STEI-ITB FTI-UNAND

IEEE INDONESIA SECTION

ICITSI 2020

INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGY SYSTEMS AND INNOVATION

Bandung | **October 19 – 22, 2020** | Padang

100 TAHUN ITB

IEEE Advancing Technology for Humanity

Digital Security Reference Model

Suhardi (suhardi@stei.itb.ac.id)

Professor

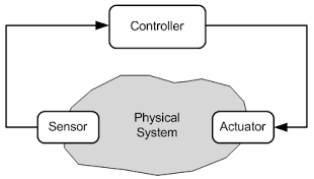
School of Electrical Engineering and Informatics

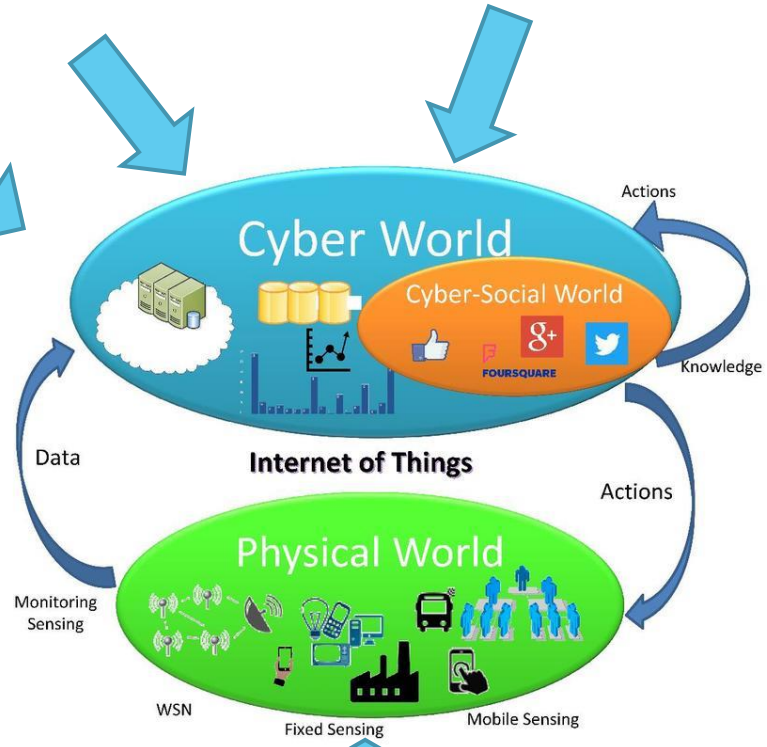
Institut Teknologi Bandung

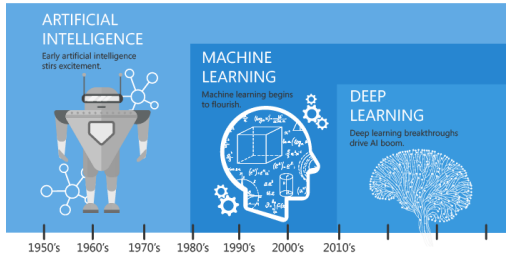
Suhardi; Aziz, Baharudin; Doss, Robin; Yustianto, Purnomo.; Digital Security Reference Model: A Survey and Proposal, accepted to ICITSI 2020

Outline

Introduction (1) :
Digital Transformation Toward IR 4.0







IR 4.0

Growing Digital Society, Increasing Digital Attacks & Cybercrime

Opportunities & Challenges for Building Digital Security

Introduction (2)

- This transformation to a digital system has also been accelerated by the Covid-19 pandemic.
- This increase in online activities has caused the need for a qualified technology to deliver a higher quality and secured service.
- The number of cyber crime case is increasing each years and COVID-19 can already be classified as the largest-ever cybersecurity threat.

Related Work

- Some works pertinent this targeted model is existing, but no comprehensive approaches can be found.
- The existing proposed model only include one or two of the three elements.

Technology and Engineering	Managerial	Legal
[16] overviews the international standards which include cryptographic mechanisms, evaluation and testing of products and information systems, countermeasures, and security services; [17] formal overview of standards and patents for IoT for Industry 4.0; [18] provide the foundations for designing a secure and interoperable toolkit for cross-border health data exchange within the European Union (EU).	[19] demonstrates how organizations and regulations are shaped which define today's IT security recommendations and norms, which describes the standards, the parallel application of which can accomplish the complex security of controlled areas; [20] proposed a method of strengthening the small- and medium-sized enterprises (SMEs)' security capability, especially focusing on a framework to be used when applying big data; [9] develop guidance to help CBRN security managers, IT/cybersecurity managers, and other decision-makers deal with threats through the application of cost-effective information security programs	[21] explains the scope and core areas of cyber security from a legal perspective, [22] examines the adequacy of the legal and regulatory frameworks in existence to curtail cybercrime [18] examine the role of the digital forensic expert, because even cyberspatial threats increased, the roles of expert evidence and the expert witness are not as widely known as it needs to be; [24] provides a comparative overview and evaluation of various legal frameworks for electronic communications security [26] provides a novel contribution for normative modelling of state cybersecurity governance under international law

Suhardi, et. al., Digital Security Reference Model: A Survey and Proposal, accepted to ICITSI 2020

The Cyber Security Body of Knowledge

5 Categories, 19 Knowledge Areas

Human, Organisasional, Regulatory	Attack and Defense	System Security	Software Platform Security	Infrastructure Security
• Risk Management and Governance • Law and Regulatory • Human Factors • Privacy and Online Rights	• Malware and Attack Technologies • Adversarial Behaviour • Security Operations and Incident Management • Forensics	• Cryptography • Operating System and Virtualisation • Distributed System Security • Authentication, Authorization, and Accountability (AAA)	• Software Security • Web & Mobile Security • Secure Software Lifecycle	• Network Security • Hardware Security • Cyber-Physical System Security • Physical Layer Security and Telecommunications

Proposed Model

The reference model proposed in this paper consists of three layers:

- technology and engineering layer;
- managerial layer; and
- legal layer.

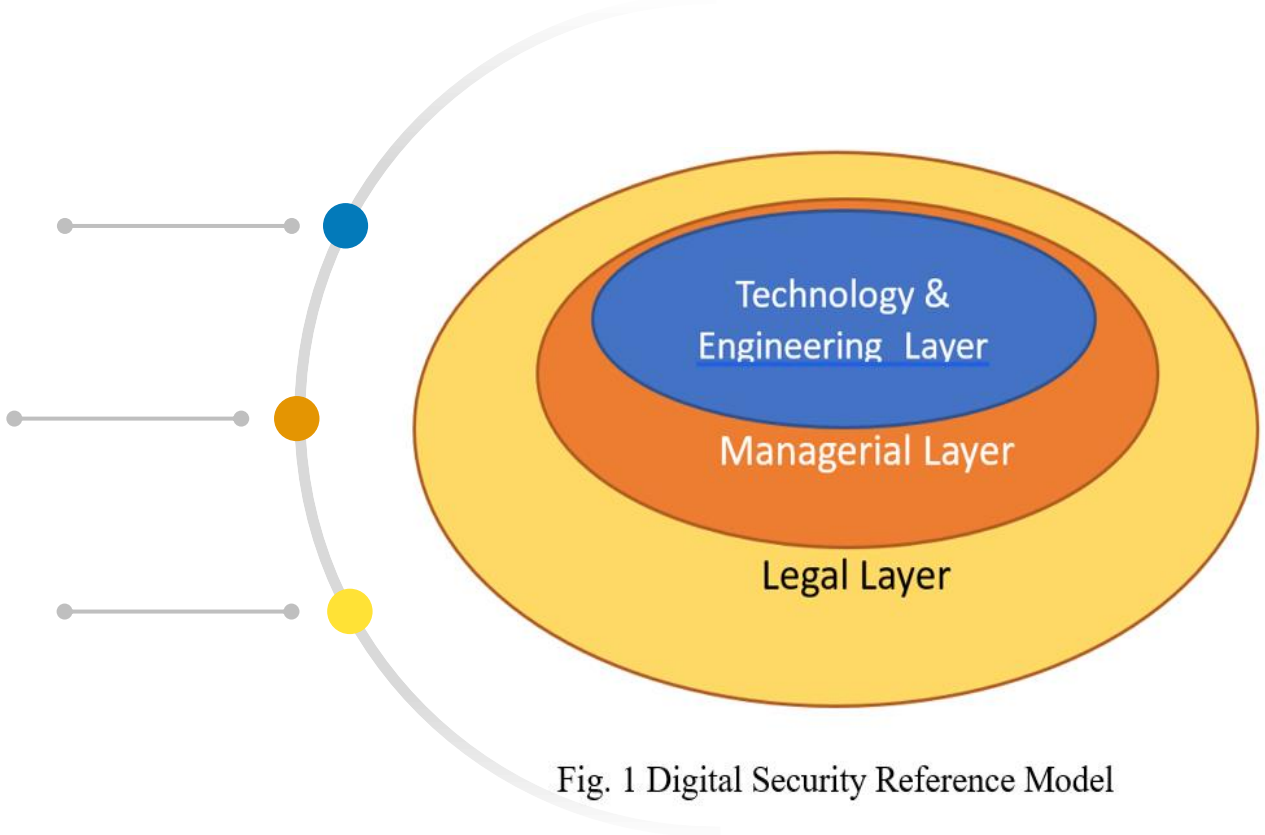


Fig. 1 Digital Security Reference Model

Technology and Engineering Layer

Authentication this technology is applied to ensure the identity of a user who is the party that has authority over the system.

Access control is the selective restriction of access to a system, while access management gives the process. Some technology that included in these aspects are: firewall, IDPS.

Cryptography is essential to the data stored on the server or transmitted as encrypted so that the adversary cannot decrypt the encrypted data without having the secret key.

Anti-malware: will protect the system from various types of malware.

System Security : protection from the adversary or damage to hardware, software, or electronic data

- Hardware, Software, Protokol

Managerial Layer

- **Awareness**: several awareness programs are needed to educate users or employees in the organization about various potential threats.
- **Information security**: this will manage the processes, tools, and policies.
- **Operational security**: a process that classifies information assets, then determines the controls needed to protect them.
- **Network security**: comprehensive security policies and provisions adopted adaptively and proactively by network administrators.

Legal Layer

- Privacy and Online Rights
- Legal and laws are needed to be enforced to several private or public sectors that are the target of the highest cyber incident [3], such as:
  1. government,
  2. public services (e.g., healthcare),
  3. financial services,
  4. professional services (e.g., lawyers),
  5. technology services, and
  6. telecommunication.
- When the technology & engineering layer and managerial layer are compromised by attacker, so the legal layer will become a solution to bring the attacker to the court based on the digital forensics of digital evidences

Discussion

The proposed comprehensive reference model here has two use case actors:

1. Engineers, using this reference model as a guide to design and develop digital security system, and can choose a framework that is following the project being worked on
2. Researchers, using this reference model as the initial stage for the development of research in the field of digital security, especially from a comprehensive perspective, which includes three aspects, technology, management, and legal

Conclusion

- There are several reference models for digital security engineering but none of them explain them comprehensively, namely involving the three layers, technology, management, and law.

- For future research, this model can still be more detailed and specific based on developments in science, technology, and applicable law.

- This paper attempts to describe a security engineering model that involves technological, management, and legal aspects.

TERIMA KASIH – THANKYOU VERYMUCH