels.
3) *Security versus Usability in Medical Devices:* Striking the right balance between security and usability is crucial in medical devices. Excessive security measures may hinder critical interventions in emergency situations. Solutions need to be developed to ensure that medical devices are both secure and accessible when needed.

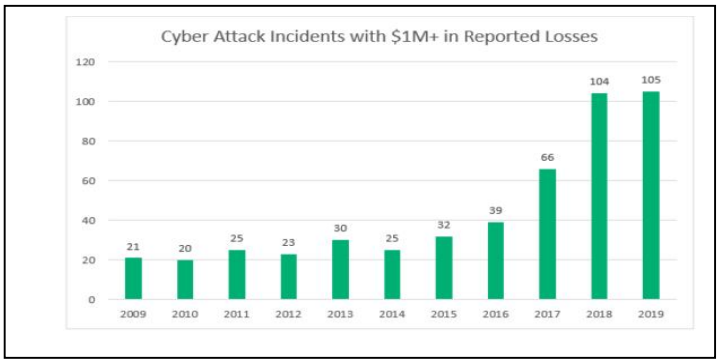


Fig. 1. Cyber Attack Incidents with $1M above in reported loses.
(Source: 42 Cyber Attack Statistics by Year: A Look at the Last Decade - InfoSec Insights (sectigostore.com))

III. SOLUTIONS

1) *Prevention:* The article emphasizes the importance of preventive measures in dealing with attacks on CPSs. Efforts should be focused on preventing attacks rather than waiting for them to happen. This can be achieved through robust security measures and safety plans.
2) *Coordination and Tracking of Security-related Changes:* To mitigate the risk of malicious insiders, coordination and tracking of security-related changes in ICS systems are essential. This ensures that any changes are properly authorized and monitored.

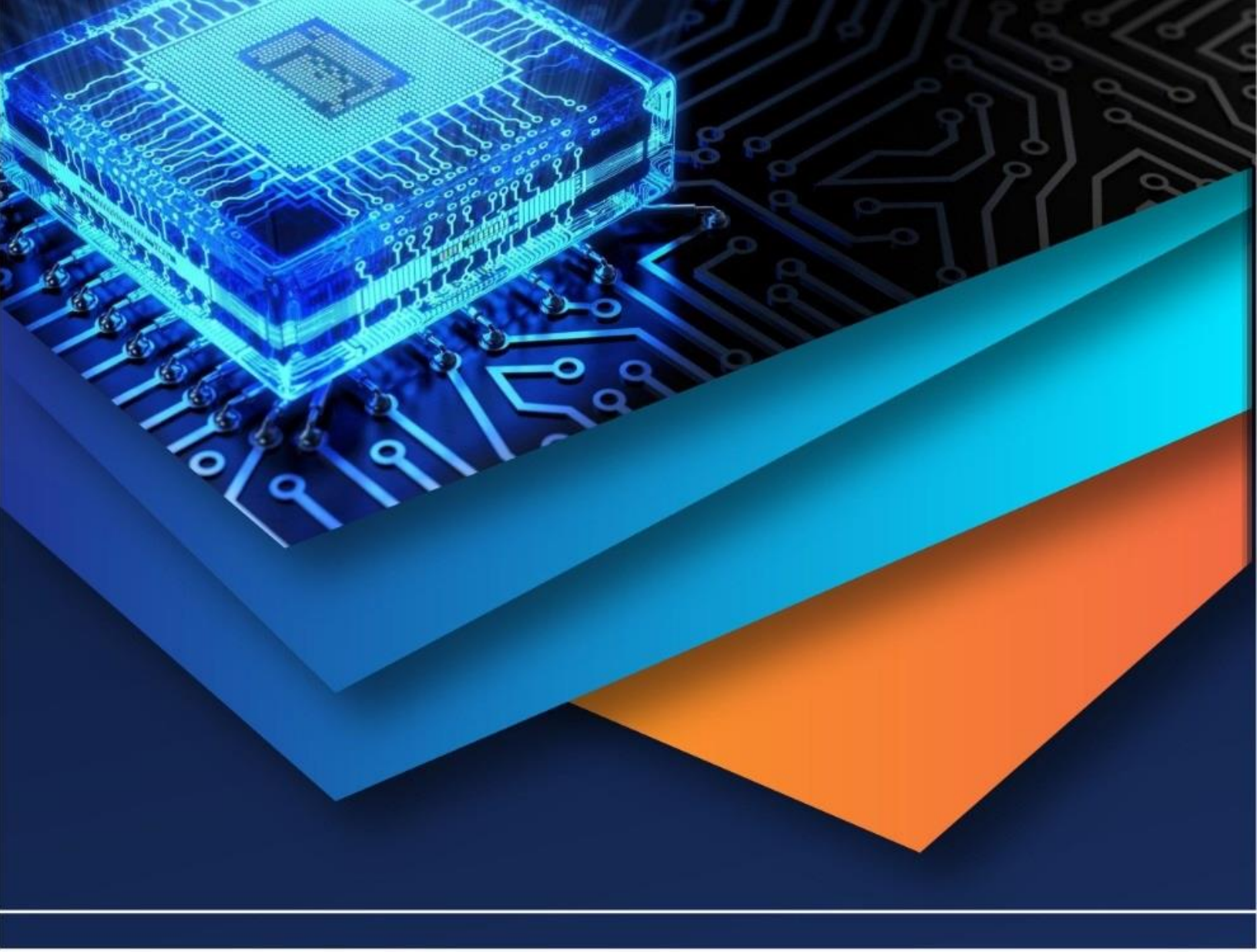
3) *Lightweight Solutions and Encryption Techniques:* Smart grids can benefit from lightweight solutions and encryption techniques to enhance security. These measures can help protect against cyber-attacks and ensure the integrity and confidentiality of data.
4) *Early-stage Verification:* The article highlights the importance of integrating verification, validation, and certification processes into the design phase of CPSs. Model-based generative techniques can enable early-stage verification, enhancing the guarantees provided by the verification process

IV. CONCLUSION

CPSs present various challenges related to security, change management, and usability. However, there are opportunities to overcome these challenges through preventive measures, coordination, lightweight solutions, and early-stage verification. Future research and advancements in CPS applications can further enhance the security and effectiveness of these systems.

REFERENCES

[1] Amit Kumar Tyagi and N. Sreenath, "Cyber Physical System:Analyses,challenges and possiblesolutions,"in:www.keaipublishing.com/en/journals,doi:https//doi.org/10.1016/j.iotcps.2021.12.002
[2] Yi Tang,Ming Ni and Xiang Yun Fu "Challenges and Evolution of Cyber Attacks in Cyber Attacks in Cyber Physical Power System,"in:IEEE PES Asia-Pacific Power and Energy Conference-Xi'an -China 2016,doi:978-1-5090-5417-6/16/$31.00
[3] Richard A. Kemmerer-Department of Computer Science,University of California Santa Barbara, "Cybersecurity,"in: 25th International Conference on Software Engineering(ICSE'03), doi:0270;5257/03



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY