ENHANCING SMART GRID SECURITY: MITIGATING DATA POISONING USING EDGE COMPUTING, BLOCKCHAIN, AND DEEP LEARNING

Fateh Bahadur Kunwar[1], Rakesh Kumar Yadav[2] and Hitendra Singh[3]
[1] Research Scholar, CSE, Maharishi University of Information Technology, Lucknow, India
[2,] Associate Professor, CSE, Maharishi University of Information Technology, Lucknow, India
[3] Assistant Professor, CSE, Maharishi University of Information Technology, Lucknow, India

Journal	Samvakti Journal of Research in Information Technology https://www.samvaktijournals.com/sjrit Volume 6 Issue 1 (2025); Page No : 34 - 54
Discipline	Information Security

Date Received : November 20, 2024
ID : sjrit.2024.9
Doi No. : 10.46402/sjrit.2024.9
Publication Date: April 28, 2025
Paper Type : Article
Doi Url : https://dx.doi.org/10.46402/sjrit.2024.9

ABSTRACT

The increasing integration of smart technology in vital infrastructures, such as smart grids, raises serious concerns about their vulnerability to cyber assaults. In this study, data poisoning attacks against Cyber-Physical Systems (CPS) in smart grids are examined, with a particular emphasis on the Smart Grid Management (SCM) component. The research suggests a complex defence system that makes use of blockchain, edge computing, and an advanced deep learning (DL) strategy. Through the reduction of latency and improvement of system responsiveness, the integration of Edge Computing seeks to improve real-time processing capabilities at the network's edge. To create a distributed ledger that is safe from tampering and maintains data integrity throughout the smart grid, blockchain technology is used. Using machine learning to detect and eliminate possible risks, the DL-driven advanced strategy focuses on anomaly detection and mitigation. The study looks at possible weaknesses in SCM and evaluates how well the suggested defence method works to prevent data poisoning attacks. The research intends to highlight the significance of a comprehensive cybersecurity strategy for smart grids by offering insights into

the resilience of the suggested solution in real-world settings via simulations and tests.

Keywords: Data Poisoning Attacks, Blockchain, DL-Driven, Cyber-Physical Systems, SCM, Edge Computing, smart grids

INTRODUCTION

Currently, vast amounts of data are generated each moment as a result of the pervasive utilisation of automation, social media, and technological devices. Concurrently, there is a rise in cyberattacks, encompassing data breaches and identity theft. A variety of security measures mitigate these threats. Within the domain of the internet and digitalisation, blockchain technology represents an emerging trend that provides superior security. The current security protocols rely on centralised servers and systems. The drawbacks of the situation encompass dependence on trustworthy third parties, susceptibility to security breaches, and singular points of failure. Conversely, blockchain technology functions as a decentralised system that depends on trust among network nodes rather than on reliable external entities. The initial digital currencies that rendered blockchain technology accessible were Bitcoin, Ether, and Ripple. Blockchain technology can achieve ethics, accessibility, and privacy standards across various industrial applications, such as banking, healthcare, supply chain management, and voting, without depending on a singular authority.[1][2][3].

The fourth industrial revolution, also known as a technological revolution, has emerged from the integration of digital technology from the previous industrial revolution with the physical and biological realms.[4][5][6][7] The advanced technologies of the fourth industrial revolution, which amalgamate individual ICT with scientific methodologies, facilitate disruptive innovation. Examples of these technologies encompass genetic editing, autonomous vehicles, 3D printing, and the Internet of Things (IoT). Considering the limitations of depending solely on internal business information in a dynamic environment, integrating external knowledge may improve a company's innovation performance.[8][9]. The comprehensive strategy for managing innovation, known as "open innovation," involves systematically promoting and identifying a diverse array of internal and external sources for innovation opportunities, actively integrating this exploration with organisational resources and capabilities, and extensively utilising those opportunities through various channels.[10][11][12][13]. Artificial intelligence profoundly impacts the industry's

approach to innovation. Blockchain technology could facilitate the viability and broader adoption of open innovation by enhancing intellectual property management, increasing transparency, fostering knowledge sharing, and enabling collaborative empowerment through smart contracts and open data, alongside providing novel liquidity for funding innovation, in contrast to the fragmented nature of open innovation. With appropriate data and intelligent contracts, these technological opportunities are attainable.

Artificial intelligence has significantly transformed our lifestyle. Automation is advancing at an accelerating pace across all sectors and levels[16]. Artificial Intelligence is advancing swiftly and has transformed social, economic, and political domains. Artificial intelligence has significantly transformed applications in healthcare, business, education, autonomous vehicles, tourism, social media, and agriculture. Artificial intelligence is becoming increasingly vulnerable to attacks as it is employed for more critical functions. This is due to the increasing prevalence of attacks on sectors such as healthcare, the military, and civic society.

Figure 1 illustrates the various forms of assaults on AI systems[18][19][20]. Assaults on the AI system's input, such as altering an image to modify its output, are termed input attacks. A corrupted AI system is unnecessary. There exist four categories of input attacks: physical, digital, imperceptible, and perceptible. Assaults on visible objects are termed perceivable assaults. Imperceptible assaults are characterised as attacks aimed at digital or physical targets that are not discernible to the naked eye. Digital attacks, often inconspicuous, target digital data such as documents, files, videos, and images. Physical objects are the target of physical assaults. Physical assaults are frequently direct and evident. In an AI model's deployment, the assailant's objective during a poisoning attempt is to induce intrinsic vulnerabilities that facilitate manipulation. Learning is compromised when learning algorithms in dataset poisoning identify patterns in the tainted data to construct a model. Algorithm poisoning involves the manipulation of an algorithm by identifying its vulnerabilities. Federated learning is vulnerable to such attacks since the user retains control over both the data and algorithms.[21][22][23][24][25]. A non-toxic model, trained on a thoroughly validated database, may be employed to update a hazardous model at different stages of development. *Figure 2* illustrates the targets of the attacks that transpired during the AI implementation phase. Numerous critical software applications are rendered unusable in real-world scenarios due to these defects. To facilitate this, it is imperative to implement

measures that reduce an organization's susceptibility to attacks and establish multiple layers of security. To avert "corrupt" outcomes, these measures would encompass identifying and rectifying any input contaminants, techniques, scenarios, or sources of data[26][27][28][29].

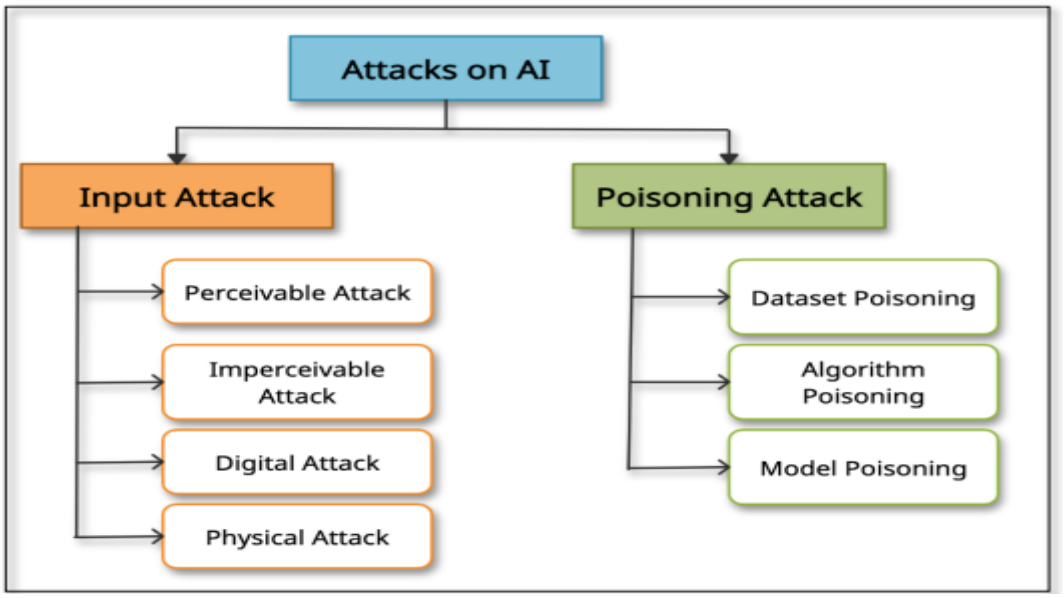

Figure 1 : Attacks Categories on AI

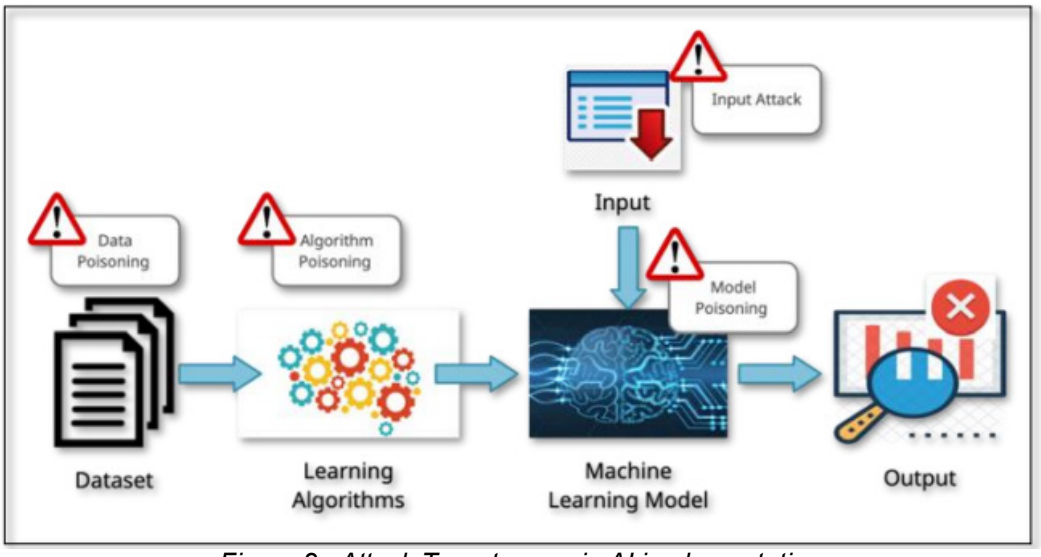

Figure 2 : Attack Target areas in AI implementation

Smart grids are essential for modernising the electricity infrastructure and enhancing productivity, reliability, and ecology. As electrical grids become increasingly interconnected, they become susceptible to various cyber hazards, particularly information poisoning attacks. This article examines the significance of studying data poisoning attacks on Cyber-Physical Systems (CPS) within intelligent grids and proposes a novel approach that integrates edge computing, blockchain-based technology, along with deep learning to enhance cybersecurity protocols. The essay also examines the importance of analysing data poisoning attacks on cyber-physical systems in smart grids.

An Explanation of Data Poisoning Attacks

A data poisoning attack is one in which the training data that is utilised by machine learning models is manipulated in order to reduce the effectiveness of such models. In the context of smart grids, these assaults might result in erroneous choices being made by the control systems, putting the whole power infrastructure's stability and dependability at jeopardy. It is essential to do research on the various forms of data poisoning assaults as well as their effects in order to strengthen the resilience of smart grids against increasing cyber threats.

Computing at the network's edge has a vital role to play in mitigating the risks associated with smart grids, which may be summarised as "the role of edge computing." Edge computing helps minimise latency and improves real-time processing capabilities. It does this by moving computational operations closer to the location where the data is generated. This is especially critical in identifying and mitigating data poisoning threats as quickly as possible, which will ultimately strengthen the smart grid's overall security posture.

Utilising Blockchain Technology

The blockchain technology presents a distributed and tamper-resistant ledger, which guarantees the honesty and openness of financial transactions in smart grids. The use of blockchain technology improves the data security by offering a framework that is both trustless and auditable. This not only protects against the manipulation of data but also guarantees the genuineness of the information that is sent over the smart grid infrastructure.

Approach Based on Deep Learning for More Advanced Work:

Deep learning is a subfield of artificial intelligence that has shown to be an effective method for locating unusual occurrences and intricate patterns hidden inside data. When deep learning models are included into the cybersecurity of

smart grids, it becomes feasible to identify and react in real time to assaults that use data poisoning. Because these models are able to learn and adapt, they are well equipped to deal with the ever-changing and dynamic nature of cyber threats.

Synergies between Edge Computing, Blockchain, and Deep Learning:

The combination of edge computing, blockchain, and deep learning produces a powerful cybersecurity framework thanks to the synergies between these three technologies. Computing at the edge of the network makes it easier to create decentralised blockchain networks, which in turn ensures that safety precautions are spread out over the smart grid. An adaptable and self-learning defence against data poisoning assaults may be provided by deep learning models that are placed at the edge of the network. These models constantly examine the data for any abnormalities.

Security, Privacy, and Ethical Considerations:

Increasing security is of the utmost importance; nevertheless, it is of equal importance to address concerns about privacy as well as ethical issues. In order to win the confidence of the general public and prevent unexpected effects, it is essential to find the optimal compromise between stringent cybersecurity measures and individual rights to privacy.

Performance assessment and Regulatory Compliance:

Metrics for performance assessment need to be defined in order to confirm the efficacy of the suggested strategy. Regulatory compliance is also important. It is possible to run simulations and tests in order to evaluate the system's capacity to correctly identify and defend against data poisoning assaults. In addition, making sure that the planned cybersecurity measures comply with the applicable legislative frameworks guarantees that they are in accordance with the norms and rules that have already been set.

REVIEW OF LITERATURE

Wang et al.[30] offer an authentication approach based on transfer learning empowered blockchains (ATLB) in order to preserve anonymity in industrial applications. By transferring locally or across regions, ATLB lowers the amount of time needed for model training and adds a transfer learning-based authentication method.

Salim et al.[31] hand over authentication (HO-Auth) strategy builds a user profile-based system for instant authorization and uses deep learning (DL) to authenticate devices. By ensuring that data from legitimate devices reaches the blockchain decentralised networks, the technique shields cloud applications against corrupt data. The suggested approach distinguishes between the malicious user and the truthful one by examining the CSI movement pattern gathered from many receivers.

Gaur et al.[32] suggest an authentication system that classifies medical data using the SVM model before storing it in a blockchain-based ledger system in the context of e-health. The authentication procedure may be automated using smart contracts, doing away with the need for a central authority.

Hammad et al.[33] combine preprocessing, feature extraction, and classification into a single unit for lower latency and cost effectiveness Using edge computing servers.

Hussain et al[34] intelligent control medical authentication system makes use of DL models for face recognition in healthcare settings, including ResNet-50, VGG-16, and the local binary patterns histogram (LBPH) method.

Hayashi and Ruggiero[35] presented an activity recognition model using the SVM algorithm is for automatic session management in smart home applications. Finally, provide a multi-phase method using deterministic trust transfer protocol (DTTP) to accomplish safe data transmission and use biometric technologies to identify intruders.

OBJECTIVES

The following questions have particular assessments carried out:

- To examine the web poisons attack methodology in contrast to the physical approach.
- To evaluate the efficacy of the potential poisons attack comprehensively.
- To investigate the batch-point-selection poisoning strategy to minimise time overhead efficiently.
- To investigate the optimal strategies for online single-point poisoning and online batch poisoning attacks
- To examine the true effects of poisoning attacks on power prediction

RESEARCH METHODOLOGY

Experimental setup

Executing the prediction algorithm on Linux-based edge-embedded boards enabled us to replicate the edge computation environment of the smart grid. The central processing unit (CPU) of these boards typically comprises a Cortex-A7, operating at 1.2 GHz, with 256 MB of RAM and 512 MB of ROM. The data was processed using the mathematics, pandas, sklearn, and numpy libraries, and the experiments were conducted in Python. The statistical gradient descent (SGD) linear regression model, which emulates the behaviour of a dynamic model in an artificial intelligence (AI) edge environment, is the designated model for this experiment. The primary criteria for evaluation are the execution duration of the attack, loss over time (LOT), and mean squared error (MSE) loss. Utilising the compromised model to predict the test set samples facilitates the calculation of the MSE loss. Subsequently, the difference between the expected values and the actual values is calculated. The duration of an assault is defined as the interval from the initiation to the conclusion of the attack. The maximum mean squared error (MSE) divided by the total duration of an attack is one method to ascertain the level of threat (LOT). In evaluating the attack's efficiency regarding time overhead, LOT provides a more comprehensive analysis than the MSE statistic. The OptP method, a conventional offline poisoning attack strategy, has served as the foundation for numerous investigations, rendering it highly representative.

Data set

The open power dataset, which was produced from the combined cycle power plant dataset, consists of 9568 data samples acquired between 2006 and 2011. Aside from the average ambient temperature, pressure, and relative humidity, the characteristics also include the exhaust hoover and hourly temperature, with the anticipated label being the net energy production per hour. In order to simulate the appearance of real-time data streams, we followed the steps outlined in and inputted these samples in batches. The possible range of features and labels is [0, 1] because we normalised all the sample values. The features and labels maintained a constant range of values thanks to this normalisation process.

Basic parameters settings

We used 5%, 10%, 15%, and 20% poisoning rates to pollute the creek. Studies conducted in the past seldom contained poisoning rates over 20%. We utilised 0.001 as the convergence termination criterion (ε) for the ε algorithm. We

updated the characteristic scores for the contaminated point samples align with the direction of gradient increase using a decay parameter (α) of 0.01.

RESULTS AND DISCUSSION

Data poisoning attacks require that a machine learning model have an objective function. Based on the goal function, we create a poisoning attack method that creates poisoned samples with the most potential to affect the model's performance. We suppose that the linear regression model's objective function under attack is *Equation 1*

$$\boldsymbol{y = h(X) = \theta_1 x_1 + \theta_2 x_2 + \cdots + \theta_k x_k = \theta^T X}$$

$$\boldsymbol{y = h(X) = \theta_1 x_1 + \theta_2 x_2 + \cdots + \theta_k x_k = \theta^T X}$$

Equation 1 : Objective function of a linear regression model

y is the label vector, while $\boldsymbol{\theta}$ is the parameter vector. The symbol $\boldsymbol{X}$ stands for the model's feature matrix, in which the subscripts k and n correspond to the feature dimension and sample count, respectively. Mean Square Error is used to represent the loss function (MSE):

$$(Ds,\boldsymbol{\theta})=1n\sum ni=1(h(\boldsymbol{x}i)-yi)2)2$$

Equation 2 : Mean Square Error (MSE) loss function

The first set of input samples should be $Ds=\{(\boldsymbol{x}i,yi)\}ni=1$ = 1, following the formula in *Equation 2*, with yi standing for the response label variable of $\boldsymbol{x}i$ and $\boldsymbol{x}i$ for the feature vector. Finding the ideal parameter, $\boldsymbol{\theta}**$, for the minimal loss function shown in *Equation 3* is the typical training objective. Samples stored in smart-grid edge devices are represented by Ds in the edge computing environment, while sample capacity is represented by n. Parameter $\boldsymbol{\theta}**$ is often calculated iteratively using techniques like the gradient descent approach described in *Equation 4*. Sorted according to the number of iterations, it goes by three names: batch gradient descent (BGD), mini-batch gradient descent (MBGD), and stochastic gradient descent (SGD). The BGD method only uses a single iteration of the $\boldsymbol{\theta}i$ parameters for each sample. Unlike the MBGD method, which repeats the parameter iteration for every batch size sample, the SGD method repeats the iteration for every sample. Less computer resources may cause SGD to converge more rapidly, making it more appropriate for edge computing environments where resources are limited.

$$\boldsymbol{\theta}*=arg(Ds,\boldsymbol{\theta})$$

Equation 3 : Optimal parameter vector

$$\boldsymbol{\theta}i+1=\boldsymbol{\theta}i-\alpha\nabla\ (Ds, \boldsymbol{\theta}i)$$

Equation 4 : Gradient descent update rule

Our solution to incremental learning's catastrophic forgetting issue is a caching strategy based on sliding windows. provides information on how to store the online training sample stream that arrives at the edge node at intervals b and b+1+1. Figure 1 shows the samples taken at time b and time b+1+1, with the solid boxes representing those times and the dashed boxes representing the times. L stands for the cache's capacity. The denotation for the number of samples that are being ignored or covered is β. The function bs= {($\boldsymbol{x}i$,)}+Li=b at time b is obtained using this method. The percentage of training data that is forgotten is governed by the edge node's β parameter. The old samples from the previous time step are entirely replaced by the new ones once β=O. Conversely, if β=0=0, it indicates that the new samples do not replace any of the old ones from the preceding time step.

$(x_1, y_1), (x_2, y_2), ..., (x_t, y_t), (X_{t+1}, Y_{t+1}), ..., (x_{t+}\beta, y_{t+}\beta), (X_{t+}\beta_{+1}, Y_{t+}\beta_{+1}), ..., (x_{t+}L_{-1}, y_{t+}L_{-1}), (x_{t+}\beta_{+}L_{-1}, y_{t+}\beta_{+}L_{-1})$

Figure 1. Cache strategy of samples

Keeping with the prior strategy, this research assumes that attackers may use attack points or manipulate the $\boldsymbol{P}b$ to input damaging data and poison the learning process when training data is received sequentially, undermining the online learning process. This section will provide a model for a grey poisoning assault that may be used to address the online learning regression issue.

Our opponent model is defined in accordance with the guidelines given in, which include outlining the adversary's objectives and defining their skill set. An ideal assault approach is then defined using this data.

Online and Offline Poisoning Attacks: Effectiveness Comparison

We partitioned the 9568 sample points into 10 pieces and fed them sequentially into the ODPA-SP algorithm to make it seem as if the data stream points were entering the cache one by one. The time series correlation was more pronounced in power data samples. Thus, the order of the samples in this experiment was preserved for each simulated training procedure. Our method maintained a temporal relationship between the power data samples all during training, which allowed us to provide trustworthy findings. After ten tries, we recorded the timestamps and outcomes of each attack to determine the average loss and total execution time. In order to mimic an offline poisoning

attack, we also record the attack's duration and loss when all 9568 sample points are fed simultaneously into the ODPA-SP algorithm. Table 1 shows that the combined time of the 10 assaults was 17.37 seconds, which is less than the offline attack's length by half. Conversely, the offline attack and the ten attacks both resulted in similar average losses. The findings show that the online assault strategy may reduce time overhead while keeping poisoning effective.

Cache	MSE	Time				
Cache_1	0.0440204	1.699955	**Average_Test_MSE (Online)**	**Total time of 10 caches (Online)**	**MSE of 9568 (Offline)**	**Total time of 9568 (Offline)**
Cache_2	0.0442852	1.642623				
Cache_3	0.0493196	1.677615				
Cache_4	0.0391493	1.869981				
Cache_5	0.040855	2.021997				
Cache_6	0.0480127	1.68938				
Cache_7	0.0487629	1.710946				
Cache_8	0.0401011	1.692828				
Cache_9	0.0451106	1.674517				
Cache_10	0.0488317	1.692794	**0.0448449**	**17.372636 s**	0.0448471	34.713239 s

Table 1 : Online and offline poisoning attacks comparison

Performance of Point Selection Strategy

You can see the outcomes of the experiment in the figure. All three assaults have the potential to skew linear regression models' prediction abilities, and when poisoning rates rise, the MSE change is also linear and upward.

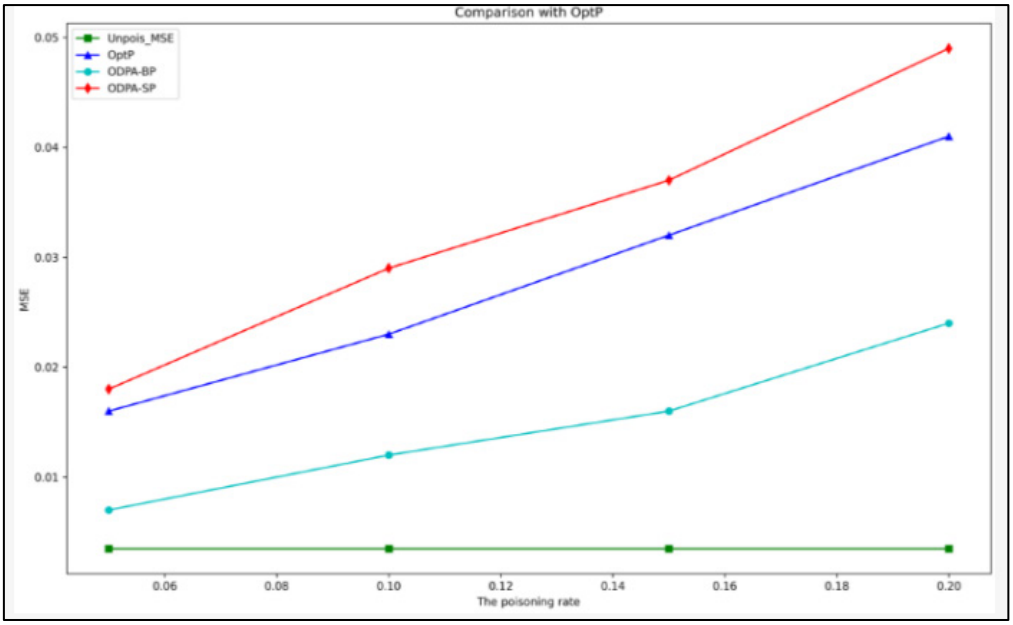

Figure 3 : MSE comparison of attacks

Application of the Batch-Poisoning Technique

No less than 285, 1125, and 9568 data points were used in the three methods by the researchers. They measured the execution time at four different poisoning rates throughout the test. Although it does not provide a big mean square error (MSE), the findings show that the ODPA-BP method considerably decreases execution time when contrasted with the other two methods. The time overhead of the assault is reduced using the batch-poisoning approach, as seen below.

Sam Num		285				1125				9568			
Pois_Rate		0.05	0.1	0.15	0.2	0.05	0.1	0.15	0.2	0.05	0.1	0.15	0.2
Time(s)	**OptP**	0.286477	0.4178 2	0.477785	0.5984 9	0.798881	1.153583	1.513819	1.942288	12.318 18	19.376 246	26.765 12	34.670 963
	ODPA-BP	**0.056842**	**0.0808 12**	**0.102725**	**0.119408**	**0.182836**	**0.276719**	**0.417298**	**0.606962**	**4.3426 872**	**6.7384 31**	**9.5356 06**	**12.059 491**

Sam Num		285				1125				9568			
	ODPA-SP	0.1913 6	0.2845 99	0.3468 48	0.3880 27	0.7791 18	1.1884 95	1.5425 14	1.9119 88	12.2801 06	18.7207 26	26.1316 43	34.0338 81

Table 2 : Three attacks Time comparison

An analysis comparing ODPA-SP with ODPA-BP

Figure 6 juxtaposes the LOT index alongside the aggregate count of poisoning specimens, while the total number of samples is represented on the horizontal dimension. Table 3 displays the findings. The results indicate that when selecting picking attack algorithms, it is more imperative to utilise LOT comprehensively rather than solely focus on the extent of enhancement in MSE. A comparison of the three algorithms' LOT index performance is displayed in Figure 6, where the red line has a significantly larger peak values than the others two lines. This indicates that, despite achieving a favourable performance on the MSE index, the ODPA-BP algorithm exhibits the highest overall efficiency, signifying it reduces the time necessary to attain the maximum MSE loss. The graphic illustrates the performance trajectories of the three algorithms as the quantity of contaminated samples escalated. All three techniques performed effectively with 285 samples and a poisoning rate of 0.2, corresponding to approximately 57 poisonous samples. This gives good advice for finding the optimal cache size.

Pois_Num		15	29	43	57	81	113	169	225	478	957	1435	1914
Time(s)	Optp	0.2864 6	0.4178 2	0.4777 85	0.5984 9	0.7988 81	1.1535 83	1.5138 19	1.9422 88	12.381 818	19.376 246	26.736 512	34.670 963
	ODPA-	0.0568 32	0.0808 12	0.1027 25	0.1194 08	0.1828 36	0.2767 19	0.4172 98	0.6069 62	4.3468 72	6.7384 31	9.5356 06	12.059 491
	ODPA-	0.1913 8	0.2845 99	0.3468 48	0.3880 27	0.7791 18	1.1884 95	1.5425 14	1.9119 88	12.280 106	18.720 726	26.131 643	34.033 881

Pois_Num			15	29	43	57	81	113	169	225	478	957	1435	1914
MSE		Opt P	0.0014	0.0025	0.0031	0.0038	0.0016	0.0023	0.0032	0.0041	0.0017	0.0024	0.0034	0.0043
		ODPA-05	0.0005	0.0008	0.0012	0.0015	0.0007	0.0012	0.0016	0.0024	0.0009	0.0013	0.0018	0.0025
		ODPA-15	0.0015	0.0023	0.0028	0.0038	0.0018	0.0029	0.0037	0.0049	0.0019	0.0025	0.0034	0.005
Loss_Over_Time	(LOT)	Opt P	0.000589 09	0.000598 344	0.000648 827	**0.000634 931**	0.000200 28	0.000199 379	0.000211 386	0.000211 091	0.000013 73	0.000012 386	0.000012 717	0.000012 402
		ODPA-055	0.1055 558	0.000989 952	0.1168 167	**0.1256 197**	0.000382 857	0.000433 653	0.000383 419	0.000395 412	0.000020 705	0.000019 292	0.000018 877	0.000020 731
		ODPA-836	0.000836 12	0.000808 155	0.000807 27	**0.000979 313**	0.000231 03	0.000244 006	0.000239 868	0.000256 278	0.000015 472	0.000013 354	0.000013 011	0.000014 691

Table 3 : Comparative study of three attacks

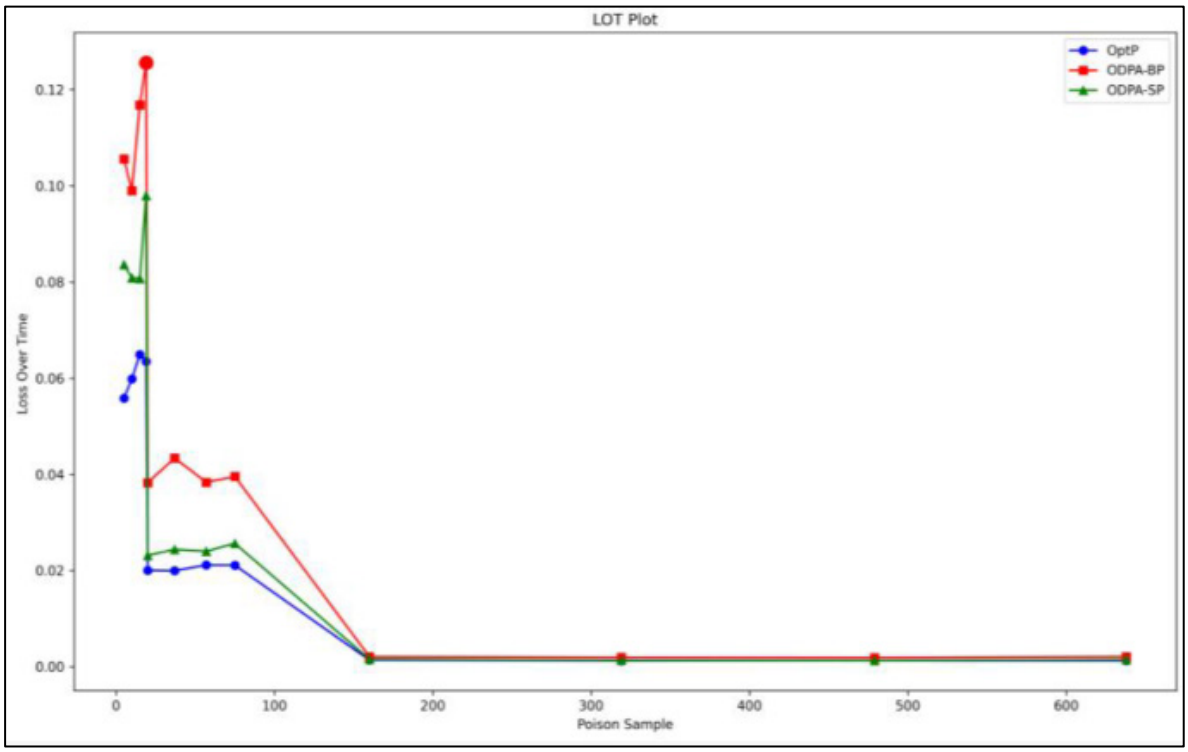

Figure 4 : LOT competition of attacks

The Real Effect of Poisoning Incidents on Power Forecasts

Figure 4 illustrates that the objective function of a machine learning model is essential for executing toxic data assaults This intended function underpins the development of the intoxication attack methodology, enabling the generation of tainted samples that can substantially degrade the model's efficacy. Specifications of the symbols utilised in this section are provided in Table 2. The horizontal dimension represents the real amounts of electricity alongside the number of forecast samples, Based on the picture, it's clear that the quantities of energy generated by assaults vary greatly from what's really happening on the ground. The most pronounced departure from the expected values, which worsens as the MSE increases, is shown by the solid blue and red circles. Typically, a fluctuation of around 5% in the electric energy prediction is required to provide sufficient safety. However, the graphic shows that the variance has already beyond this limit. There will be a major imbalance in the power system's load due to either an overestimation or an underestimation of the expected electric energy unless something is done. So, this experiment is meant to show how crucial it is to take precautions against poisoning attacks.

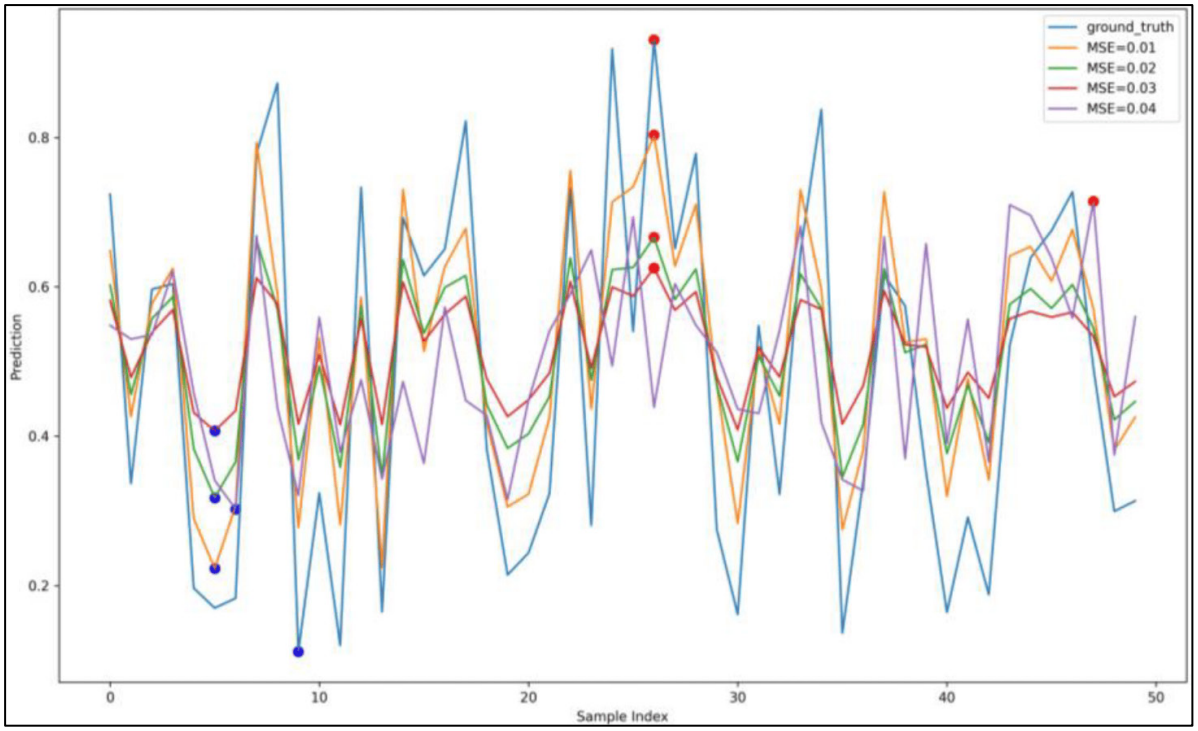

Figure 5 : Poisoning attacks impact on power prediction

CONCLUSION

Finally, this study tackles the important problem of cyber-physical system data poisoning in smart grids, namely in the Smart Grid Management (SCM) space. A complete defence mechanism to strengthen the resilience of smart grids against growing cyber threats is offered by integrating Edge Computing, Blockchain, and an innovative strategy powered by deep learning. By integrating Edge Computing, the system's real-time data processing capability is improved, minimising latency-related threats. By using blockchain technology, data integrity and immutability are guaranteed, avoiding unwanted tampering and creating a transparent and reliable operating environment for smart grid systems. With its emphasis on anomaly detection and mitigation, the DL-driven advanced method provides an adaptable layer of defence that can change and adapt to fight new threats. The efficiency of the suggested defence mechanism is assessed by comprehensive simulations and tests, providing insightful information about its performance in many settings and practical applicability.

Findings of the study

- The results highlight the need of a multi-layered cybersecurity approach for smart grids, taking into account the ever-changing nature of cyber threats and the significance of preventative actions to protect vital infrastructure.
- The findings of this study support ongoing efforts to secure and future-proof these systems against cyber threats, ensuring the dependability and resilience of our energy infrastructure in the face of a constantly changing digital landscape. Smart grids continue to play a crucial role in modernising energy distribution systems.

SCOPE FOR FURTHER RESEARCH

To further examine poisoning assault and defence techniques, in further research, we want to examine increasingly complex deep learning and neural network models implemented online.

REFERENCES

[1] O. A. Wahab, A. Mourad, H. Otrok, and T. Taleb, “Federated machine learning: Survey, multi-level classification, desirable criteria and future directions in communication and networking systems,” IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 1342–1397, 2021, doi: 10.1109/COMST.2021.3058573).

[2] D. C. Nguyen, M. Ding, Q.-V. Pham, P. N. Pathirana, L. B. Le, A. Seneviratne, J. Li, D. Niyato, and H. V. Poor, “Federated learning meets blockchain in edge computing: Opportunities and challenges,” IEEE Internet of Things Journal, vol. 8, no. 16, pp. 12 806–12 825, 2021, doi: 10.1109/COMST.2021.3058573).

[3] M. Alazab, S. P. RM, M. Parimala, P. K. R. Maddikunta, T. R. Gadekallu, and Q.-V. Pham, “Federated learning for cybersecurity: concepts, challenges, and future directions,” IEEE Transactions on Industrial Informatics, vol. 18, no. 5, pp. 3501–3509, 2021, doi: 10.1109/TII.2021.3119038.

[4] S. Zaman, K. Alhazmi, M. Aseeri, M. R. Ahmed, R. T. Khan, M. S. Kaiser, and M. Mahmud, "Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey," in IEEE Access, vol. 9, pp. 94668-94690, 2021, doi: 10.1109/ACCESS.2021.3089681.

[5] V. Mothukuri, R. M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, and G. Srivastava, “A survey on security and privacy of federated learning,” Future Generation Computer Systems, vol. 115, pp. 619– 640, 2021. https://doi.org/10.1016/j.future.2020.10.007

[6] B. Ghimire and D. B. Rawat, "Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things," in IEEE Internet of Things Journal, vol. 9, no. 11, pp. 8229-8249, 1 June1, 2022, doi: 10.1109/JIOT.2022.3150363.

[7] X. Ma, J. Zhu, Z. Lin, S. Chen, and Y. Qin, “A state-of-the-art survey on solving non-iid data in federated learning,” Future Generation Computer Systems, vol. 135, pp. 244–258, 2022 doi: 10.1016/j.future.2022.05.003.

[8] Z. Liu, J. Guo, W. Yang, J. Fan, K.-Y. Lam, and J. Zhao, “Privacy-preserving aggregation in federated learning: A survey,” IEEE Transactions on Big Data, 2022 https://arxiv.org/abs/2203.17005.

[9] P. Boobalan, S. P. Ramu, Q.-V. Pham, K. Dev, S. Pandya, P. K. R. Maddikunta, T. R. Gadekallu, and T. Huynh-The, “Fusion of federated learning and industrial internet of things: A survey,” Computer Networks, vol. 212, p. 109048, 2022, doi: 10.48550/arXiv.2101.00798.

[10] Z. Yang, M. Chen, K.-K. Wong, H. V. Poor, and S. Cui, “Federated learning for 6g: Applications, challenges, and opportunities,” Engineering, vol. 8, pp. 33–41, 2022 doi: 10.1016/j.eng.2021.12.002.

[11] Sarker, I.H., Khan, A.I., Abushark, Y.B. et al. Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions. Mobile Netw Appl 28, 296–312 (2023). https://doi.org/10.1007/s11036-022-01937-3.

[12] L. Lyu, H. Yu, and Q. Yang, “Threats to federated learning: A survey,” arXiv preprint arXiv:2003.02133, 2020, doi: 10.48550/arXiv.2003.02133.

[13] Q. Yang, Y. Liu, T. Chen, and Y. Tong, “Federated machine learning: Concept and applications,” ACM Transactions on Intelligent Systems and Technology (TIST), vol. 10, no. 2, pp. 1–19, 2019. doi: 10.1145/3298981.

[14] V. Shejwalkar, A. Houmansadr, P. Kairouz, and D. Ramage, “Back to the drawing board: A critical evaluation of poisoning attacks on production federated learning,” in 2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022, pp. 1354–1371, doi: 10.1109/SP46214.2022.9833647.

[15] M. Kuzlu, C. Fair, and O. Guler, “Role of artificial intelligence in the internet of things (iot) cybersecurity,” Discover Internet of things, vol. 1, 7, pp. 1–14, 2021, doi: 10.1007/s43926-020-00001-4

[16] A. Oseni, N. Moustafa, H. Janicke, P. Liu, Z. Tari, and A. Vasilakos, “Security and privacy for artificial intelligence: Opportunities and challenges,” arXiv preprint arXiv:2102.04661, 2021 doi: 10.48550/arXiv.2102.04661.

[17] M. A. Ferrag, O. Friha, L. Maglaras, H. Janicke, and L. Shu, “Federated deep learning for cyber security in the internet of things: Concepts, applications, and experimental analysis,” IEEE Access, vol. 9, pp. 138509–138542, 2021, doi: 10.1109/ACCESS.2021.3118642.

[18] W. Saad, M. Bennis, and M. Chen, “A vision of 6g wireless systems: Applications, trends, technologies, and open research problems,” IEEE network, vol. 34, no. 3, pp. 134–142, 2019, doi: 10.1109/MNET.001.1900287.

[19] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, “AI and 6g security: Opportunities and challenges,” in 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit). IEEE, 2021, pp. 616–621, doi: 10.1109/EuCNC/6GSummit51104.2021.9482503.

[20] A. Chouman, D. M. Manias, and A. Shami, “Towards supporting intelligence in 5g/6g core networks: Nwdaf implementation and initial analysis,” in 2022 International Wireless Communications and Mobile Computing (IWCMC). IEEE, 2022, pp. 324–329, doi: 10.48550/arXiv.2205.15121.

[21] G. Zhu, D. Liu, Y. Du, C. You, J. Zhang, and K. Huang, “Toward an intelligent edge: Wireless communication meets machine learning,” IEEE communications magazine, vol. 58, no. 1, pp. 19–25, 2020 , doi: 10.1109/MCOM.001.1900103.

[22] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, “What should 6g be?” Nature Electronics, vol. 3, pp. 20–29, 2020, doi: 10.1038/s41928-019-0355-6.

[23] F. Tariq, M. R. A. Khandaker, K. -K. Wong, M. A. Imran, M. Bennis and M. Debbah, "A Speculative Study on 6G," in IEEE Wireless Communications, vol. 27, no. 4, pp. 118-125, August 2020, doi: 10.1109/MWC.001.1900488.

[24] C. Annadurai, I. Nelson, K. N. Devi, R. Manikandan, N. Z. Jhanjhi, M. Masud, and A. Sheikh, “Biometric authentication-based intrusion detection using artificial intelligence Internet of Things in smart city,” Energies, vol. 15, no. 19, article no. 7430, 2022 doi: 10.3390/en15197430.

[25] A. Ashtari and B. Alizadeh, “A comparative study of machine learning classifiers for secure RF-PUF-based authentication in Internet of Things,” Microprocessors and Microsystems, vol. 93, article no. 104600, 2022, 10.1016/j.micpro.2022.104600.

[26] G. Oligeri, S. Sciancalepore, S. Raponi, and R. Di Pietro, “PAST-AI: physical-layer authentication of satellite transmitters via deep learning,” IEEE Transactions on Information Forensics and Security, vol. 18, pp. 274-289, 2023, doi: 10.1109/TIFS.2022.3219287.

[27] A. K. Sahu, S. Sharma, and R. Raja, “Deep learning-based continuous authentication for an IoT-enabled healthcare service,” Computers and Electrical Engineering, vol. 99, article no. 107817, 2022, doi: 10.1016/j.compeleceng.2022.107817.

[28] S. Chinnaswamy and K. Annapurani, “Trust aggregation authentication protocol using machine learning for IoT wireless sensor networks,” Computers & Electrical Engineering, vol. 91, article no. 107130, 2021, doi: 10.1016/j.compeleceng.2021.107130.

[29] S. Maurya, S. Joseph, A. Asokan, A. A. Algethami, M. Hamdi, and H. T. Rauf, “Federated transfer learning for authentication and privacy preservation using novel supportive twin delayed DDPG (S-TD3) algorithm for IIoT,” Sensors, vol. 21, no. 23, article no. 7793, 2021, doi: 10.3390/s21237793.

[30] X. Wang, S. Garg, H. Lin, M. J. Piran, J. Hu, and M. S. Hossain, “Enabling secure authentication in industrial IoT with transfer learning empowered blockchain,” IEEE Transactions on Industrial Informatics, vol. 17, no. 11, pp. 7725-7733, 2021 , doi: 10.1109/TII.2021.3049405.

[31] Shailendra Rathore, Yi Pan, and Jong Hyuk Park, "BlockDeepNet: A Blockchain-Based Secure Deep Learning for IoT Network," *Sustainability*, vol. 11, no. 14, 2019, doi: 10.3390/su11143974

[32] R. Gaur, S. Prakash, S. Kumar, K. Abhishek, M. Msahli, and A. Wahid, “A machine-learning–blockchain-based authentication using smart contracts for an IoHT system,” Sensors, vol. 22, no. 23, article no. 9074, 2022, doi: 10.3390/s22239074.

[33] M. Hammad, A. M. Iliyasu, I. A. Elgendy, and A. A. Abd El-Latif, “End-to-end data authentication deep learning model for securing IoT configurations,” Human-centric Computing and Information Sciences, vol. 12, article no. 4, 2022, doi: 10.22967/HCIS.2022.12.004.

[34] T. Hussain, D. Hussain, I. Hussain, H. AlSalman, S. Hussain, S. S. Ullah, and S. Al-Hadhrami, “Internet of Things with deep learning-based face recognition approach for authentication in control medical systems,” Computational and Mathematical Methods in Medicine, vol. 2022, article no. 5137513, 2022, doi: 10.1155/2022/5137513.

[35] V. T. Hayashi and W. V. Ruggiero, “Hands-free authentication for virtual assistants with trusted IoT device and machine learning,” Sensors, vol. 22, no. 4, article no. 1325, 2022, doi: 10.3390/s22041325.

End