

Figure 3: Security goals of CPS.

Reviewer 3

Reviewer # 3 (Concern # 1)

The background introduction in the abstract should be briefly introduced or moved to the Introduction section.

We highly appreciate the reviewer's insightful suggestion. We have moved the content from the abstract to the introduction section. Moreover, the abstract is revised. The revised abstract is copied here for your convenience.

Abstract A cyber-physical system (CPS) integrates various interconnected physical processes, computing resources, and networking units, as well as, monitors the process and applications of the computing systems. Interconnection of the physical and cyber world initiates threatening security challenges, especially with the increasing complexity of communication networks. Despite efforts to combat these challenges, it is difficult to detect and analyze cyber-physical attacks in a complex CPS. Machine learning-based models have been adopted by researchers to analyze cyber-physical security systems. This paper discusses the security threats, vulnerabilities, challenges, and attacks of CPS. Initially, the CPS architecture is presented as a layered approach including the physical layer, network layer, and application layer in terms of functionality. Then, different cyber-physical attacks regarding each layer are elaborated, in addition to, challenges, and key issues associated with each layer. Afterward, deep learning models are analyzed for malicious URLs and intrusion detection in cyber-physical systems. A multilayer perceptron architecture is utilized for experiments using the malicious URL detection dataset and KDD Cup99 dataset and its performance is compared with existing works. Lastly, we provide a roadmap of future research directions for cyber-physical security to investigate attacks concerning their source, complexity, and impact.

Reviewer # 3 (Concern # 2)

Some long sentences should be divided into several short ones by adding commas, such as "From a theoretical point of view complex and huge systems can be represented with differential equations of high order but variables of such mathematical models are more vulnerable to noise."
We highly appreciate the reviewers for pointing out the mistake. We have simplified the long sentences in the revised manuscript.

Reviewer # 3 (Concern # 3)

As a survey, the introduction of references is not sufficient. It is suggested to introduce the following recent works in physical layer security field [R1]-[R2] to highlight the state of the art of this paper.
[R1] Lin, Z., Niu, H., An, K., Wang, Y., Zheng, G., Chatzinotas, S. and Hu, Y., 2022. Refracting RIS aided hybrid
[R2] Lin, Z., An, K., Niu, H., Hu, Y., Chatzinotas, S., Zheng, G. and Wang, J., 2022. SLNR-based Secure Energy E

Thank you very much for your valuable suggestions. Following your suggestions, we have added these works in the physical layer field and also provided citations. The newly added part is copied here for your convenience.

Page 6 of the revised manuscript

In order to build a re-configurable radio-based environment of the propagation channel and increase the received signal power, re-configurable intelligent surfaces (RIS) have been studied as a possible approach. A study focused on joint beamforming design and optimization for hybrid satellite-terrestrial relay networks with RIS support, when links from the satellite and base station (BS) to numerous users are blocked [36]. A satellite system should be secure and energy efficient in designing a communication system. A design is proposed by the researcher to improve security and decrease power consumption in [37].

Reviewer # 3 (Concern # 4)

Both the motivation and contributions are not well clarified, which should be further improved to emphasize the novelty of this paper.
Thank you very much for your comments. Respected reviewer, we have presented CPS architecture in a layered approach to providing more clarity in terms of functionality. After that, we discussed CPS attacks on each layer. Then by considering the nature of different attacks, a simple deep learning model namely Multi-layer perceptron (MLP) is deployed for attack detection, especially the detection of malicious URL and CPS attacks. If we consider past studies some researchers have applied hybrid models and some have applied complex deep learning models.
We have applied a simple deep learning architecture, MLP for intrusion detection because MLPs work well for classification prediction issues where inputs have a class or label given to them. MLP works well for regression prediction issues in which a real-valued quantity is predicted from a collection of inputs.
We revised the contributions part of the paper as well.

In order to build a re-configurable radio-based environment of the propagation channel and increase the received signal power, re-configurable intelligent surfaces (RIS) have been studied as a possible approach. A study focused on joint beamforming design and optimization for hybrid satellite-terrestrial relay networks with RIS support, when links from the satellite and base station (BS) to numerous users are blocked [**?**]. A satellite system should be secure and energy efficient in designing a communication system. A design is proposed by the researcher to improve security and decrease power consumption in [**?**].

Reviewer # 3 (Concern # 5)

The figure 1-3 look too blurry and the font size is too small. Their resolution ratio should be much improved.
Thank you very much for your comments. We have updated the figures.

Reviewer # 3 (Concern # 6)

In table 3, why the precision and F1-score of some schemes are missing.
Thank you very much for your comments. Respected reviewer, Table 3 shows the classification results of the proposed approach and existing methods from the literature. A few of those studies did not report results regarding precision and F1 score, so those columns are left blank.

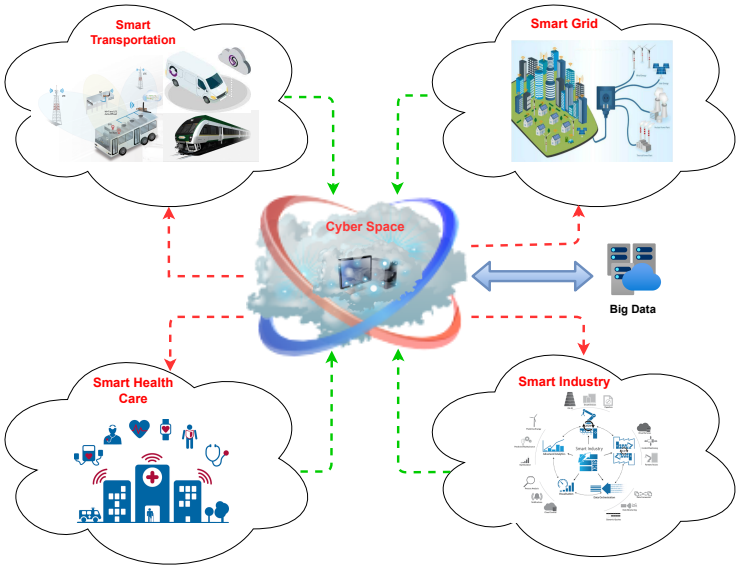

Figure 1: Applications of CPS.

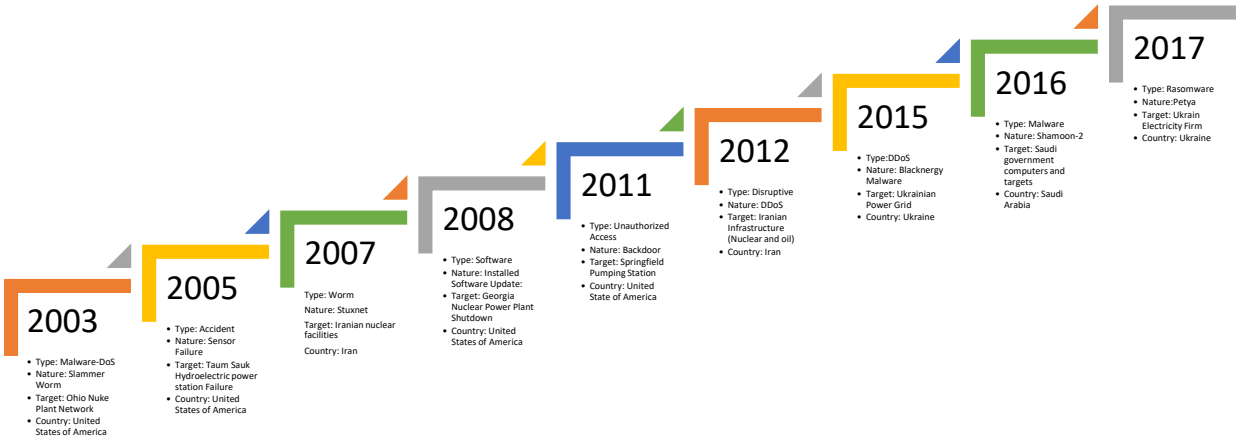

Figure 2: Real CPS attacks in recent years.



Figure 3: Security goals of CPS.