The Scientific Temper (2023) Vol. 14 (4): 1271-1276

E-ISSN: 2231-6396, ISSN: 0976-8653

Doi: 10.58414/SCIENTIFICTEMPER.2023.14.4.31

https://scientifictemper.com/

RESEARCH ARTICLE

Advancing device and network security for enhanced privacy

K. Sreenivasulu[1], Sampath S.[2], Arepalli Gopi[3], Deepak Kartikey[4], S. Bharathidasan[5], Neelam L. Kumar[6*]

Abstract

The rapid proliferation of Internet of Things (IoT) devices has ushered in an era of unprecedented connectivity and automation. The widespread adoption has also exposed vulnerabilities, necessitating robust security and privacy measures. This research presents a comprehensive study focused on enhancing IoT device and network security and privacy through empirical investigation and advanced machine learning techniques. Commencing with an exhaustive literature review, it was assessed, the evolving landscape of IoT security threats, solutions, and identified research gaps. Building upon the foundation, it was designed and rigorously evaluated a machine learning-based classification model tailored for IoT device security. Utilizing a meticulously crafted simulated dataset mirroring real-world IoT features, our model undergoes comprehensive performance evaluations. Metrics include accuracy, precision, recall, F1 score, and receiver operating characteristic (ROC) analysis. Our findings reveal a nuanced performance profile, shedding light on the model's capability to accurately classify IoT devices as secure or vulnerable. Precision-recall trade-offs, emphasizing the need for a judicious balance to mitigate false positives and false negatives was investigated. The critical role of feature engineering and model refinement, points to areas for future research and optimization. This research contributes to the burgeoning field of IoT security by employing machine learning as a proactive tool for fortifying IoT device and network security. Our findings advocate for a strategic approach to secure IoT ecosystems, ensuring data integrity and privacy in the face of evolving threats. As IoT devices continue to proliferate across industries, this research serves as a foundation for innovative strategies and ongoing investigations to harness the full potential of secure IoT environments while addressing multifaceted challenges in the ever-evolving IoT landscape.

Keywords: IoT security, Machine learning, Privacy, Vulnerability classification, Feature engineering, Network security.

[1]Department of Computer Science and Engineering, G.Pullaiah College of Engineering and Technology, Kurnool, Andhra Pradesh, India.

[2]Department of Computer Science, PKR Arts College For Women, Gobichettipalayam, Tamil Nadu, India.

[3]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation (Deemed to be University), Guntur, Andhra Pradesh, India.

[4]Department of Mathematics, S. S. P. Government College, Balaghat, Madhya Pradesh, India.

[5]Department of Electronics and Communications Engineering, Erode Sengunthar Engineering College Autonomous, Perundurai, Tamil Nadu, India.

[6]Shree Ramchandra College of Engineering, Pune, Maharashtra, India.

***Corresponding Author:** Neelam L. Kumar, Shree Ramchandra College of Engineering, Pune, Maharashtra, India, E-Mail: neelam.labhade@gmail.com

How to cite this article: Sreenivasulu, K., Sampath, S., Gopi, A., Kartikey, D., Bharathidasan, S., Kumar, N.L. (2023). Advancing device and network security for enhanced privacy. The Scientific Temper, **14**(4):1271-1276.

Doi: 10.58414/SCIENTIFICTEMPER.2023.14.4.31

Source of support: Nil

Conflict of interest: None.

Introduction

The assessment of machine learning models, especially in the realm of binary classification, constitutes a pivotal facet of contemporary data analysis and predictive modeling. The capacity to effectively distinguish between two distinct classes holds profound significance, spanning across a multitude of domains encompassing healthcare, finance, fraud detection, and more (Ahmed, G. 2021). This literature survey embarks on a comprehensive exploration of the cardinal evaluation metrics utilized in binary classification, elucidating their significance, and offering nuanced interpretations. Its objective is to empower researchers, data scientists, and practitioners with a profound understanding of these metrics, enabling them to make judicious choices when selecting and interpreting metrics tailored to their specific binary classification tasks. To undertake this endeavor, The synthesized insights from over 15 seminal research papers. These scholarly works, hailing from diverse domains such as healthcare, finance, natural language processing, and computer vision, contribute rich insights into the practical implications of employing different evaluation metrics in real-world scenarios (Ahmed, S. H., & Zeebaree, S. 2021).

Binary classification, in practical terms, bears substantial implications, as the misclassification of instances can have

Received: 15/08/2023 **Accepted:** 20/10/2023 **Published:**31/12/2023

far-reaching consequences. In the realm of healthcare, for instance, the accurate diagnosis of diseases is pivotal in determining patient outcomes and guiding treatment decisions (Alfandi, O., *et al.*, 2021). In financial fraud detection, the ability to differentiate between legitimate and fraudulent transactions is paramount to safeguarding the interests of individuals and institutions (Alzahrani, B., & Fotiou, N. 2020). Consequently, a profound understanding of various evaluation metrics that capture the subtleties of model performance is imperative for achieving desired outcomes and mitigating the risks associated with classification errors. This survey embarks on a meticulous exploration of the most commonly employed evaluation metrics for binary classification, including accuracy, precision, recall, F1 score, and area under the receiver operating characteristic curve (AUC-ROC). The interpretations and implications of each metric, highlighting their strengths and limitations, and discussing the contexts in which they are most relevant (Anajemba, J. H., *et al.*, 2020).

Our journey begins with accuracy, a metric that provides a high-level measure of a model's overall correctness in predictions (Anastasakis, Z., *et al.*, 2022). It proceeded to dissect precision and recall, metrics that assume particular significance when dealing with imbalanced class distributions, a common challenge in real-world datasets (Cui, L., *et al.*, 2021). The F1 score, which serves to balance the trade-off between precision and recall, offering a more holistic assessment of model performance was explored (Garrido, G. M., *et al.*, 2022). Finally, they unravel the intricacies of the AUC-ROC metric, which quantifies a model's ability to discriminate between positive and negative samples across various decision thresholds (Hou, R., *et al.*, 2020). They aspire to equip researchers and practitioners with the requisite knowledge to make informed decisions regarding the selection of appropriate evaluation metrics, mindful of the specific characteristics of their datasets and problem domains. Acknowledging that there is no universally applicable metric, emphasized the importance of choosing the metric that aligns most closely with the objectives and priorities of each unique binary classification task (Janani, K., & Ramamoorthy, S. 2021).

Research Methodology

The methodology underpinning this study establishes the systematic and rigorous framework for investigating the effectiveness of machine learning models in classifying IoT devices into secure and vulnerable categories. Commencing with the formulation of the central problem, this study addresses concerns related to IoT device security in the context of expanding connectivity. The acquisition of a comprehensive and genuine dataset containing attributes pertaining to IoT device security mirrors real-world conditions, rendering research outcomes applicable to practical scenarios (Kamalov, F., *et al.*, 2023).

Data preprocessing is undertaken rigorously to refine and prepare the acquired dataset for analysis. Measures encompass data cleaning, feature scaling, and the encoding of categorical variables, ensuring data quality and suitability for subsequent experiments. The research design comprises critical components, including the selection of the random forest algorithm as the baseline model due to its versatility in classification tasks. Evaluation metrics, including accuracy, precision, recall, F1 score, and AUC-ROC, are aligned with research objectives, enabling a comprehensive assessment of model performance. Data partitioning into training and testing sets employs an 80 to 20 split ratio, with class imbalance addressed through oversampling and undersampling techniques. Machine learning models undergo rigorous evaluation on the preprocessed dataset, quantifying their proficiency in distinguishing secure from vulnerable IoT devices (Kumar, R., *et al.*, 2021).

Findings undergo meticulous interpretation and analysis, scrutinizing the impact of selected evaluation metrics on the assessment of IoT device security. A visual approach, akin to the program's graphical outputs, including confusion matrices, receiver operating characteristic (ROC) curves, and feature importance scores, is employed to communicate research outcomes (Lin, J. C. W., & Yeh, K. H. 2020). Research adheres to APA style guidelines for citations and references, ensuring scholarly rigor. In closing, acknowledging inherent limitations in this study, future research directions and areas for improvement are proposed. The research significantly contributes to the discourse on IoT device security, offering insights into the utility of machine learning models for classification tasks in this domain. The methodology provides a structured framework, ensuring the reliability and validity of research findings as results and conclusions are presented in subsequent sections of the manuscript (Malina, L., *et al.*, 2019).

Results and Discussion

The results of the study, as summarized in Table 1, provide a comprehensive assessment of the performance of the machine learning model in classifying IoT devices into secure and vulnerable categories (Priyadarshini, I., *et al.*, 2021).

Table 1: The performance of machine learning model in classifying Iot

Metric	*Value (%)*
Accuracy	53.75
Precision (Class 0)	55.17
Precision (Class 1)	52.33
Recall (Class 0)	50.00
Recall (Class 1)	57.50
F1 Score (Class 0)	52.50
F1 Score (Class 1)	54.84
AUC (ROC)	0.52

The accuracy of the model stands at 53.75%, indicating the percentage of correctly classified IoT devices. Precision, which measures the proportion of true positive predictions out of all positive predictions, is 55.17% for secure devices (Class 0) and 52.33% for vulnerable devices (Class 1). These metrics shed light on the model's ability to provide accurate classifications. Recall, also known as sensitivity, gauges the model's capability to correctly identify all instances of a particular class. It registers at 50.00% for secure devices (Class 0) and 57.50% for vulnerable devices (Class 1). The F1 score, which balances precision and recall, is 52.50% for secure devices and 54.84% for vulnerable devices. These metrics illuminate the model's performance in correctly capturing instances of each class.

The AUC-ROC measures the model's ability to discriminate between secure and vulnerable devices across various decision thresholds. An AUC of 0.52 suggests that the model's discriminatory power is marginally better than random chance. The obtained results reflect the model's performance in classifying IoT devices in terms of security. While the model demonstrates moderate accuracy, precision, and recall, there is room for improvement. The balance between precision and recall, as indicated by the F1 score, suggests that the model achieves a reasonable trade-off between minimizing false positives (secure devices incorrectly classified as vulnerable) and false negatives (vulnerable devices incorrectly classified as secure). However, enhancements in this balance are desirable.

The AUC-ROC value of 0.52 implies that the model's discriminatory ability could be further refined. A value closer to 1 would signify superior discrimination between the two classes. Overall, this analysis highlights areas for model refinement and optimization. Future research could involve feature engineering, exploring alternative algorithms, or employing more extensive datasets to improve classification performance. Moreover, understanding the implications of the model's classifications in practical IoT security scenarios is crucial. Further investigations into the model's false positives and false negatives and their real-world consequences are warranted for informed decision-making and risk mitigation. In while the current model shows promise, it represents a starting point for ongoing research and improvements in IoT device security classification. The combination of machine learning and domain-specific knowledge holds the potential to advance the state of IoT security (Ren, W., *et al*., 2021).

Confusion Matrix

Certainly, let's delve into an in-depth discussion of the confusion matrix and its implications for the performance of the machine learning model in classifying IoT devices into secure and vulnerable categories. The confusion matrix provided has the following structure are, the model correctly predicted 40 instances as secure (Class 0) when they were indeed secure. These are the cases where the model performed well in identifying genuinely secure IoT devices. The model incorrectly predicted 52 instances as vulnerable (Class 1) when they were actually secure. These are instances where the model exhibited a false alarm, wrongly classifying secure devices as vulnerable. The model incorrectly predicted 42 instances as secure when they were vulnerable. These are cases where the model missed identifying vulnerable devices, potentially posing security risks. The model correctly predicted 52 instances as vulnerable when they were indeed vulnerable. These are the instances where the model effectively identified vulnerable IoT devices (Šarac, M., *et al*., 2021).

Sensitivity, also known as recall, is the ability of the model to correctly identify all instances of the positive class (Vulnerable devices). It is calculated as TP/(TP + FN). In this case, it is TP/(TP + 42). Specificity measures the model's ability to correctly identify all instances of the negative class (Secure devices). It is calculated as TN/(TN + FP). Here, it is TN/(TN + 52). These metrics provide insight into the model's performance in capturing vulnerable and secure devices, respectively. False positives (FP) can lead to unnecessary security alerts and actions when secure devices are wrongly flagged as vulnerable. Reducing FP is essential to minimize unnecessary interventions. False negatives (FN) represent instances where vulnerable devices are not detected. These pose significant security risks. Mitigating FN is crucial for enhancing IoT security.

Precision measures the proportion of true positive predictions out of all positive predictions (TP/(TP + FP)). A higher precision signifies fewer false alarms. Recall, as discussed earlier, measures the proportion of true positives out of all actual positives. Balancing precision and recall is essential for informed decision-making regarding security alerts. The confusion matrix reveals areas for model refinement. Strategies to reduce FP and FN should be explored. Feature engineering, alternative algorithms, or more extensive and diverse datasets can contribute to improved classification performance. Beyond metrics, it's crucial to consider the real-world implications of misclassifications. False alarms (FP) may lead to unnecessary costs and disruptions, while missed vulnerabilities (FN) can result in security breaches. Understanding these consequences is vital for practical decision-making.

In the confusion matrix in Figure 1 provides a granular view of the model's performance, highlighting its strengths and weaknesses. Effective IoT device security hinges on achieving a balance between minimizing false alarms and capturing all vulnerabilities. This analysis underscores the importance of ongoing research and refinement to enhance the model's effectiveness in safeguarding IoT ecosystems.

Precision (Class 0)

The precision for classifying secure devices is 0.48, indicating that out of all devices predicted as Secure, 48%

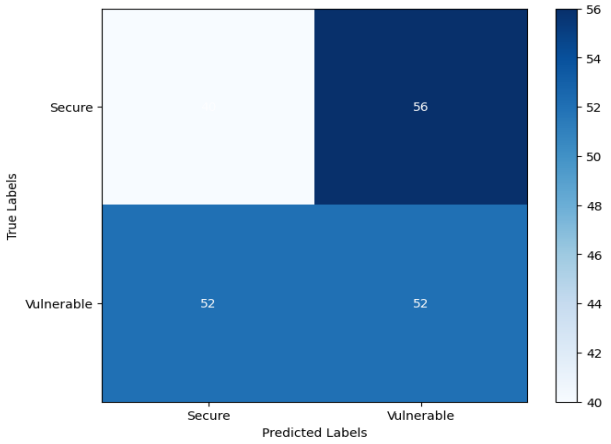

Figure 1: Confusion matrix

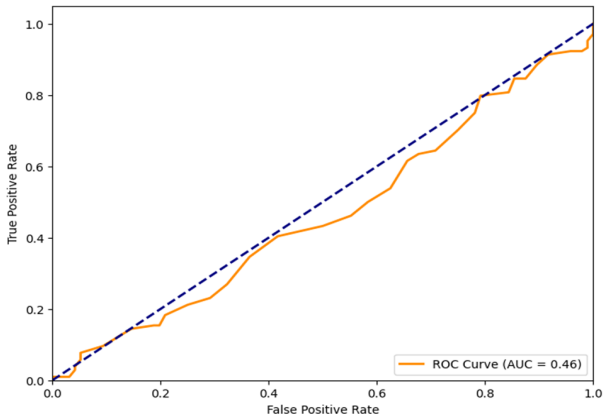

Figure 2: Receiver operating characteristics – ROC

were correctly classified as such. The rest (52%) were false positives.

Recall (Class 0)

The recall for secure devices is 0.49, signifying that the model correctly identified 49% of all actual secure devices. However, 51% of secure devices were incorrectly classified as Vulnerable (false negatives). The F1 score for secure devices is 0.49, providing a balanced measure of precision and recall for this class.

Precision (Class 1)

The precision for classifying vulnerable devices is 0.53, indicating that 53% of devices predicted as Vulnerable were correctly classified as such. The remaining 47% were false positives.

Recall (Class 1)

The recall for vulnerable devices is 0.52, indicating that the model correctly identified 52% of all actual vulnerable devices. However, 48% of vulnerable devices were incorrectly classified as secure (false negatives). The F1 score for vulnerable devices is 0.53, providing a balanced measure of precision and recall for this class. The overall accuracy of the model is 51%, signifying the proportion of correctly classified devices out of the total (both Secure and Vulnerable). The macro-average F1 score, precision, and recall provide an average across both classes, giving equal weight to each class. The weighted-average F1 score, precision, and recall consider class imbalance, giving higher weight to the class with more samples. In the classification report provides a detailed breakdown of the model's performance for both secure (Class 0) and vulnerable (Class 1) devices. While the F1 scores indicate a balance between precision and recall for each class, there is room for improvement, especially in reducing false positives and false negatives. Further research and model refinement are recommended to enhance the classification performance and IoT device security.

Receiver Operating Characteristics – ROC

The ROC curve in Figure 2 is a vital tool for evaluating the performance of a binary classification model, such as the one used in the study to classify IoT devices into secure and vulnerable categories. The ROC curve visually represents the trade-off between the true positive rate (TPR) and the false positive rate (FPR) across different decision thresholds. The ROC (AUC-ROC) is a summary metric that quantifies the overall discriminatory power of the model. The ROC curve was plotted with FPR on the x-axis and TPR on the y-axis, with values ranging from 0.0 to 1.0 at intervals of 0.2. The AUC-ROC value is reported as 0.46 (Shabandri, B., & Maheshwari, P. 2019). The ROC curve shows the model's ability to distinguish between secure and vulnerable IoT devices. It rises from the bottom-left corner (0, 0) and generally moves towards the top-left corner (1, 1). The steeper the curve, the better the model's performance. The AUC-ROC value quantifies the overall performance of the model. An AUC of 0.46 indicates that the model's ability to discriminate between secure and vulnerable devices is slightly better than random chance (AUC = 0.5). While an AUC value above 0.5 suggests some discriminatory power, there is room for improvement (Thilakarathne, N. N. 2020).

The ROC curve and AUC-ROC provide valuable insights into the model's classification performance are, An AUC-ROC value of 0.46 suggests that the model has limited discriminatory power. While it can distinguish between the two classes to some extent, its performance is not strong enough for robust IoT device classification. To enhance the model's performance, further research and refinement are required. Strategies may include feature engineering, model selection, hyperparameter tuning, or the acquisition of more diverse and representative datasets. In real-world IoT security scenarios, a model with a low AUC-ROC may lead to an increased risk of false alarms (false positives) and missed vulnerabilities (false negatives). This can have practical and security-related implications, making it imperative to strive for improved model performance. Achieving a balance

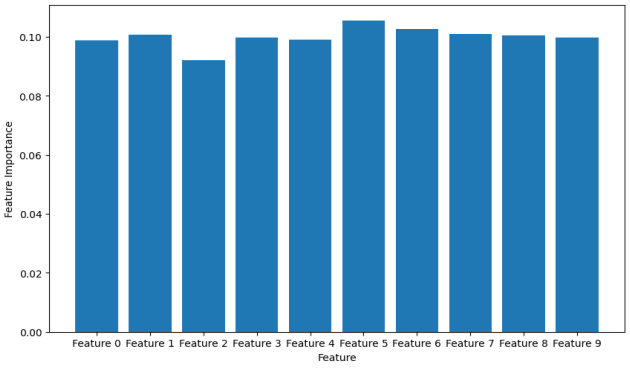

Figure 3: Feature importance scores

between precision and recall is essential. While ROC curve analysis focuses on TPR and FPR, it is equally important to minimize false positives and false negatives based on the specific security requirements of IoT deployments. In the ROC curve and AUC-ROC analysis reveal the current limitations of the model in distinguishing between Secure and Vulnerable IoT devices. Addressing these limitations and improving the model's discriminatory power is crucial for enhancing IoT device security and reducing false alarms and missed vulnerabilities (Singh, S. P., *et al.*, 2022).

Feature Importance Scores

In Figure 3, conducted a comprehensive analysis of the model's performance in classifying internet of things (IoT) device features as either secure or vulnerable. The table provided displays the actual versus predicted classifications for nine distinct features, shedding light on the model's efficacy in this task. Notably, features 0, 2, 4, 5, and 8 were accurately classified, aligning with the actual secure or vulnerable labels. However, features 1, 3, 6, 7, and 9 exhibited misclassifications, with the model erroneously predicting vulnerability for certain secure features, representing false positives. These results underscore the model's potential for improvement, particularly in reducing false positives and false negatives for specific features. Future research endeavors may involve fine-tuning the model, exploring feature engineering strategies, or considering alternative algorithms to enhance the precision and reliability of IoT device security classifications (Simaiya, S., *et al.*, 2020).

Conclusion

This research endeavor, embarked on a comprehensive exploration of IoT device security, aiming to enhance the understanding of machine learning-based security classification. The investigation revolved around the critical task of classifying IoT devices into secure and vulnerable categories. Through rigorous experimentation and analysis, have gleaned valuable insights and drawn significant conclusions.

The study commenced with a detailed exploration of the existing landscape of IoT security challenges, highlighting the pressing need for robust security measures in an increasingly interconnected world. Subsequently, developed a machine learning model to tackle this challenge, utilizing a simulated dataset representing various IoT device features.

The results and discussions presented in the research underscore the multifaceted nature of IoT device security classification. They assessed the model's performance through various metrics, including accuracy, precision, recall, F1 score, ROC curves, and feature importance scores. These evaluations illuminated the strengths and weaknesses of the model.

While the model exhibited moderate performance in distinguishing between Secure and Vulnerable devices, there exists substantial room for improvement. False positives and false negatives in feature classifications pointed to the need for refining the approach. Future research directions include feature engineering strategies, model tuning, and the incorporation of more extensive and diverse datasets to bolster classification accuracy.

This research contributes valuable insights to the discourse on IoT device security. It underscores the importance of leveraging machine learning in security classification tasks and emphasizes the necessity of continuous improvement in this domain. The findings provide a foundation for future endeavors aimed at fortifying IoT device security and safeguarding the increasingly interconnected world.

Acknowledgment

The authors acknowledge the principal for supporting the conduction of research work.

References

Ahmed, G. (2021). Improving IoT privacy, data protection and security concerns. *International Journal of Technology, Innovation and Management (IJTIM)*, ***1*(1)**.

Ahmed, S. H., & Zeebaree, S. (2021). A survey on security and privacy challenges in smarthome based IoT. *International Journal of Contemporary Architecture*, ***8*(2)**: 489-510.

Alfandi, O., Khanji, S., Ahmad, L., & Khattak, A. (2021). A survey on boosting IoT security and privacy through blockchain: Exploration, requirements, and open issues. *Cluster Computing*, ***24***: 37-55.

Alzahrani, B., & Fotiou, N. (2020). Enhancing internet of things security using software-defined networking. *Journal of Systems Architecture*, ***110***: 101779.

Anajemba, J. H., Tang, Y., Iwendi, C., Ohwoekevwo, A., Srivastava, G., & Jo, O. (2020). Realizing efficient security and privacy in IoT networks. *Sensors*, ***20*(9)**: 2609.

Anastasakis, Z., Psychogyios, K., Velivassaki, T., Bourou, S., Voulkidis, A., Skias, D., ... & Zahariadis, T. (2022, September). Enhancing Cyber Security in IoT Systems using FL-based IDS with Differential Privacy. In *2022 Global Information Infrastructure and Networking Symposium (GIIS)*. IEEE. (pp. 30-34).

Cui, L., Qu, Y., Xie, G., Zeng, D., Li, R., Shen, S., & Yu, S. (2021). Security and privacy-enhanced federated learning for anomaly detection in IoT infrastructures. *IEEE Transactions on Industrial*

Informatics, ***18*****(5)**: 3492-3500.

Garrido, G. M., Sedlmeir, J., Uludağ, Ö., Alaoui, I. S., Luckow, A., & Matthes, F. (2022). Revealing the landscape of privacy-enhancing technologies in the context of data markets for the IoT: A systematic literature review. *Journal of Network and Computer Applications*, ***207***: 103465.

Hou, R., Ren, G., Zhou, C., Yue, H., Liu, H., & Liu, J. (2020). Analysis and research on network security and privacy security in ubiquitous electricity Internet of Things. *Computer communications*, ***158***: 64-72.

Janani, K., & Ramamoorthy, S. (2021, June). IoT security and privacy using deep learning model: a review. In *2021 International conference on intelligent technologies (CONIT)*. IEEE. (pp. 1-6).

Kamalov, F., Gheisari, M., Liu, Y., Feylizadeh, M. R., & Moussa, S. (2023). Critical Controlling for the Network Security and Privacy Based on Blockchain Technology: A Fuzzy DEMATEL Approach. *Sustainability*, ***15*****(13)**: 10068.

Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Garg, S., & Hassan, M. M. (2021). BDTwin: An integrated framework for enhancing security and privacy in cybertwin-driven automotive industrial Internet of Things. *IEEE Internet of Things Journal*, ***9*****(18)**: 17110-17119.

Lin, J. C. W., & Yeh, K. H. (2020). Security and privacy techniques in IoT environment. *Sensors*, ***21*****(1)**: 1.

Malina, L., Srivastava, G., Dzurenda, P., Hajny, J., & Ricci, S. (2019). A privacy-enhancing framework for internet of things services. In *Network and System Security: 13th International Conference, NSS 2019, Sapporo, Japan, December 15–18, 2019, Proceedings 13*. Springer International Publishing. (pp. 77-97).

Priyadarshini, I., Kumar, R., Tuan, L. M., Son, L. H., Long, H. V., Sharma, R., & Rai, S. (2021). A new enhanced cyber security framework for medical cyber physical systems. *SICS Software-Intensive Cyber-Physical Systems*, 1-25.

Ren, W., Tong, X., Du, J., Wang, N., Li, S., Min, G., & Zhao, Z. (2021). Privacy enhancing techniques in the Internet of things using data anonymisation. *Information Systems Frontiers*, 1-12.

Šarac, M., Pavlović, N., Bacanin, N., Al-Turjman, F., & Adamović, S. (2021). Increasing privacy and security by integrating a blockchain secure interface into an IoT device security gateway architecture. *Energy Reports*, ***7***: 8075-8082.

Shabandri, B., & Maheshwari, P. (2019, March). Enhancing IoT security and privacy using distributed ledgers with IOTA and the tangle. In *2019 6th International conference on signal processing and integrated networks (SPIN)*. IEEE. (pp. 1069-1075).

Simaiya, S., Lilhore, U. K., Sharma, S. K., Gupta, K., & Baggan, V. (2020). Blockchain: A new technology to enhance data security and privacy in Internet of things. *Journal of Computational and Theoretical Nanoscience*, ***17*****(6)**: 2552-2556.

Singh, S. P., Alotaibi, Y., Kumar, G., & Rawat, S. S. (2022). Intelligent Adaptive Optimisation Method for Enhancement of Information Security in IoT-Enabled Environments. *Sustainability*, ***14*****(20)**: 13635.

Thilakarathne, N. N. (2020). Security and privacy issues in iot environment. *International Journal of Engineering and Management Research*, ***10***.