International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
***Article Received:** 30 May 2023 **Revised:** 25 July 2023 **Accepted:** 18 August 2023*

A New Privacy Preservation Intrusion Detection (PPID) Techniques for Multiclass Attacks to Measure Its Reliability for Detecting Suspicious Activities

Dr. Abhilash Maroju,

Ph.D. Research Graduate, Department of Information Technology, University of the Cumberlands , USA.
doctorabhilashmaroju@gmail.com

Dr. Rohith Vallabhaneni,

PhD Research Graduate, Department of Information Technology, University of the Cumberlands , USA.
rohit.vallabhaneni.2222@gmail.com

Dr. Srinivas A Vaddadi,

PhD Research Graduate, Department of Information Technology, University of the Cumberlands , USA. Vsad93@gmail.com

Sravanthi Dontu,

PhD Research Student, Department of Information Technology, University of the Cumberlands, USA.
sravanthi.dontu13@gmail.com

ABSTRACT

There is currently no way that can secure Supervisory Control and Data Acquisition (SCADA) systems from invasions. This technology is not only capable of withstanding numerous types of attacks, but it also prevents the data from being exposed when it is processed by other applications, particularly Intrusion Detection Systems (IDS). Enterprises with mission-critical control environments can have their SCADA systems overseen. Ensuring the security of sensitive information becomes increasingly challenging when physical and digital systems are interconnected. As a result, privacy preservation approaches have been effective in securing private information and identifying harmful actions; yet, they fall short when it comes to detecting errors and determining the sensitivity percentage of data that is disclosed. In order to identify intrusion events and prioritise data, our recently developed Privacy Preservation Intrusion Detection (PPID) approach makes use of the correlation coefficient and Expectation Maximisation (EM) clustering methods. With the power system datasets for multiclass assaults, we test this technique's capacity to reliably detect suspicious activity. As shown above, the experimental findings demonstrate that the proposed strategy is more efficient and effective than three other methods that can be used with current SCADA systems.

1. INTRODUCTION

One of the most challenging aspects of the administration of security for large-scale, high-speed networks is the identification of suspected anomalies in network traffic patterns. These irregularities might be produced by Distributed Denial of Service (DDoS) assaults or the transmission of worms. The following are essential components of a secure network:

- Data confidentiality: Those without the right authorization should not have access to the data that is being transmitted across the network.
- Data integrity: The integrity of data should be preserved during its entire lifecycle, from transmission to reception. Regardless of the cause, corruption or data loss is not tolerated.
- Data availability: The network ought to be able to withstand DoS attacks.

Article Received: *30 May 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

In 1988, a young man named Robert Morris, who was 23 years old at the time, unleashed the first worm, infecting more than 6,000 computers on the ARPANET network. This marked the first major danger to online computer systems. Large corporations' computer systems, including Yahoo!, eBay, Amazon, CNN, ZDnet, and Dadet, were the targets of the first large-scale denial-of-service assaults on February 7, 2000.

Intrusion Detection Systems were developed in response to these risks and those that are anticipated to emerge in the future. Any time data travels into or out of a network, an intrusion detection system (IDS) watches for unusual patterns that could mean an intruder is trying to get into the system.

2. BACKGROUND

The objective of Cyber-Physical Systems (CPS) is to combine physical components (sensors and actuators) with software (embedded computational algorithms) to form a unified real-time control system [1]. Integrating cyber and physical components in accordance with the system design, CPS relies on communication channels (such as computer networks and the Internet) with shared communication protocols to bring the various pieces together. There is a wide range of topics that are covered by CPS. These topics include more traditional types of industrial control systems such as ICS and SCADA, as well as more recent types of smart systems that are built on the Internet of Things (IoT).

Despite the use of the phrase "Cyber-Physical System" in academic circles, the abbreviations "IoT" and "IIoT" are more often used in industry to denote consumer-grade devices and industrial control systems, respectively.

The exponential growth [2] of Cyber-Physical Systems (CPS) has outpaced cybersecurity advancements, leading to new threat models and security challenges. Unfortunately, there isn't a complete structure in place to ensure safe design, viral resistance, and effective risk reduction. Smart home automation systems and other consumer-grade Internet of Things devices are the main focus of both academic and corporate interest. There seems to be less of an emphasis on IIoT from both academics and businesses, despite the fact that its failures can have significantly more serious consequences, such as disruptions to the power system, oil pipeline shutdowns, and transportation networks [2].

Enterprise networks can be protected from intrusions using well-established Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) from firms like Cisco, CrowdStrike, FortiNet, Palo Alto, etc. But CPS doesn't have any IDS/IPS features yet that are comparable [3].

The ubiquitous connectivity introduced by Industry 4.0 has not been completely embraced by legacy ICS and SCADA setups [4]. Also, security measures in ICS are usually not given much attention or priority. The long-held misconception that an air-gapped and trustworthy network keeps the ICS environment separate from the rest of the network is to blame for this [5]. Increased connectivity to hostile networks has led to a surge in malicious breaches into Cyber-Physical Systems (CPS), resulting in massive economic losses and putting people's lives in jeopardy.

Industry control systems (ICS) and supervisory control and data acquisition (SCADA) research integrated into CPS came from academic institutions. Rapid progress has been achieved, particularly in reliability and security engineering, as a result of active cooperation [6] between academic institutions and businesses.

There is a lack of harmony between academic study and professional practice in the fields of anomaly detection, intrusion detection, and intrusion prevention. The purpose of this study is to provide a synopsis of the current research in this field so that future studies can better understand where the field is strong and where it needs improvement.

Long ago, maximum predictability and reliability were the holy grails of ICS design. People thought that basic cybersecurity measures, such using strong passwords or imposing strict authentication requirements, were preventing them from accessing the system. As a result, these systems' designers and operators consciously shied away from taking such precautions [7]. To avoid accidentally quarantining or halting critical system processes due to false positives, typical anti-malware programmes were also avoided, such as signature-based antivirus software. For the most part, these older systems didn't have any kind of access to the public Internet or even to other business networks; they were often run on private, trusted networks.

As a result of the lack of standards during the early stages of ICS design, numerous proprietary communication protocols emerged, many of which used the "security by obscurity" approach [8]. The absence of an effective peer review procedure necessitated this method. Newly found vulnerabilities would also remain in the system for as long as the system existed because manufacturers usually didn't have a way to provide updates or bug fixes. In such instances, the isolation of the network was considered the only defence against potential dangers.

Traditional design ideas became obsolete as ICS systems shifted from legacy to contemporary CPS. As wireless networks got more popular and people moved away from using isolated air-gapped networks, the earlier design concerns became obsolete because of the need of standardised communication protocols used on the public internet.

The traditional protocols used by ICS, such as Modbus, DNP, Fieldbus, HART, and others, are being gradually replaced by the TCP/IP protocols used by Cyber-Physical

Article Received: *30 May 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

Systems (CPS) [9-12]. Businesses' needs to connect to other networks and the Internet at large are driving this change.

Assumption of a hostile network environment is necessary in the current CPS scenario, which depicts a world where threat actors are prevalent and highly interconnected. The vulnerability of CPS has grown dramatically because to its increasing interoperability with public and private networks. Attacks on power grids and other forms of critical national infrastructure (CNI) have so grown in frequency and severity.

3. METHODOLOGY

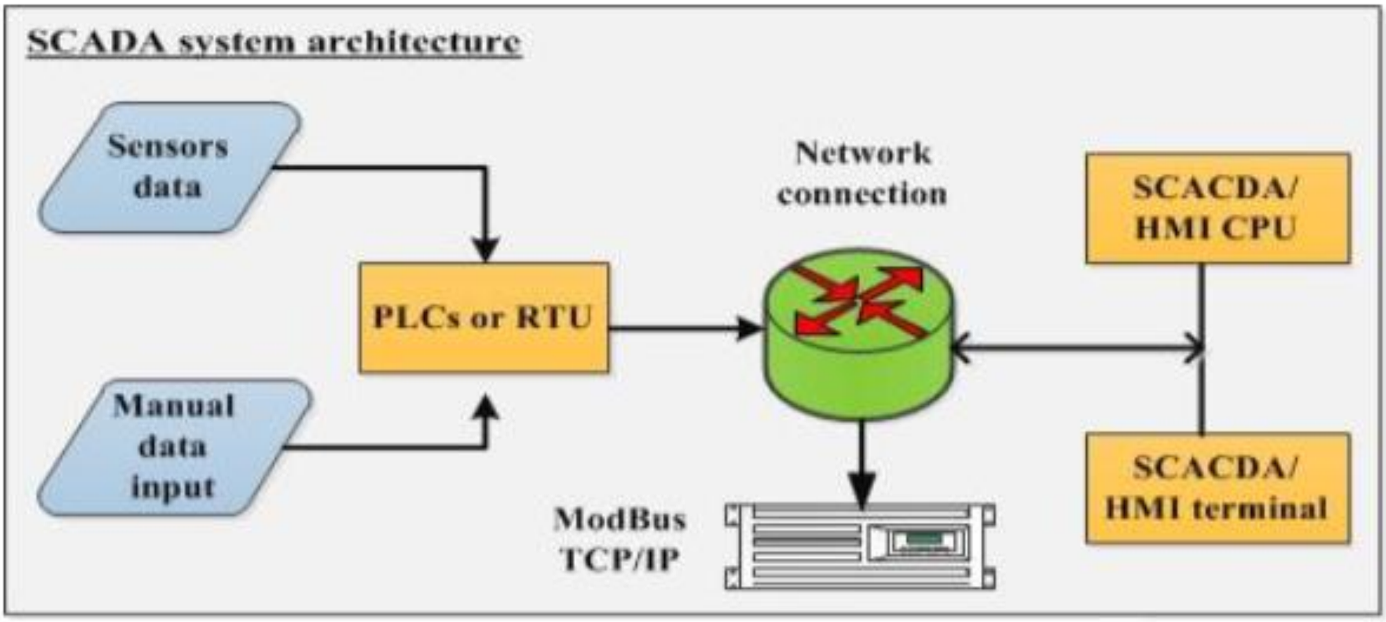


Figure 1. Basic architecture of SCADA systems

3.1 Architecture of privacy preservation Intrusion Detection Technique

For the purpose of detecting hostile observations of SCADA systems and preventing the loss of sensitive or private information, we present an excellent privacy preservation intrusion detection technique. Figure 2 shows the four stages that make up the architecture of this method. These steps indicate the ease with which this technique may be applied to all forms of SCADA technology, particularly electricity systems, which are utilised in this investigation. The first and most important step in the process of constructing privacy and intrusion detection mechanisms is the collection of SCADA data from a data source. This serves to simplify the process both during the preprocessing stage and during the analysis phase. Due to the fact that SCADA data is gathered from a variety of nodes, each of which has a unique protocol, which is incompatible with the methods used for machine learning, this data needs to be processed before it can be executed by those algorithms. The second benefit of employing the PCC technique is that it prevents the disclosure of confidential information regarding SCADA by the selection of portions of critical features. This is due to the fact that certain characteristics end up being ignored, but the strategies of machine learning will make use of the most significant ones. A large number of features is necessary for machine learning techniques to learn and validate a large number of features properly. But this reveals private SCADA system data; so, implementing small features can be a good way to avoid this. An innovative metric for this is the "sensitivity percentage of data disclosure," which measures the chosen feature's proportion to the overall number of features used in a dataset.

***Article Received:** 30 May 2023 **Revised:** 25 July 2023 **Accepted:** 18 August 2023*

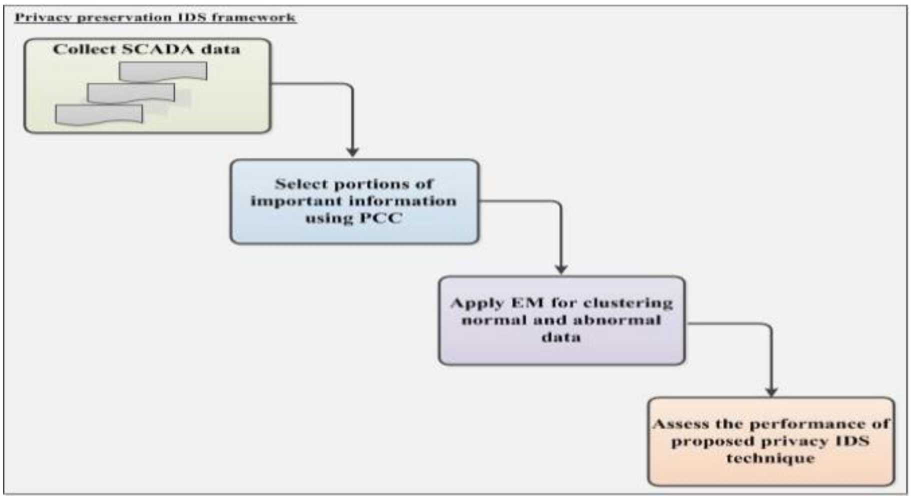
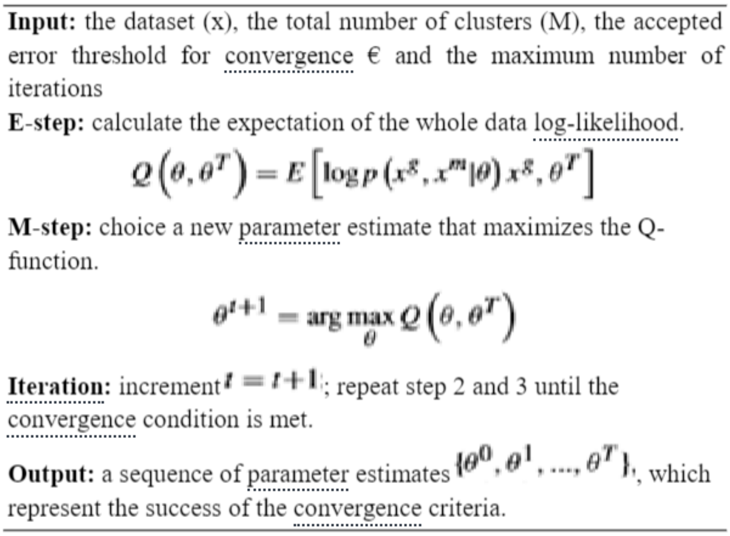

Privacy preservation IDS framework
Collect SCADA data
Select portions of important information using PCC
Apply EM for clustering normal and abnormal data
Assess the performance of proposed privacy IDS technique

Figure 2. Framework of privacy preservation intrusion detection technique.

Algorithm 1: the EM algorithm main steps



Input: the dataset (x), the total number of clusters (M), the accepted error threshold for convergence € and the maximum number of iterations

E-step: calculate the expectation of the whole data log-likelihood.

$$Q\left(\theta,\theta^{T}\right)=E\left[\log p\left(x^{g},x^{m}|\theta\right)x^{g},\theta^{T}\right]$$

M-step: choice a new parameter estimate that maximizes the Q-function.

$$\theta^{t+1}=\arg\max_{\theta}Q\left(\theta,\theta^{T}\right)$$

Iteration: increment $t=t+1$; repeat step 2 and 3 until the convergence condition is met.

Output: a sequence of parameter estimates $\{\theta^{0},\theta^{1},...,\theta^{T}\}$, which represent the success of the convergence criteria.

4. RESULTS AND STUDY

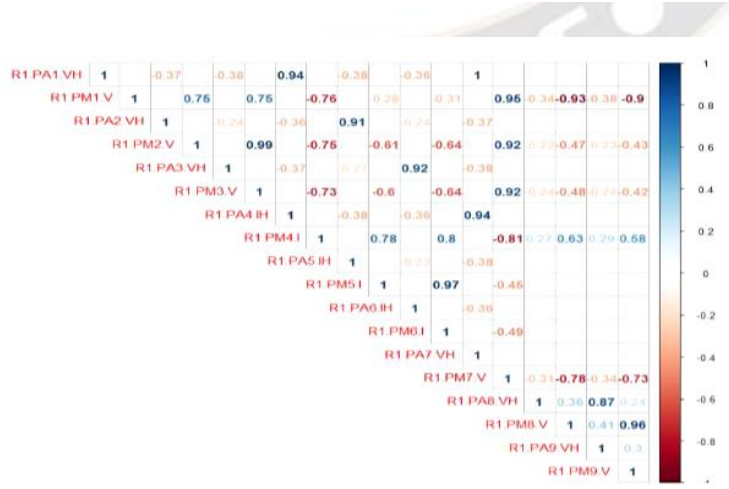


Figure 3. Ranked features using PCC technique

***Article Received:** 30 May 2023 **Revised:** 25 July 2023 **Accepted:** 18 August 2023*

As shown in Figure 3, the PCC method is utilised in order to rank these characteristics within the range of [-1, 1].

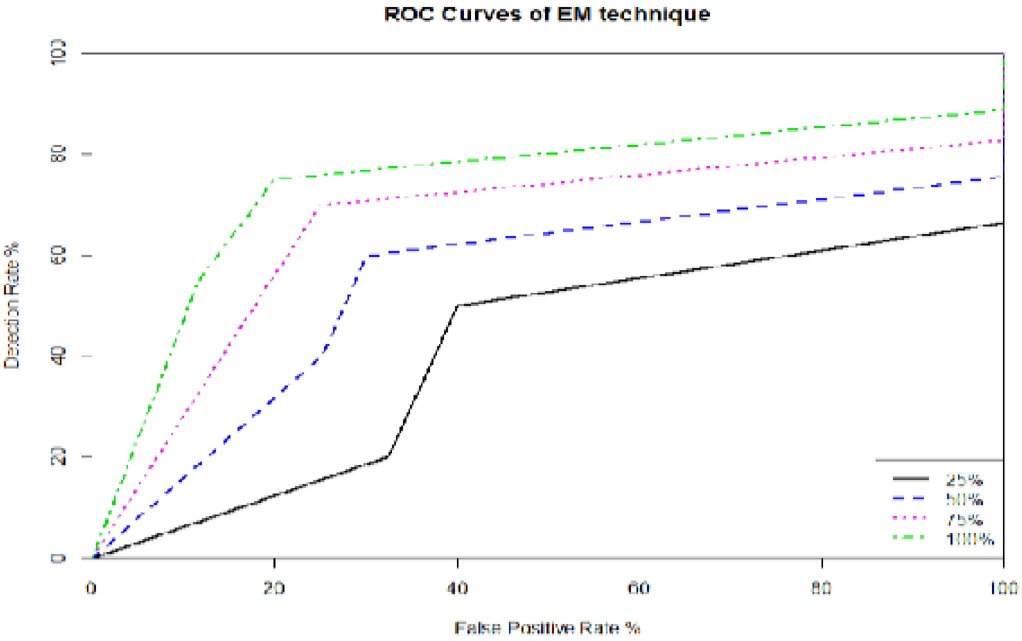
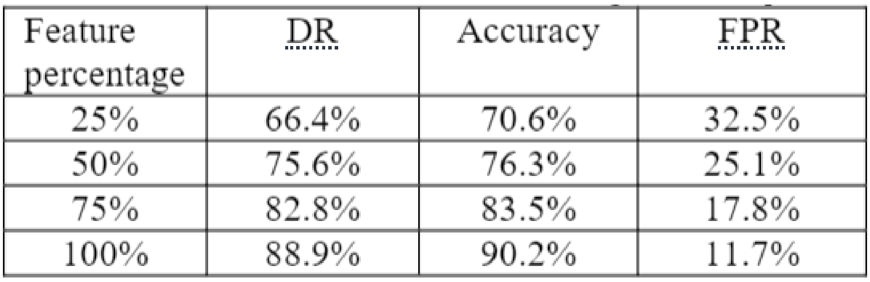


Figure 4. ROC curves of EM technique for feature percentages

A representation of the correlation between the DRs and FPRs for the chosen features is shown in Figure 4 by the Receiver Operating features (ROC) curve.

Table 1. Evaluation of features selection using EM technique



Feature percentage	DR	Accuracy	FPR
25%	66.4%	70.6%	32.5%
50%	75.6%	76.3%	25.1%
75%	82.8%	83.5%	17.8%
100%	88.9%	90.2%	11.7%

Table 1 shows the total DR, accuracy, and FPR values, which are the outcomes of the performance evaluation of the EM, which was conducted in each quarter of these features.

CONCLUSION

The correlation coefficient EM clustering techniques are utilised in this research project to develop a novel intrusion detection mechanism for the purpose of protecting information privacy. By utilising the correlation coefficient technique, significant elements can be chosen from SCADA data in order to extract segments that contain less sensitive information. After that, the SCADA data is organised using the EM clustering approach for efficient and effective abnormal activity detection. Using the power system dataset for multiclass assaults, this study compares the performance evaluation of this mechanism with three other peer methods. The outcomes demonstrate that the proposed method outperforms the alternatives when it comes to identifying SCADA assaults. The findings of the experiment indicate that significantly lowering the number of features that limit the disclosure of sensitive information leads in a minor reduction in the detection rate of attacks.

REFERENCES

1. Bansal, S.; Kumar, D. IoT Ecosystem: A Survey on Devices, Gateways, Operating Systems, Middleware and

Communication. *Int. J. Wirel. Inf. Netw.* **2020**, *27*, 340–364. [**Google Scholar**] [**CrossRef**]

2. Serpanos, D. The Cyber-Physical Systems Revolution. *Computer* **2018**, *51*, 70–73. [**Google Scholar**] [**CrossRef**]
3. Langner, R. To kill a centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve. The Langner Group. 2013. Available online: **https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf** (accessed on 15 October 2022).
4. Alhaidari, F.A.; Al-Dahasi, E.M. New Approach to Determine DDoS Attack Patterns on SCADA System Using Machine Learning. In Proceedings of the 2019 International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 3–4 April 2019; pp. 1–6. [**Google Scholar**] [**CrossRef**]
5. Hewage, C. Opportunities, Challenges and Strategies for Integrating Cyber Security and Safety in Engineering Practice. *Eng. Technol. Open Access J.* **2021**, *3*, 555622. [**Google Scholar**] [**CrossRef**]
6. Pivoto, D.G.S.; de Almeida, L.F.F.; Da Rosa Righi, R.; Rodrigues, J.J.P.C.; Lugli, A.B.; Alberti, A.M. Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review. *J. Manuf. Syst.* **2021**, *58*, 176–192. [**Google Scholar**] [**CrossRef**]
7. Agrawal, N.; Kumar, R. Security Perspective Analysis of Industrial Cyber Physical Systems (I-CPS): A Decade-wide Survey. *ISA Trans.* **2022**, *130*, 10–24. [**Google Scholar**] [**CrossRef**]
8. Qassim, Q.S.; Jamil, N.; Mahdi, M.N.; Rahim, A.A.A. Towards SCADA Threat Intelligence based on Intrusion Detection Systems—A Short Review. In Proceedings of the 2020 8th International Conference on Information Technology and Multimedia (ICIMU), Selangor, Malaysia, 24–26 August 2020; pp. 144–149. [**Google Scholar**] [**CrossRef**]
9. Amin, M.; El-Sousy, F.F.M.; Aziz, G.A.A.; Gaber, K.; Mohammed, O.A. CPS Attacks Mitigation Approaches on Power Electronic Systems With Security Challenges for Smart Grid Applications: A Review. *IEEE Access* **2021**, *9*, 38571–38601. [**Google Scholar**] [**CrossRef**]
10. Wolf, M.; Serpanos, D. *Safe and Secure Cyber-Physical Systems and Internet-of-Things Systems*; Springer International Publishing: Cham, Switzerland, 2020
11. Ramya Manikyam, J. Todd McDonald, William R. Mahoney, Todd R. Andel, and Samuel H. Russ. 2016.Comparing the effectiveness of commercial obfuscators against MATE attacks. In Proceedings of the 6th Workshop on Software Security, Protection, and Reverse Engineering (SSPREW'16)
12. R. Manikyam. 2019.Program protection using software based hardware abstraction.Ph.D. Dissertation.University of South Alabama