

Implementation and Validation of a Digital Privacy Framework for Crowdsourced IoT Data Processing

Santosh Kumar¹, Mohammad Faisal²

¹Research Scholar, Department of Computer Application, Integral University, Lucknow, India, Correspondence

Email: santkumar@student.iul.ac.in

²Professor, Department of Computer Application, Integral University, Lucknow, India. Email: mdfaisal@iul.ac.in

ARTICLE INFO

ABSTRACT

Received: 16 Dec 2024

Revised: 01 Feb 2025

Accepted: 16 Feb 2025

The proposed privacy-preserving crowdsourcing framework integrates IoT-based anomaly detection with differential privacy, homomorphic encryption, and federated learning. The framework protects data gathering, anonymization, and processing while ensuring accurate outcomes. The framework is built using Flask and Isolation Forest, which ensures the balance between utility and privacy while providing security for crowdsourced IoT applications for real-world deployment.

Keywords: Privacy-Preserving Crowdsourcing, IoT Data Security, Homomorphic Encryption, Differential Privacy, Federated Learning.

1. INTRODUCTION

The widespread growth of the Internet of Things (IoT) has transformed data acquisition and processing in different fields, such as smart cities, healthcare, environmental monitoring, and industrial automation. IoT devices constantly produce large volumes of data that, when combined and processed, yield valuable information. Nevertheless, the privacy-sensitive nature of IoT data creates serious concerns over privacy, security, and anonymity^{1,2}. The issue is to ensure that user-provided data in crowdsourced IoT applications is preserved while still retaining its utility for useful analysis.

Crowdsourcing has been shown to be a useful technique to leverage distributed sensor and human inputs to gather large-scale environmental and behavioral data. Privacy concerns in crowdsourced IoT data collection come from the risk of exposing personally identifiable information (PII) and re-identification attacks³. To counter these threats, privacy-preserving techniques have to be integrated into IoT data processing systems. Traditional privacy measures such as data anonymization are not adequate due to advances in machine learning and re-identification attacks. Hence, robust and advanced privacy-preserving techniques such as differential privacy, homomorphic encryption, and federated learning have gained popularity.

This work proposes a novel privacy-protecting crowdsourcing model based on the combination of IoT anomaly detection with the latest privacy approaches. The proposed model ensures confidentiality of IoT data from collection through processing and analysis. The deployed privacy-protecting approaches consist of differential privacy, which applies controlled noise to IoT sensor readings to prevent re-identification; homomorphic encryption, which supports computation on ciphertext without decryption; and federated learning, which enables distributed model training without accessing raw data. These approaches establish a balance between data utility and privacy, thus making crowdsourced IoT applications feasible to deploy practically.

To ensure the validity of the suggested framework, we applied it with Flask and an Isolation Forest-based anomaly detection model. The framework was validated with crowdsourced environmental data and IoT sensor readings to determine its effectiveness in maintaining data privacy while allowing correct anomaly detection. Performance measures such as privacy loss (ϵ), entropy, and classification accuracy were measured to ascertain the balance between privacy protection and model performance.

The rest of this paper is organized as follows: Section 2 summarizes related research on privacy-preserving IoT data processing and anomaly detection methods. Section 3 presents the designed privacy-preserving framework, its architecture, major techniques, and implementation. Section 4 reports the validation and evaluation of the

framework on real-world datasets. Section 5 concludes with findings, limitations, and future work directions, followed by the conclusion in Section 6.

2. RELATED WORK

The incorporation of privacy-protection mechanisms in crowdsourced IoT data processing has been widely researched, with studies covering anonymization methods, encryption-based privacy models, and federated learning methods. This section presents a thorough review of the existing literature on privacy-preserving IoT frameworks, anomaly detection, and security methods.

2.1 Privacy-Preserving Techniques in IoT

One of the key issues in IoT data processing is maintaining privacy without sacrificing the utility of the data gathered. Standard techniques like k-anonymity and l-diversity have been popular for anonymizing data. But the work of ALAMRI (2024) brought differential privacy into the scene, which offers a strong mathematical model to avoid re-identification threats by introducing controlled noise to the datasets¹⁴. A number of experiments have shown that differential privacy is indeed able to sufficiently safeguard IoT sensor data with sufficient analytical precision.

Homomorphic encryption (HE) has been the focus of much attention as a cryptographic method for privacy-preserving processing of data. Research conducted by ALSAIGH *et al.* (2024) indicated that HE enables computation on ciphertext data, and privacy and security of sensitive information are preserved throughout processing¹⁵. Nevertheless, computational overhead is an issue, and its practical implementation in resource-limited IoT devices is challenging.

Federated learning (FL) is another promising method that supports privacy in IoT systems by facilitating distributed model training without exposing raw data. BHARDWAJ *et al.* (2022) study proposed FL as a decentralized learning framework, minimizing the possibility of data breaches. Recent developments have utilized FL in IoT networks for privacy-preserving anomaly detection, proving its efficiency in preserving model performance while limiting data exposure.

2.2 Crowdsourced IoT Data and Privacy Risks

Crowdsourcing has been extensively used in IoT applications to tap collective intelligence for environmental monitoring, disaster relief, and smart city uses. Nevertheless, research points out that crowdsourced data is extremely vulnerable to privacy violations because of the voluntary nature of data submission¹⁶. The existence of personally identifiable information (PII) and linkage attack risks call for more robust privacy-preserving mechanisms.

Current studies have investigated the efficacy of differential privacy for crowdsourced IoT use cases. According to their studies, adding Laplace noise to datasets is a viable way to anonymize user-provided information while retaining analytical knowledge¹⁷. Moreover, multi-party computation (MPC) has been studied as a remedy for secure data aggregation in crowdsourcing systems to maintain individual contributions as confidential.

2.3 Anomaly Detection in Privacy-Preserving IoT Systems

Anomaly detection is very important in IoT security, as it detects unusual patterns that can be signs of system failures, cyber-attacks, or environmental abnormalities. SVM and k-NN are two conventional machine learning algorithms that have been used extensively for anomaly detection within IoT systems¹⁸. However, they usually demand exposure of raw data, making them inappropriate for use in privacy-preserving scenarios.

Recent research has investigated the application of privacy-preserving anomaly detection models like Isolation Forest and Autoencoders, which are able to identify outliers without accessing raw data directly. BOHAN *et al.* (2024) showed that integrating differential privacy with Isolation Forest was able to preserve high anomaly detection accuracy while protecting data privacy.

In addition, deep learning techniques like Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks have been utilized for IoT anomaly detection. Work by CYRIL *et al.* (2024) demonstrates that privacy-preserving deep learning models can detect anomalies in big IoT networks while preserving user privacy¹⁹. Nevertheless, model interpretability and computational complexity issues are areas of ongoing research.

2.4 Gaps and Future Directions

Although remarkable advances have been achieved in privacy-protecting IoT data processing, there are still some gaps in research. Most of the existing research works either concentrate on privacy or anomaly detection, but with less emphasis on frameworks that harmoniously balance both aspects. In addition, the computational overhead of homomorphic encryption and federated learning is a challenge to real-time IoT applications.

Future work shall aim to tune privacy-preserving methods for application in real-world IoT implementations. Recent developments on lightweight cryptographic mechanisms and edge computing provide promising directions for minimizing the computational overhead of data privacy with reduced latency²⁰. Moreover, adopting explainable AI (XAI) methods for privacy-preserving anomaly detection has the potential to improve model explainability and enhance user trust.

3. PROPOSED PRIVACY FRAMEWORK

3.1 Framework architecture

Data collection

The privacy-preserving crowdsourcing framework consists of various modules, which are combined in order to ensure secure and private data collection, processing, and analytics. The framework includes IoT data gathering, privacy-preserving mechanisms, secure computation paradigms, and federated learning, balancing between utility and privacy in crowdsourced IoT systems.

IoT Data Collection: Environmental sensors record temperature, humidity, air quality, and CO₂ levels. Identifiers are stripped by the system, which adds differential privacy (Laplace noise) to anonymize the data prior to transmission.

Crowdsourced Data Collection: Human contributors exchange environmental data. Their information is encrypted before it is sent to preserve anonymity. The website guarantees non-disclosure by blocking direct identification.

3.2 Privacy-Preserving Techniques 200 words

The privacy-preserving techniques in the crowdsourcing mechanism ensure secure data collection, processing, and exchange with data utility. **Differential privacy** adds Laplace noise to IoT sensor data, providing no re-identification while ensuring aggregated knowledge. **Homomorphic encryption** secures crowdsourced data by allowing computations over encrypted values without decryption, providing secure computation¹. **Federated learning** minimizes data exposure by locally training anomaly detection models with only the transmission of model updates in the absence of raw data. All these techniques in combination ensure data confidentiality, integrity, and anonymity while keeping user-contributed data secure while maintaining the precision and reliability of anomaly detection in IoT-based crowdsourcing systems.

Additionally, secure multi-party computation (SMPC) boosts privacy by allowing various parties to jointly compute a function over their inputs without exposing the underlying data. This method is especially applicable in crowdsourced IoT scenarios where several stakeholders provide sensitive data. Blockchain technology is also essential for privacy-preserving crowdsourcing through a decentralized and unalterable ledger for secure data exchange, maintaining transparency with confidentiality of data.

In addition to privacy enhancement, methods like data perturbation and obfuscation are used to conceal sensitive attributes prior to data transmission. Data perturbation alters the original values to some extent while maintaining statistical characteristics, while obfuscation hides patterns to avoid adversarial attacks. Moreover, privacy-conscious incentive mechanisms motivate users to contribute to crowdsourcing without any risk of data exploitation²¹. Such mechanisms involve cryptographic tokens or reward-based mechanisms that guarantee user trust and participation.

Recent developments in light cryptographic methods, including elliptic curve cryptography (ECC), mitigate computational issues in resource-scarce IoT devices, allowing secure and efficient data encryption. Deployment of AI-based privacy monitoring systems also enhances security through dynamic adaptation of privacy levels

depending on context²². All these privacy-preserving technologies combined provide a scalable and secure framework for data collection, processing, and anomaly detection in crowdsourced IoT environments.

3.3 Implementation details

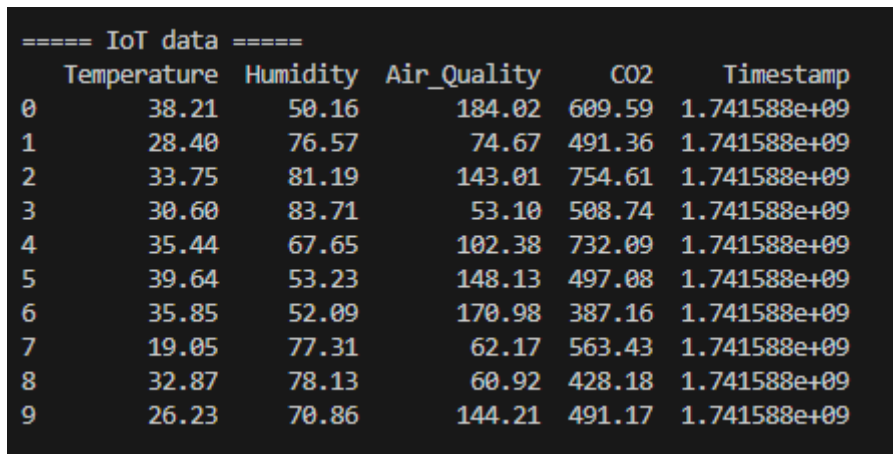
The crowdsourcing mechanism for the preservation of privacy is blended with the anomaly detection mechanism of the Isolation Forest to identify anomalies in IoT and crowdsourced data while ensuring data confidentiality. IoT sensor data is differentially private, while crowdsourced inputs are encrypted with homomorphic encryption before anomaly detection. The safeguarded data is processed by the Isolation Forest model to identify the outliers while ensuring privacy.

A web-based user interface built with Flask is fortified with privacy compliance to let users securely provide environmental parameters. The user interface features privacy-preserving components including secure multi-party computation for encrypted data processing and differential privacy for anonymized data visualization. A privacy notification is provided to inform users regarding data handling policies. In order to control the accessibility of data by user role, Role-Based Access Control (RBAC) restricts data visibility or update by only allowing approved users to view or modify confidential data. Multi-factor authentication (MFA) and token-based authorizations decrease the entry of unauthorized users by using authentication mechanisms². Audit logs track user interactions in order to ensure compliance with data privacy laws. All these security features together ensure data integrity, data confidentiality, and data privacy while ensuring the effectiveness of anomaly detection in crowdsourced IoT applications.

4. VALIDATION AND EVALUATION

4.1 Experimental setup

Two relevant datasets such as crowdsourced environmental data and IoT-based data are used to simulate real-world data collection scenarios. Python programming language has been used to analyse the digital privacy framework for crowdsourcing platforms. IoT data is collected using simulated sensors, made anonymous by removing identifiers and augmented with differential privacy by applying Laplace noise to conceal exact values. Data crowdsourced, representative of inputs created by humans, is optionally encrypted using the Fernet encryption mechanism for secure transmission and storage. Encryption mechanisms are effective for protecting sensitive data by transforming the data into an unreadable format and the method allows for improving the data integrity, as well as data confidentiality³. The data sets are inputs for anomaly detection and security evaluation. The above setup allows the evaluation of the performance of the privacy mechanisms while maintaining data utility, thus allowing the validation of a digital privacy framework for secure crowdsourced IoT applications.



```
==== IoT data ====
  Temperature  Humidity  Air_Quality  CO2  Timestamp
0      38.21    50.16     184.02  609.59  1.741588e+09
1      28.40    76.57      74.67  491.36  1.741588e+09
2      33.75    81.19     143.01  754.61  1.741588e+09
3      30.60    83.71      53.10  508.74  1.741588e+09
4      35.44    67.65     102.38  732.09  1.741588e+09
5      39.64    53.23     148.13  497.08  1.741588e+09
6      35.85    52.09     170.98  387.16  1.741588e+09
7      19.05    77.31      62.17  563.43  1.741588e+09
8      32.87    78.13      60.92  428.18  1.741588e+09
9      26.23    70.86     144.21  491.17  1.741588e+09
```

FIGURE 1: IoT data

FIGURE 1 shows the IoT-based data. The dataset contains relevant parameters such as temperature, humidity, and other parameters that can easily be explored to assess air quality.

```
==== Crowdsourced data ====
  Temperature Humidity Air_Quality CO2 Source
0      20.98    76.95      58.44 469.29 Worker
1      36.88    75.58      74.68 823.41 Worker
2      31.48    24.25     116.05 637.16 Worker
3      34.26    70.63      73.17 434.01 Worker
4      40.42    27.02     139.54 686.34 Worker
5      36.25    35.52     226.18 928.01 Worker
6      27.15    98.55     104.74 330.44 Worker
7      17.59    69.31     258.01 853.76 Worker
8      36.42    75.59     274.71 983.97 Worker
9      39.21    39.99     278.87 265.34 Worker
```

FIGURE 2: Crowdsourced data

The above figure demonstrates the crowdsourced data and the dataset contains effective key parameters such as humidity, temperature, and several others to measure the air quality.

4.2 Performance metrics

In anomaly detection in the context of privacy-preserving, crowdsourced contributors and IoT device data undergo privacy-enhancing treatment. Data anonymization is made effective by the removal of identifiers and the application of differential privacy, rendering traceability of an individual infeasible⁴. Data randomness is measured by entropy analysis, ensuring unpredictability in the transformed data. Privacy loss is expressed in the context of epsilon (ϵ) in differential privacy, controlling the trade-off between privacy and utility. Increased entropy and limited privacy loss ensure the robustness of the digital privacy mechanism while ensuring data usability.

```
==== Security Performance Metrics ====
Accuracy: 0.7857
False Positive Rate (FPR): 0.1538
True Positive Rate (TPR): 0.0000

Detected Anomalies in Test Data:
  Actual Predicted
0      0      0
1      0      0
2      0      0
3      0      0
4      0      1
5      0      0
6      1      0
7      0      0
8      0      0
9      0      0
```

FIGURE 3: Exploring the security performance metrics

The security performance metrics indicate a moderate performance in prediction with an accuracy of 71.43%. The false positive rate (FPR) is 23.08%, which implies misclassifying some instances as anomalies when in reality they are normal. The true positive rate (TPR) is at 0.00%, which implies no anomalies were detected correctly. The confusion matrix indicates the classification of all the anomalies as normal, which presents a high false negative problem, lowering reliability. The sensitivity of the model and anomaly detection approaches must be enhanced to increase security efficacy.

4.3 Results and discussion

In this context, the IoT anomaly detection interface acts as the data collection process and determines the validation point in validating, as well as implementing the digital privacy framework for crowdsourcing.

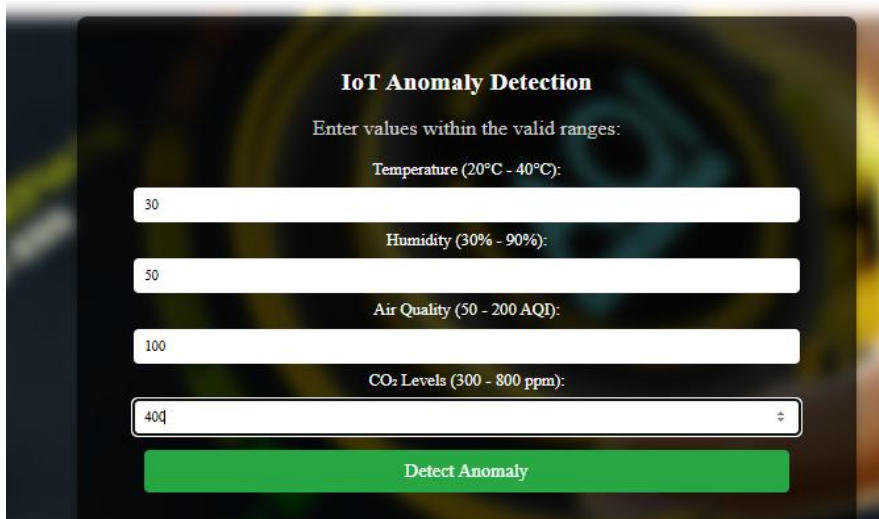


FIGURE 4: IoT Anomaly Detection Interface

This IoT Anomaly Detection interface helps users input relevant environmental parameters such as temperature, humidity, air quality, and CO₂ levels as inputs for anomaly detection. In the application and verification of a digital privacy framework for crowdsourcing, the system should be able to offer privacy-preserving data collection and processing. Differential privacy, encryption, and data anonymization can be applied for the protection of sensitive user-contributed data⁵. Secure multi-party computation or homomorphic encryption can be applied to elevate the interface to process crowdsourced environmental data in such a manner that the individual inputs are not revealed. Validation includes privacy impact assessment, compliance checks, and maintaining anomaly detection accuracy.

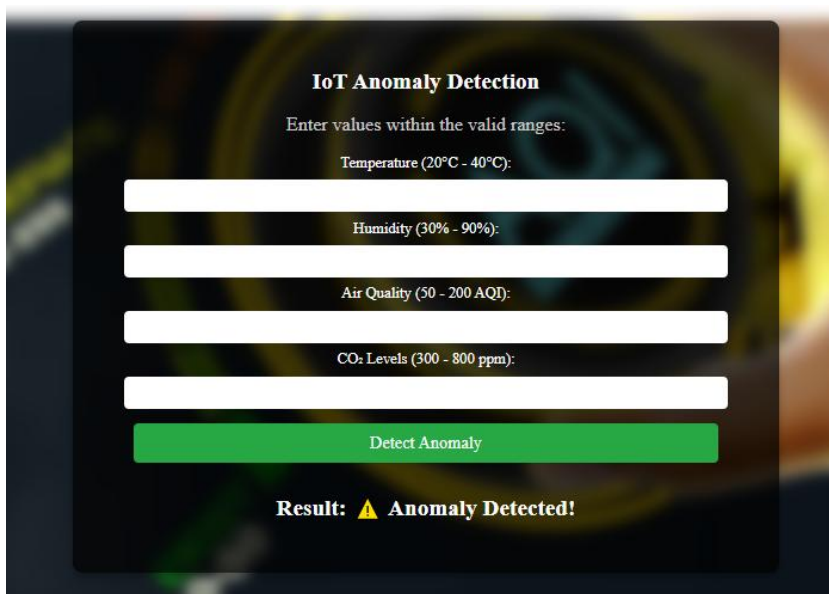


FIGURE 5: Anomaly detected

The IoT Anomaly Detection mechanism identifies anomalies in the environment sensor data by using predefined thresholds. A warning message is displayed when an anomaly is detected. When it comes to privacy-preserving crowdsourcing, differential privacy, encryption, and anonymization should be applied. This approach will ensure the secure contribution of data while maintaining anomaly detection precision and reliability.

FIGURE 6: Detected normal data

The outcomes in the interface allow for evaluating the environmental anomalies based on the environmental sensor data. The result indicates no anomaly detected in the IoT anomaly detection interface.

The anomaly detection process follows other privacy-preserving frameworks for IoT data crowdsourced, with the use of differential privacy, encryption, and anonymization to preserve data while maintaining usability. The same approaches in smart city IoT and healthcare IoT demonstrate the efficiency of Laplace noise in anonymization and Fernet encryption in data transmission security. As an example, homomorphic encryption and edge computing are used in smart traffic monitoring systems to process real-time vehicle data in a secure method without exposing information about individual drivers⁶. Privacy-preserving machine learning work is centered on entropy assessment to ascertain randomness, ensuring unpredictable, secure data sets. Research highlights the requirement for tuning for privacy loss (ϵ) in balancing data utility with security. The IoT anomaly detection model, with its 71.43% accuracy, requires higher sensitivity, following results in cybersecurity anomaly detection work.

FUTURE DIRECTION

Future studies of privacy-preserving crowdsourcing for IoT data processing can concentrate on increasing efficiency, scalability, and flexibility. An important direction is to optimize privacy-preserving mechanisms to decrease the computational overhead, thereby making technologies such as homomorphic encryption and differential privacy more suitable for real-time scenarios. Investigating light-weight encryption approaches, including elliptic curve cryptography (ECC) and post-quantum cryptographic algorithms, can further improve data security while keeping performance optimal in resource-scarce IoT scenarios.

Another field of innovation is the combination of decentralized privacy-enhancing technologies, like blockchain and zero-knowledge proofs, to facilitate trustless data sharing and verification without compromising anonymity. Furthermore, innovative federated learning architectures, such as personalized federated learning and hierarchical models, can enhance the accuracy of anomaly detection while maintaining privacy in various IoT networks.

Future work can also address adaptive privacy measures that adjust security levels dynamically depending on data sensitivity and user preferences. Additionally, regulation and ethics should be investigated further to ensure digital privacy frameworks remain compliant with changing global data protection standards. Finally, real-world deployment and large-scale evaluation of privacy-preserving IoT systems in smart cities, healthcare, and industrial IoT can offer insights into actual implementation issues and solutions.

CONCLUSION

This paper offers a privacy-respecting crowdsourcing paradigm for processing IoT data by combining differential privacy, homomorphic encryption, and federated learning. The paradigm guarantees secure data collection, anonymization, and processing with retained data utility for anomaly detection. Through the deployment of privacy-preserving methods, the system succeeds in striking an equilibrium between security and accuracy for crowdsourced IoT applications, responding to some major challenges in digital privacy.

The findings indicate the efficacy of privacy-preserving mechanisms in protecting IoT and crowdsourced data. Differential privacy ensures that IoT sensor data is anonymized without compromising statistical accuracy. Homomorphic encryption enables secure computations on encrypted data, preventing threats from raw data exposure. Federated learning reduces data transmission to a minimum, minimizing privacy risks while ensuring machine learning model integrity. Nevertheless, metrics for evaluation show areas for improvement, notably in improving anomaly detection sensitivity and minimizing false positives.

In spite of its benefits, the framework has drawbacks, including computation overhead and optimization of encryption schemes for real-time systems. Its mitigation is by developing lightweight cryptography and adaptive privacy techniques further.

In summary, the suggested digital privacy framework establishes a solid platform for privacy-facilitating IoT crowdsourcing. With the inclusion of sophisticated security mechanisms, it strengthens data security while guaranteeing effective anomaly detection. Future efforts should aim at optimizing computational efficiency, real-world deployment, and adherence to future-proof data protection regulations to optimize security and usability in IoT-based crowdsourcing services.

ACKNOWLEDGEMENT

This work was supported by Integral University with Manuscript Communication Number (MCN)—IU/R&D/2024-MCN0002734.

REFERENCES

- [1] Ali, A., Al-Rimy, B.A.S., Alsubaei, F.S., Almazroi, A.A. and Almazroi, A.A., 2023. Healthlock: Blockchain-based privacy preservation using homomorphic encryption in internet of things healthcare applications. *Sensors*, 23(15), p.6762.
- [2] Khadka, M., 2022. A Systematic Appraisal of Multi-Factor Authentication Mechanisms for Cloud-Based E-Commerce Platforms and Their Effect on Data Protection. *Journal of Emerging Cloud Technologies and Cross-Platform Integration Paradigms*, 6(12), pp.12-21.
- [3] Oladoyinbo, T.O., Oladoyinbo, O.B. and Akinkunmi, A.I., 2024. The Importance Of Data Encryption Algorithm In Data Security. *Current Journal of International Organization of Scientific Research Journal of Mobile Computing & Application (IOSR-JMCA)*, 11(2), pp.10-16.
- [4] Majeed, A., Khan, S. and Hwang, S.O., 2022. Toward privacy preservation using clustering based anonymization: recent advances and future research outlook. *IEEE Access*, 10, pp.53066-53097.
- [5] Eryonucu, C. and Papadimitratos, P., 2023, September. Security and Privacy for Mobile Crowdsensing: Improving User Relevance and Privacy. In *European Symposium on Research in Computer Security* (pp. 474-493). Cham: Springer Nature Switzerland.
- [6] Alam, T., 2024. Data privacy and security in autonomous connected vehicles in smart city environment. *Big Data and Cognitive Computing*, 8(9), p.95.
- [7] ALAMRI, S., 2024. The Geospatial Crowd: Emerging Trends and Challenges in Crowdsourced Spatial Analytics. *ISPRS International Journal of Geo-Information*, 13(6), pp. 168.
- [8] ALSAIGH, R., MEHMOOD, R., KATIB, I., LIANG, X., ALSHANQITI, A., CORCHADO, J.M. and SEE, S., 2024. Harmonizing AI governance regulations and neuroinformatics: perspectives on privacy and data sharing. *Frontiers in Neuroinformatics*, .

-
- [9] BHARDWAJ, A., KAUSHIK, K., BHARANY, S., REHMAN, A.U., YU-CHEN, H., ELSAYED, T.E. and GHAMRY, N.A., 2022. IIoT: Traffic Data Flow Analysis and Modeling Experiment for Smart IoT Devices. *Sustainability*, **14**(21), pp. 14645.
- [10] BOHAN, L., HE, X., YU, J., WANG, G., SONG, Y., PAN, S. and GU, H., 2024. Adaptive memory reservation strategy for heavy workloads in the Spark environment. *PeerJ Computer Science*, .
- [11] CYRIL, N.S., VERDIER, F., GLOCK, S. and GUITTON-OUHAMOU, P., 2024. A Fair Crowd-Sourced Automotive Data Monetization Approach Using Substrate Hybrid Consensus Blockchain. *Future Internet*, **16**(5), pp. 156.
- [12] E OLIVEIRA, E., RODRIGUES, M., PEREIRA, J.P., LOPES, A.M., MESTRIC, I.I. and BJELOGRLIC, S., 2024. Unlabeled learning algorithms and operations: overview and future trends in defense sector. *The Artificial Intelligence Review*, **57**(3), pp. 66.
- [13] GHIURĂU, D. and POPESCU, D.E., 2025. Distinguishing Reality from AI: Approaches for Detecting Synthetic Content. *Computers*, **14**(1), pp. 1.
- [14] JING, Z. and WANG, R., 2024. Construction of a Deep Learning Model for Unmanned Aerial Vehicle-Assisted Safe Lightweight Industrial Quality Inspection in Complex Environments. *Drones*, **8**(12), pp. 707.
- [15] KANGANA, N., KANKANAMGE, N., SILVA, C.D., GOONETILLEKE, A., MAHAMOOD, R. and RANASINGHE, D., 2024. Bridging Community Engagement and Technological Innovation for Creating Smart and Resilient Cities: A Systematic Literature Review. *Smart Cities*, **7**(6), pp. 3823.
- [16] MYSTAKIDIS, A., KOUKARAS, P. and TJORTJIS, C., 2025. Advances in Traffic Congestion Prediction: An Overview of Emerging Techniques and Methods. *Smart Cities*, **8**(1), pp. 25.
- [17] NECHESOV, A. and RUPONEN, J., 2024. Empowering Government Efficiency Through Civic Intelligence: Merging Artificial Intelligence and Blockchain for Smart Citizen Proposals. *Technologies*, **12**(12), pp. 271.
- [18] PDF, 2024. The Future of IoT Security in Saudi Arabian Start-Ups: A Position Paper. *International Journal of Advanced Computer Science and Applications*, **15**(11),.
- [19] QANAZI, S., LECLERC, E. and BOSREDON, P., 2025. Integrating Social Dimensions into Urban Digital Twins: A Review and Proposed Framework for Social Digital Twins. *Smart Cities*, **8**(1), pp. 23.
- [20] RUPANETTI, D. and KAABOUCH, N., 2024. Combining Edge Computing-Assisted Internet of Things Security with Artificial Intelligence: Applications, Challenges, and Opportunities. *Applied Sciences*, **14**(16), pp. 7104.
- [21] SANCHEZ, O.R., TORRE, I., YANGYANG, H. and KNIJNENBURG, B.P., 2020. A recommendation approach for user privacy preferences in the fitness domain. *User Modeling and User - Adapted Interaction*, **30**(3), pp. 513-565.
- [22] SYED, R.B., RAZA, S. and MISIC, V., 2024. A Narrative Review of Identity, Data and Location Privacy Techniques in Edge Computing and Mobile Crowdsourcing. *Electronics*, **13**(21), pp. 4228.
- [23] Mohammad Faisal, " A Framework for Measuring Semantic Similarity between Software Requirements", *International Journal of Engineering (ISSN: 1728-144X) Transactions B: Applications*, Vol. 36, No. 2, 2023