Journal of Information Systems Engineering and Management
2025, 10(34s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Enhancing Hand Vein Authentication: Gray Wolf Optimization Mitigates Data Poisoning Attacks

Rajaa Ahmed Ali [1], Ziyad Tariq Mustafa Al-Ta'i [2]

[1]*Department of Computer Science – The Institute of informatics for post-graduation – University of Information Technology and Communication*

[2]*Department of Computer Science – College of Science – University of Diyala2*

ARTICLE INFO

Received: 18 Dec 2024

Revised: 10 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

Nowadays most vital organizations depend on biometric systems to protect their resources and authenticate their customers. Hand vein is one of the biometrics which used for more critical infrastructures. In this paper a hand vein pattern-based biometric authentication system is proposed. The suggested system is designed with attack phase and defense phase. In attack phase, hand veins are preprocessed, and features extracted using PCA-net. These features are clustered using Gray Wolf Optimization (GWO). Lastly, hand veins are poisoned using label flipping mechanism. In defense phase, poisoned hand vein samples are discriminated using Ada-Boost algorithm. The proposed system is highly secure and minimize security loopholes of existing authentication system, through best results: (717) features by PCA-net; best fitness and Silhouette score from GWO (0.75997); ADA-Boost accuracy (baseline step) (0.664857), ADA-Boost accuracy (poisoning step) (0.820512), ADA-Boost accuracy (correction step) (0.827298). Experimental results confirm the effectiveness of the introduced method, where cluster performance improvement is indicated in terms of fitness convergence and silhouette scores. Results show the effectiveness of biometric-based authentication to prevent cyber attacks with privacy and security.

Keywords Data poisoning attacks, federated learning, biometric authentication, hand vein recognition, image processing, PCA Net, Gray Wolf Optimization (GWO).

INTRODUCTION

Traditional systems are unable to distinguish between an authorized person and intruder who can fraudulently access the system. Biometric systems are more convenient to use because there is no need to remember any password and with a single biometric trait different accounts can be secured without the burden of remembering passwords. Biometric systems offer great advantages over traditional systems but they are vulnerable to attacks [1].

Federated learning (FL) means that a way to develop and validate AI models from diverse data sources while mitigating the risk of compromising data security or privacy. A taxonomy of attacks on Federated Learning (FL) systems is shown in figure (1) [2].

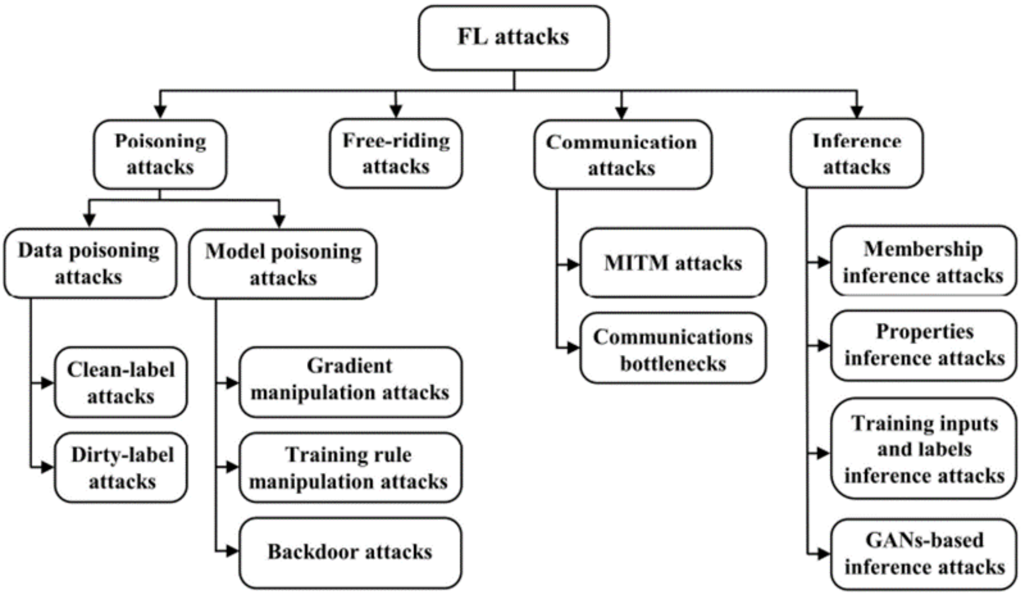
FL attacks
Poisoning attacks
Free-riding attacks
Communication attacks
Inference attacks
Data poisoning attacks
Model poisoning attacks
MITM attacks
Communications bottlenecks
Membership inference attacks
Properties inference attacks
Training inputs and labels inference attacks
GANs-based inference attacks
Clean-label attacks
Dirty-label attacks
Gradient manipulation attacks
Training rule manipulation attacks
Backdoor attacks

Figure 1: Federated Learning (FL) system attack taxonomy [2]

As shown in Figure (2), an adversary participant may adversarial manipulate existing inputs or add poison instances to corrupt the global model's output [2].

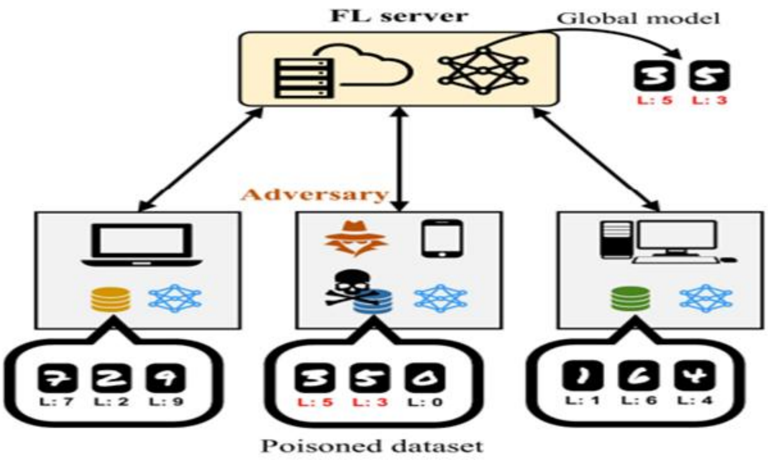

Figure 2: Federated learning systems: an illustration of a data poisoning attack[2].

A label-flipping attack is a type of adversarial attack in machine learning, particularly targeting supervised learning models [3]. In this attack, an adversary maliciously modifies the labels in the training data while keeping the features intact. This manipulation causes the model to learn incorrect mappings between features and labels, leading to degraded performance or biased predictions [4].

Cybercrime and cybersecurity are emerging broad areas in the present that address issues for dealing with computers and networks [5]. The concepts are divergent as in the case of the increased cybercrime incidence; there is failure on the part of cybersecurity [6]. Cybercrimes include label-flipping attacks on biometric systems, especially in subfield of cyber-forensics [7][8][9]. In which, attackers might insert malicious data into the dataset, affecting the efficiency of the biometric protection system [10].

In this research, the authors provided a fast method for performing optimum label flipping poisoning assaults, as well as a technique for detecting and relabeling questionable information, and therefore minimizing the effect of such attacks.

RELATED WORK

The previous studies in the subject take several techniques as shown in the following studies:

Xuezhou Zhang et.al. (2019) [11], they studied data poisoning attacks in the online setting where training items arrives sequentially, and the attacker may perturb the current item to manipulate online learning. The attacker has no knowledge of future training items nor the data generating distribution. They formulated online data poisoning attack as a stochastic optimal control problem and solved it with model predictive control and deep reinforcement learning. Experiments validated the control approach in generating near-optimal attacks on both supervised and unsupervised learning tasks

Zhang et al. (2020) [12], they investigated data poisoning threats in online learning, where data for training is delivered progressively, and the attacker can taint the present data point to interfere with the process of online learning. They provided a methodical approach based on model predictive control, deep learning, and reinforcement techniques, and they described the optimal online attack problem as a stochastic optimal control problem.

Ma et al. (2021) [13], the researchers initiated the first systematic investigation of data poisoning attack on the pairwise ranking algorithms, which can be generally formalized as the dynamic and static games between the ranker and the attacker. These results showed that the proposed methods can significantly reduce the performance of the ranker in the sense that the correlation between the true ranking list and the aggregated results with toxic data can be decreased dramatically.

Robert Wu et. al (2021) [14], the authors evaluated the robustness of an algorithm known as Efficient NAS (ENAS) against data agnostic poisoning attacks on the original search space with carefully designed ineffective operations. By evaluating algorithm performance on the CIFAR-10 dataset. The results provided insights into the challenges to surmount in using NAS for more adversarial robust architecture search.

Mohammad et.al. (2024) [15], they examined label flipping, instance injection, backdoors, and other attack categories that enable malicious outcomes ranging from IP theft to accidents in autonomous systems. Promising detection approaches include statistical tests, robust learning, and forensics. However, significant challenges remain in translating academic defenses like adversarial training and sanitization into practical tools ready for operational use. With safety and trustworthiness at stake, more research on benchmarking evaluations, adaptive attacks, fundamental tradeoffs, and real-world deployment of defenses is urgently needed. Understanding vulnerabilities and developing resilient machine learning pipelines will only grow in importance as data integrity is fundamental to developing safe artificial intelligence.

THE PROPOSED SYSTEM

The proposed system consists of two phases: attack and defense. Each phase includes multiple processes that work together to fulfill the system's aims.

The data set that has been used is HandVein_RL850 [16] which consists of 420 images of hand veins. Figure (3) shows samples of dataset and Attack phase of the proposed system is shown in figure (4).

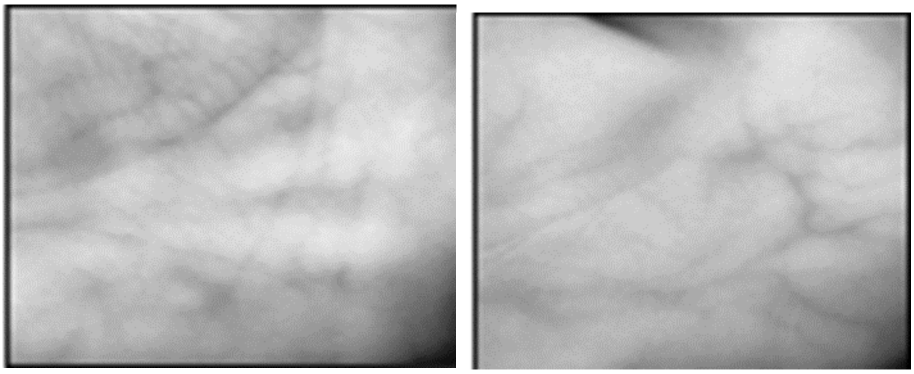

Figure 3: Samples of data Set

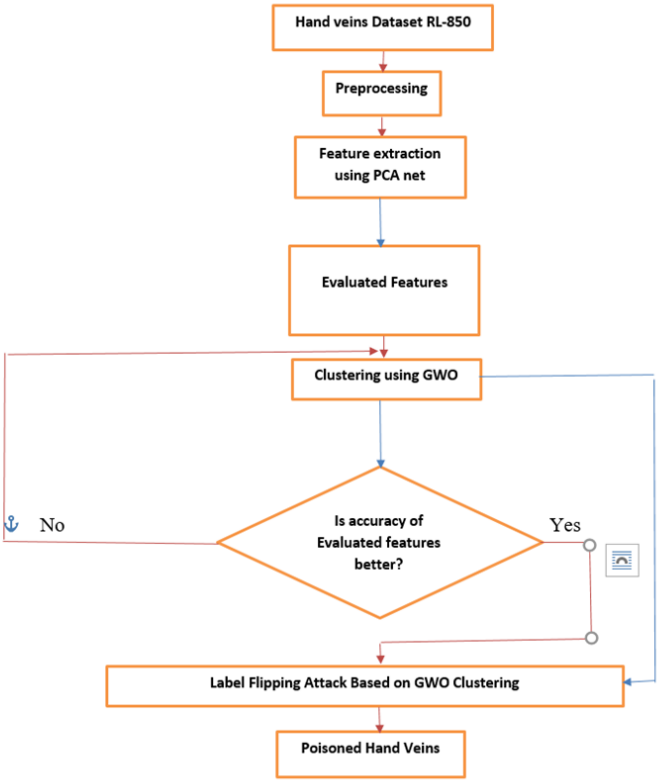
Hand veins Dataset RL-850
Preprocessing
Feature extraction using PCA net
Evaluated Features
Clustering using GWO
No
Is accuracy of Evaluated features better?
Yes
Label Flipping Attack Based on GWO Clustering
Poisoned Hand Veins

Figure 4: Block Diagram of Proposed System in Attack Phase

In figure (4), in preprocessing step, hand veins are filtered using box filters, HFEF and CLAHE. Then the filtered data are discrete cosine transformed (DCT) in order to separate the image into parts with different importance. The DCT transformed data are fused to combine two or more images into one composite image, which integrates the information contained within the individual images. The result is an image that has a higher information content compared to any of the input images. The inverse discrete cosine transform reconstructs a sequence from its discrete cosine transform (DCT) coefficients. The IDCT function is the inverse of the DCT function which is used to merge all the sub-bands image. Data pre-processing can be shown in figure (5 left part). Feature extraction is done depending on using PCA NET. Feature extraction is shown in figure (5 right part).

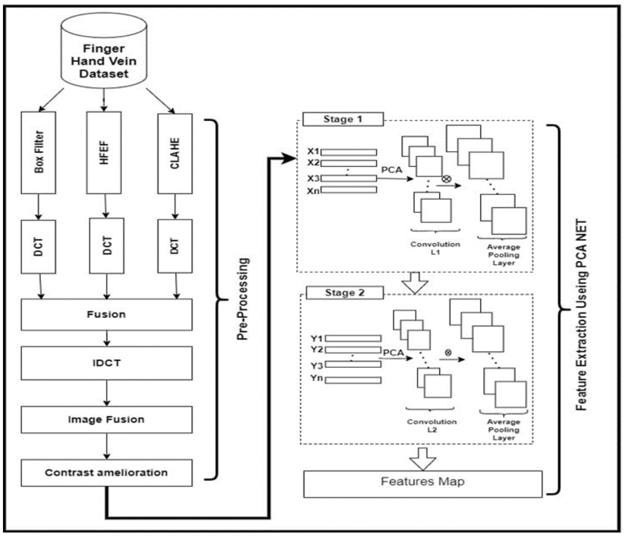

Figure 5: Block Diagram of Preprocessing and Feature Extraction

Evaluation of extracted features is very important in this work, because the features in attack phase need to be compared later which represents the success of poisoning process. Clustering algorithms are used to establish pattern similarities so that data that exhibit similar characteristics can be classified into their corresponding target groups. In this paper, Gray Wolf Algorithm (GWO) is used for clustering purposes. Figure (6) shows the flowchart of GWO.

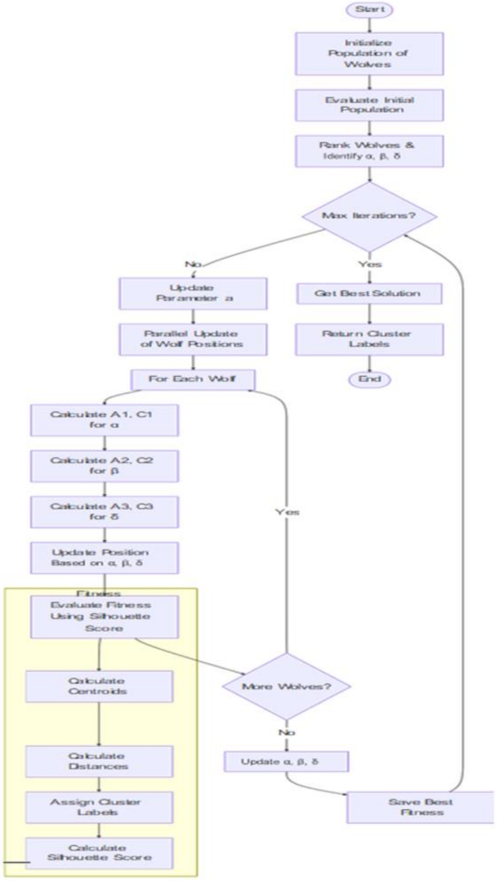

Figure 6: Flowchart of Gray Wolf Algorithm

Figure (7) shows the label flipping process. First, the hand veins data set is classified into benign and malicious clusters by GWO clustering. Then, the silhouette clustering value of the sample is calculated according to the clustering results to select the sample data that are vulnerable to pollution. Finally, the label flip attack is carried out on the selected susceptible data to obtain a contaminated dataset, and the contaminated data poison the whole dataset.

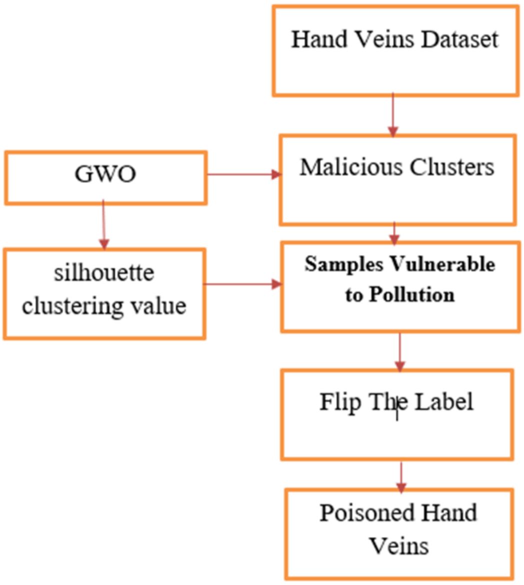

Figure 7: Block Diagram of the Mechanism for Label Flipping Attack

The proposed system in defense phase is shown in figure (8).

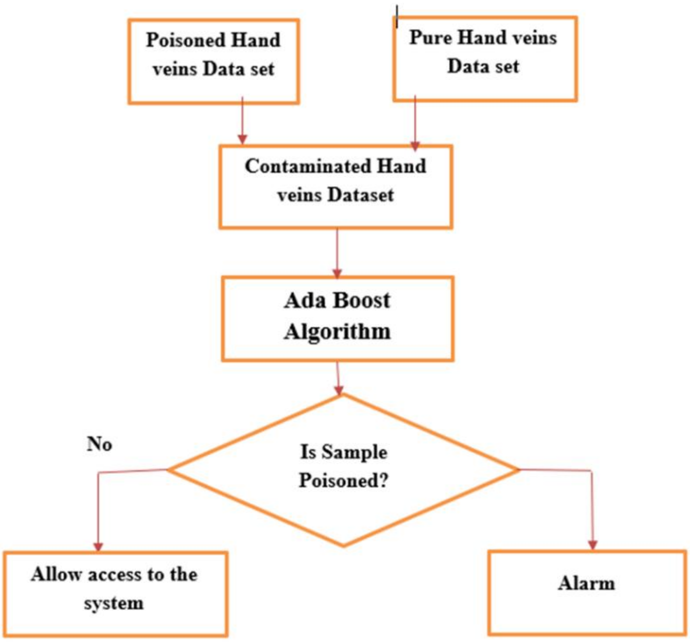
Poisoned Hand veins Data set
Pure Hand veins Data set
Contaminated Hand veins Dataset
Ada Boost Algorithm
No
Is Sample Poisoned?
Allow access to the system
Alarm

Figure8: Block Diagram of the Proposed System in Defense Phase

RESULTS

The output of features extraction by using PCA net as shown in figure (9).

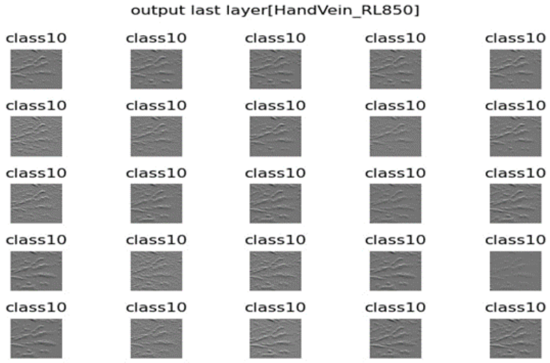

Figure 9: Hand Vein Classes from PCAnet

the number of features which are extracted (717) as shown in figure (10).

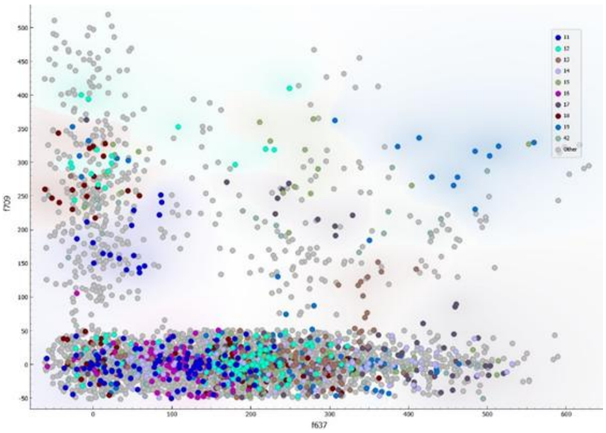

Figure 10: Samples of Extracted Features

Figure (11) shows GWO converge fitness.

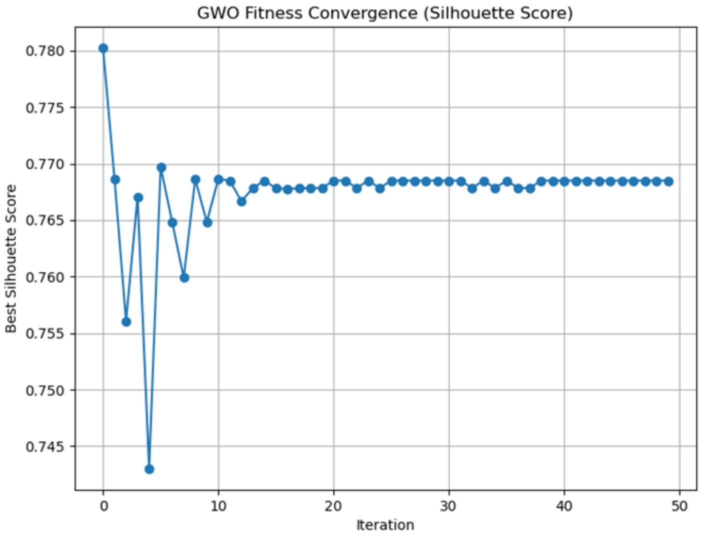

Figure 11: GWO Converge Fitness

The results of Gray Wolf Optimization (GWO) are shown in table (1).

Table 1: Results of the Gray Wolf Algorithm

Iteration	Best Fitness	Silhouette Score
0	6.712399	-0.10799
1	0.749847	0.749847
2	0.744435	0.744435
3	0.752124	0.752124
4	0.752124	0.752124
5	0.752124	0.752124
6	0.752124	0.752124
7	0.75997	0.75997
8	0.752124	0.752124
9	0.752124	0.752124
10	0.75997	0.75997

The performance of AdaBoost algorithm is clarified in table (2).

Table 2: Performance of AdaBoost Algorithm

Algorithm	Step	Accuracy (Overall)	F1 Score (Overall)	Precision (Overall)	Recall (Overall)	Training Time (s)	Inference Time (s)
AdaBoost	Baseline	0.664857	0.043945	0.055853	0.087662	2.303493	0.022974
AdaBoost	Poisoned	0.820512	0.179336	0.201478	0.177489	2.672983	0.03857
AdaBoost	Corrected	0.827298	0.147722	0.150481	0.156926	2.574078	0.022933

CONCLUSION

This work presents a complete hand vein authentication system (attack and defense). However, there some factors play a considerable role such as: PCAnet which extracts the best features of the hand vein. Another effective factor is GWO which subscribes in attack and defense stages. A final considerable factor is ADA-Boost algorithm which discriminates the poisoned hand vein correctly. In spite of the mentioned three factors, but still the limit of applying the proposed work in real time environment. Another limitation is that GWO needs to be compared by other types of clustering.

REFRENCES

[1] A. O. Alaswad, A. H. Montaser, and F. E. Mohamad, “Vulnerabilities of biometric authentication threats and countermeasures,” Int. J. Inf. Comput. Technol., vol. 4, no. 10, pp. 947–958, 2014.

[2] V. Tolpegin, S. Truex, M. E. Gursoy, and L. Liu, “Data poisoning attacks against federated learning systems,” in Computer security–ESORICs 2020: 25th European symposium on research in computer security, guildford, UK, September 14–18, 2020, proceedings, part i 25, pp. 480–501.

[3] M. Zhang, L. Hu, C. Shi, and X. Wang, “Adversarial label-flipping attack and defense for graph neural networks”, in 2020 IEEE International Conference on Data Mining (ICDM), IEEE, 2020, pp. 791–800.

[4] C. Fung, C. J. M. Yoon, and I. Beschastnikh, “Mitigating sybils in federated learning poisoning”, arXiv Prepr. arXiv1808.04866, 2018.

[5] P. Paternoster, “Social media impact and implications on society and students,” J. Media Lit. Educ, vol. 32, pp. 1–17, 2017.

[6] J. B. Hill and N. E. Marion, Introduction to cybercrime: computer crimes, laws, and policing in the 21st century. Bloomsbury Publishing USA, 2016.

[7] S. Chaure and V. Mane, "Digital Forensic Framework for Protecting Data Privacy during Investigation," EAI Endorsed Trans. Scalable Inf. Syst., vol. 11, no. 2, 2024.

[8] F. Anda Basabe, "Forensic data recovery from Android smart watches." Londres/King's College London, 2016.

[9] V. Tolpegin, S. Truex, M. E. Gursoy, and L. Liu, "Data poisoning attacks against federated learning systems," in Computer security–ESORICs 2020: 25th European symposium on research in computer security, ESORICs 2020, guildford, UK, September 14–18, 2020, proceedings, part i 25, Springer, 2020, pp. 480–501.

[10]B. Biggio, B. Nelson, and P. Laskov, "Poisoning attacks against support vector machines," arXiv Prepr. arXiv1206.6389, 2012.

[11] Xuezhou Zhang, ZhuXiaojin, Laurent Lessard, "Online Data Poisoning Attack", arXiv:1903.01666v2 [cs.LG], 30 may, 2019. Available from: https://www.researchgate.net/publication/331543730_Online_Data_Poisoning_Attack#fullTextFileContent [accessed Mar 14 2025].

[12]M. Zhang, L. Hu, C. Shi, and X. Wang, "Adversarial label-flipping attack and defense for graph neural networks," in 2020 IEEE International Conference on Data Mining (ICDM), IEEE, 2020, pp. 791–800.

[13]K. Ma, Q. Xu, J. Zeng, X. Cao, and Q. Huang, "Poisoning attack against estimating from pairwise comparisons," IEEE Trans. Pattern Anal. Mach. Intell., vol. 44, no. 10, pp. 6393–6408, 2021.

[14] Robert Wu, N. Saxena, and R. Jain, "Poisoning the Search Space in Neural Architecture Search" arXiv Prepr. arXiv2106.14406, 2021.

[15]Mohammad Aljanabi, Alaa Hamza, Maad M. Mijwil, Abdelhameed Ibrahim, " Data poisoning: issues, challenges, and needs", 7th IET Smart Cities Symposium (SCS 2023), April 2024.

[16]Dataset publicly available for research purposes, (http://www.wavelab.at/sources/PLUSVein-Contactless/).