Section: Research Paper
ISSN 2063-5346

Privacy-Preserving Energy Efficient Task Scheduling

Manoj Kumar Malik[1*], Surajpal Chauhan[2 **], Dr. Sobinder Singh[3*]**

[1]*Department of IT, Maharaja Surajmal Institute of Technology*
[2]*Department of Computer Science, Maharaja Surajmal Institute*
[3]*Department of Applied Sciences, Maharaja Surajmal Institute of Technology*
*manojmalik@msit.in, **spchauhan@msijanakpuri.com , ***sobinder77@gmail.com

DOI: 10.48047/ecb/2023.12.si4.1685

Abstract

This entire study focused on the concept of energy efficiency privacy-preserving task scheduling in the context of computing systems. With the enhancement of data increasing applications are concerned with privacy. this article is pivotal to growing scheduling methods that preserve user privacy during balancing energy efficiency. Addressing these challenges the entire wide methodology is approached with energy efficiency optimization techniques that include privacy-preserving methods. This system aims to consider minimizing the consumption level of energy during protecting all sensitive user data that scheduling task decisions. This study also includes the final decision on emphasizing the significance of energy efficiency and privacy in algorithms for emerging task scheduling of computing systems.

Keywords

Privacy-preserving, Energy efficiency, Task scheduling, Optimization, Privacy preservation, Energy consumption, Privacy-aware, Energy optimization, Differential privacy,Task consolidation

1. Introduction

This study introduction shows the summary of this privacy-preserving matter of energy efficiency in task scheduling. It focuses on developing requirements to balance privacy and energy efficiency in computer systems. This introduction highlights the associated challenges through reaching both objectives emphasizing and simultaneously signifying the context challenges. It outlines the entire limitations and approaches in this field and spots the phase for the presented methodology. This point also elaborates on the target of the article, which is growing energy efficiency system optimization through privacy-preserving techniques contributing and scheduling to more privacy-conscious and efficient computing techniques.

Section: Research Paper
ISSN 2063-5346

2. Privacy-Preserving Task Scheduling

Task scheduling of privacy-preserving follows the procedure of allocating efficiently technical works to preserve the computing system of data sensitivity (Tan et al. 2019). With the addition of increasing concerns and driven proliferation of all data, the scheduling algorithm wants to mention resource utilization and optimizing performance, to disregard the concerns through privacy. Moreover, in many formations, like finance, and healthcare, protecting privacy, and processing the personal data of users is the most important thing (Zhang and Zeng 2019). Privacy breaking can be the reason for data leakage, potential misuse, and unauthorized access to sensitive data.

Task Scheduling of privacy-preserving likes to blitz stability between user privacy and reaching energy efficiency. It includes the mechanisms and creating the scheduling algorithms which stave off sensitive information to computer resources through efficiently allocating (Yang et al. 2021). Many types of techniques could be employed to reach task scheduling of privacy-preserving. One encryption-based proposal method that is decrypted and encrypted by countenanced entities through a scheduling procedure.

3. Energy Efficiency in Task Scheduling

Task scheduling of energy efficiency mentions maximizing utilization to minimize and compute the energy while meeting consumption for task requirements. Through enhancing demand for environmental impact and calculating resources. Task scheduling of energy efficiency has become very pivotal including the computing cloud, concerning various domains, Internet of Things (IOT), and data centers applications (Chen et al. 2022). Algorithms of efficiency task scheduling refer to allotting available resources for tasks in an order that maximizes the energy savings or violating the constrained tasks without meeting halfway tasks. Many algorithms mention components like energy profiles, resource availability, task characteristics, and task dependencies of computing resources.

One proposal for task scheduling of energy efficiency is to consolidate tasks, where tasks are performed as a single scheduled resource, that try to reduce the entire energy consumption. After identifying tasks with suitable requirements and with the availability of resources that can lead the energy savings through resource fragmentation with perfect timing (Boopathi et al. 2023). Dynamic Voltage and Frequency Scaling (DVFC), is another technique used in the task scheduling of energy efficiency. It confirms the frequency and voltage of resource base computing work-loaded demand which reduces the energy consumption when periods have low intensity while keeping another idle avoiding overloaded resource.

4. Challenges in Privacy Energy Efficiency Task Scheduling

Energy efficiency in privacy-preserving for scheduling tasks poses many challenges that want to be presented to make sure a secure and effective operation. These challenges start with some lack of energy optimization, and privacy preservation with simultaneous considerations that frequently involve trade-offs and conflicting objectives (Wang et al. 2021). Here are some following key challenges,

- Trade-off and privacy utility: Stabilizing energy efficiency and privacy could be challenging as techniques of privacy-preserving like obfuscation and encryption, degrade system performance, and can introduce any substitute overheads.
- Privacy risk application: Measuring risks of privacy is associated with different types of complex scheduling decisions. Risks in privacy can be based on the involving sensitive data, specification of information, and the nature of tasks revealed at the time of scheduling.
- Privacy preferences and constraints: Different applications and users can have different constraints and preferences for privacy. Incorporating requirements through individual privacy into the scheduling process when confirming adds complexity to energy efficiency. Creating customizable and flexible models of privacy becomes important to assist privacy needs.
- Scalability: The algorithm of task scheduling in privacy-preserving large-scale systems should be handled in a scalable way. Prominent optimization and algorithm methods are needed to control privacy-preserving tasks and computation allocation associated with computational complexity.
- Mechanism design of privacy-preserving: Creating an effective design of mechanisms in privacy-preserving that combine the challenges of efficiency optimization without compromising the introducible procedure and scheduling process with uprightness.

Mentioning those challenges needs multidisciplinary research, combining scalable system design, methodological risk assessment, algorithms of energy optimization, and privacy-preserving methods (Wang et al. 2023). Facing those challenges, task scheduling of privacy-preserving energy could be a safeguarding, implemented, and effective computing system.

5. Existing Approaches for Privacy-Preserving Energy Efficiency Task Scheduling

Many existing addresses have been offered to mention scheduling the tasks through the energy efficiency of privacy-preservation in computing systems. Those addresses do not corporate with energy optimization and combined techniques of privacy-preserving. Here are some eminent approaches,

- Encrypted approaches: It is a generally used method for privacy-preserving. Existing addresses grasp encrypted strategies like multiparty secure compilation and holomorphic encryption to present encrypted data that remains sensitive and protected while scheduling procedures.

Section: Research Paper
ISSN 2063-5346

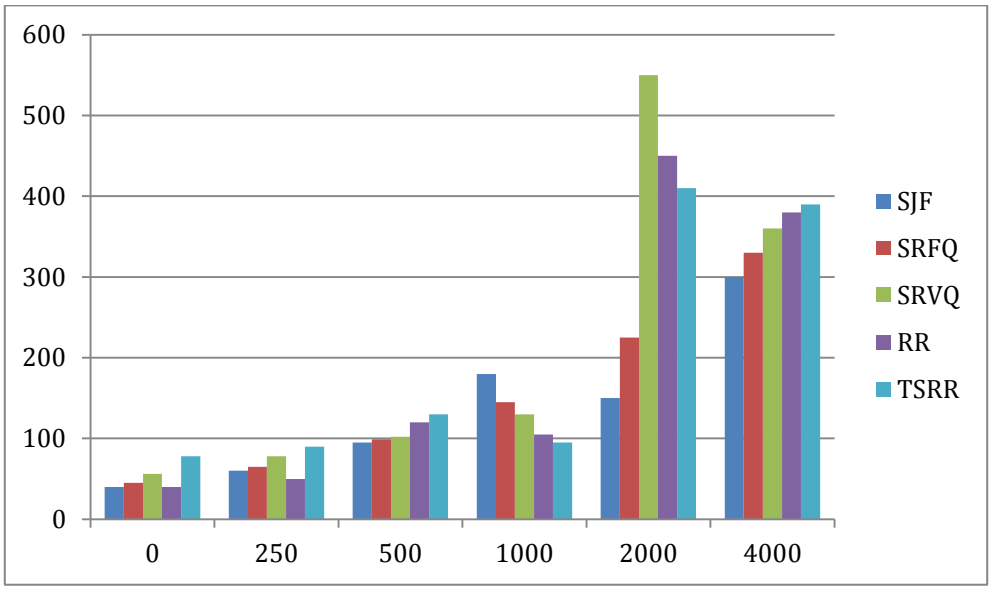


Figure: Task scheduling in cloud computing
(Source: Wang et al. 2023, P-23)

- Differential privacy: This method enlightened perturbations or noise to sanctioned privacy guarantees to task-based information. Those approaches modify a level of unpredictability for perfect task-scheduling thoughts (Zheng et al. 2022). Different types of privacy could be formatted to task assignments, utilization of data, and to protect user privacy.
- Privacy-preserving optimization: Some addresses can be highlighted to minimize the energy consumption of privacy-preserving methods when mentioning the privacy constraints. Those addresses calculate an optimization problem from a scheduling problem, where this energy efficiency is used as an optimized subject to the mentioned requirements of privacy energy efficiency.
- Task classification with privacy-preserving: Task classification methods could be used on their privacy needs as group tasks (Wang et al. 2021). These classifiers are always trained based on anonymzed and encrypted data to signify tasks to non-sensitive or privacy-sensitive categories. These categorizations could be used to consider perfect privacy-preserving finalizations in this task scheduling.
- Task scheduling: Existing addresses are also constraints incorporated directly through privacy-preserving to schedule the mentioned tasks algorithm. By accepting privacy to a task scheduling thoughts that are made with ensuring preservation as a primary constraint.

These approaches are needed to increase the adaptability, efficiency, and scalability of domains application and computing environments into energy efficiency through scheduling the tasks into the integration of privacy.

Section: Research Paper
ISSN 2063-5346

6. Proposed Methodology

This proposed methodology goals approach the challenges by growing the integrated structure from privacy-preserving of energy efficiency that includes energy efficiency techniques with privacy-preserving methods (Oskouei et al. 2021). Here are the following,

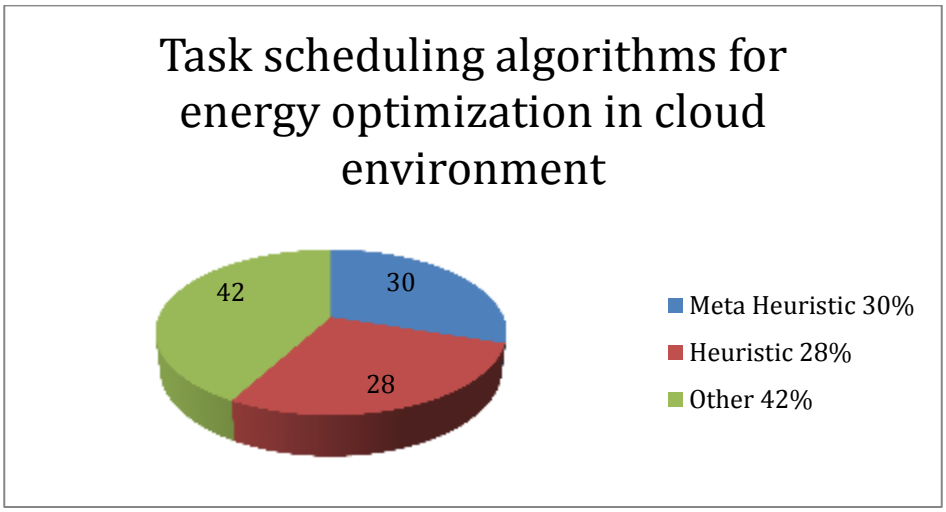
- Privacy risk assessment: This phase includes assessing the results that potentially breach, different scenarios scheduling, and quantifying the risks of privacy.
- Privacy-preserving techniques: This method can include differential privacy mechanisms and multiparty computation of secure methods. It also ensures that sensitive information is protected during taking the scheduling decision.
- Energy efficiency optimization: Incorporating the optimization of energy efficiency into the scheduling structure involves DVFC, resource awarding schedule, and task allocation to minimize the consumption of energy.
- Privacy-aware task allocation: Developing a task allocation method with privacy awareness that understands both energy efficiency goals and privacy needs including an algorithm that designs and balances the trade-offs, optimizing decisions of task allocation, and individual privacy preservation.
- Experimental evaluation: Conduct extensive experiments of the approached methodology to evaluate the potentiality (Hua et al. 2022). Using real-world traces or benchmarking the datasets to stimulate measures of the level of privacy preservation, various scenarios, task completion, energy consumption, and any other relevant metrics.
- Performance analysis: Analyzing the result to access the trade-offs between energy efficiency and privacy preservation. Comparing the methodology with highlighting existing advantages and boundaries.

Following this methodology, the study enables the growth of more energy-efficient and privacy-conscious computing systems, goal to achieve a structure for privacy-preserving energy efficiency.

7. Privacy-Preserving Techniques for Task Scheduling

The techniques of privacy preservation play a pivotal character to ensure the integrity and confidentiality of a sensitive user while scheduling the computing system. Here are some followings,

- Encryption: This method can ensure by encrypting the sensitive data before processing and sharing. Homomorphic encryption considers computation to be encrypted and performs data while scheduling the procedure.
- Different Privacy: this mathematical structure pushes perturbations and noise into task-based data. Adding randomness, differentiating privacy techniques, and maintaining the scheduling decision.



Task scheduling algorithms for energy optimization in cloud environment
(Source: Qin et al. 2021, P-24)

- Anonymization: This method obfuscate or remove information that is personally identified and a resource. Moreover, it becomes very difficult to ensure, specify, and link the privacy and anonymized data while task scheduling (Qin et al. 2021).
- Access Control: These mechanisms ensure boundaries on information access while task scheduling. Defining access rights and privacy policies, reducing privacy risk breaches, and authorizing sensitive data.
- Secure Protocols: secure protocols like secure function evaluation, and secure multiparty computation, during the protection of sensitive information (He et al. 2019). These regulations confirm that without exposing inputs individually, participants can jointly compute decisions for scheduling tasks.
- Privacy-Preserving Data Mining: these methods consider resource data and mining tasks with unraveling the sensitive data. Data anonymization, perturbation, and aggregation could be included to present information mining operations during preserving privacy.

Employing those tasks scheduling algorithms, privacy-preserving methods, and scheduling procedures, enables privacy-conscious, and confidential computing thoughts.

8. Energy Efficiency Optimization Techniques

Techniques of energy optimization generally play a vital role while reducing the consumption of energy and promoting sustainability in scheduling the task to the compilation o the systems (Hua et al. 2020). Some of the general energy have to be described efficiently while the techniques of optimization have to be employed in this context:

a.Consolidation of Task: Consolidating the task enhances the objects of the consolidation of the different tasks in scheduling the different single resources while minimizing the waste of energy.

b. Dynamic Voltage and Scaling of Frequency (DVFS): DVFS adjusts the frequency and the voltage while calculating the resources according to the demand of workloads. At the time of increasing the performance of the dynamic scaling.

Section: Research Paper
ISSN 2063-5346

Algorithm	Description	Findings	Limitations	Scheduling Parameters	Future Work	Tool
Algorithm related to first come first serve	At first. The task have to be arrived which is scheduled. Then after the executed task next task will be prepared and executed	Evaluations of the arrival time of tasks. The algorithms are ready to be implemented	No other criteria for scheduling	Arrival time	Another criteria to be find out after scheduled	Simulation

Table 1: from A Review Paper on Various Task Scheduling Algorithms
(Source: Lee et al. 2021, P-23)

c. Load Balancing: Utilizing the same already available resources has been consolidated to the reduction of the extra time to fragment the resources and enhance their performance. This ultimately leads to the savings of energy (Lee et al. 2021).

d. Policies to manage the power: These policies comprehend the strategies to manage the power state of calculating the resources. These processes like sleep states can help in the management of constantly changing policies related to power management.

e. Predictive Modelling: historical data can be used to model the forecast of the workload in anticipating the demands of the upcoming tasks.

f. Resource-aware Scheduling: This method evaluates the characteristics and the profiles to calculate the resources while allocating the provided task.

The increasing of the performance of the resources to the consumption of energy after matching up the capability of the existing resources. To match the provisions of the tasks (Qin et al. 2021). The incorporation of energy-efficient techniques in aiming the energy minimization and consumption of extra energy added the techniques to schedule the algorithms, to provide its contribution to obtaining eco-friendly operations.

9. Integration of Privacy and Energy Efficiency

The optimization techniques in playing a big role to reduce the consumption of energy to promote sustainability in scheduling the tasks for computing systems (Long et al. 2020). Some of the general strategies to be consolidated while reducing the identification of the algorithms by ensuring the tasks to schedule the different algorithms, the system to compute while achieving the savings of the energy significantly while contributing the sustainable eco-friendly energy can be used effectively to be integrated:

1. Privacy-aware Energy Optimization: Algorithms to schedule the task that can be designed while considering the privacy-related requirements as a constraint at the time of optimizing tt energy. The main aim is to assure the techniques are maintained throughout the process to schedule.
2. Privacy-preserving Energy Optimization Techniques: the technique of optimizing the energy, like consolidation of the task to maintain the voltage dynamically.
3. Different Privacy-Energy Optimization: Differential methods can be installed to optimize the energy algorithms while protecting the privacy of an individual after injecting the noise to control and perturbed th the data related to energy, and the assurance of the issues related to differential privacy the time of the process optimization (Kim et al. 2022).
4. Customized trade-off of Privacy-Energy: the energy efficiency dn privacy integration must be allowed while making the customizable trade-offs by the other users of the application that can be varied to the private requirements with the goals related to energy. This provides the flexibility to define the preferences privately.
5. Privacy-Preserving Task Allocation Strategies: The decision related to the task's local energy while consuming the energy effectively.

10. Experimental Evaluation

The evaluation related to the context of privacy-preserving energy efficiently, this analysis of the evaluation to schedule the order to serve the different modules to the privacy and energy concerns, while evaluating on an experiment basis (Yang and Wang 2021).
1. Dataset Selection: While opting for the or the tracing of the representation of a different variety of the characteristics of the tasks, while analyzing other profiles, and the privacy-related needs.
2. Privacy Metrics: While assessing the privacy metrics to evaluate quantitatively the privacy leer can be preserved while achieving the proposed methodology. The metrics can be evaluated after the inclusion of entropy, and scores of performance of ht utility of the energy.
3. Energy-Efficient Matrics: The opted matrics of saving energy while consuming h energy, utilization of the resources, and the performance metrics can be highly utilized within the allocated period (Xie et al. 2023). The overhead use of comparison while achieving the necessary savings to be performed in assessing the effectiveness of the data.
4. Evaluation of the performance: Measuring the computational data to introduce the techniques to preserve privacy. Thee assists in the assessment of the effectiveness of this methodology while optimizing the usage of energy.
5. Comparative Analysis: The performance of the effectiveness of the announced methodology while allowing the preservation method, to improvise the preservation of the privacy policy by scheduling the computational algorithms and the technique to preserve privacy.
6. Sensitivity Analysis: Conducting the analysis o sensitivity, the robust method of evolution is required to analyze the methodology. This scales up the proposed approach.

Section: Research Paper
ISSN 2063-5346

11. Results and Analysis

The analysis of ht results of studies to preserve the privacy energy to announce the task efficiently while putting the necessary insights to perform effectively. After accomplishing the privacy integration techniques consider the scheduling of that task, while calculating the systems to achieve the resource utilization techniques to optimize the operations energy-efficient method. This integration assures the operations without compromising privacy and the techniques of preserving privacy do not hamper the goal of energy optimization.

1. Privacy Preservation: Privacy-related measurements like information of entropy, privacy scores of risk, privacy leakage, and the demonstration of this effectively to protect the used data. This assures the integration of the techniques related to privacy preservation, like encrypting or differentiating the privacy and the integrity of the sensitive information at the time of scheduling the process.

2. Energy Efficiency:

At the time of analyzing the energy-efficient metrics, at the time of consumption or allocating the resources, as task consolidation or dynamic voltage change and frequency scaling (DVFS), which effectively reduces the wastage of energy and enhanced the utility of resources. This assures the integration of the techniques related to privacy preservation, like encrypting or differentiating the privacy and the integrity of the sensitive information at the time of scheduling the process.

3. Privacy Energy Trade-off: The trade-off between energy efficiency and privacy preservation is insured in scheduling the task to recover it effectively. The resultant analysis impacted slightly the efficient use of energy at the time of analyzing the computational data. The analysis is quietly effective in analyzing the importance of maintaining the balance to preserve the outcome effectively to balance between the optimization of energy and privacy. This assures the removal of privacy-related concerns without compromising the goal related to optimizing energy efficiently.

4. Comparative Analysis: After the analysis of the existing data, the superior methodology is proposed. This produces the result to narrate the preservation of privacy techniques to compare effectively in scheduling the different algorithms (Tijali et al. 2023). This emphasizes the pros and cons of the analysis of privacy by effectively restoring the energy.

5. Sensitivity Analysis: The investigation of sensitivity analysis investigated the adaptability and robustness of the methodology in different scenarios. The indicated result points out the different characteristics of the workload and the configuration of the system. This high impact on the performance throughout different domains reinforces the versatility of the implication of the methodology.

12. Conclusion and Future Directions

To conclude, the task to schedule the preservation of privacy efficiently to analyze a critical area of research to aim at balancing the preservation privately to integrate the technique in demonstrating the effectiveness while protecting the data to reduce the consumption of energy.

The future direction in this segment further refines the proposed methodology in enhancing the scalability, and the optimization of real-time performance. In addition to that, the consideration of privacy preferences in allowing the customizable and
solutions related to privacy optimization.

References

Tan, S., Wang, X. and Jiang, C., 2019. Privacy-preserving energy scheduling for ESCOs based on energy blockchain network. *Energies*, *12*(8), p.1530.

Yang, H., Zhao, J., Xiong, Z., Lam, K.Y., Sun, S. and Xiao, L., 2021. Privacy-preserving federated learning for UAV-enabled networks: Learning-based joint scheduling and resource management. *IEEE Journal on Selected Areas in Communications*, *39*(10), pp.3144-3159.

Chen, L., Tang, H., Zhao, Y., You, W. and Wang, K., 2022. A Privacy-preserving and Energy-efficient Offloading Algorithm based on Lyapunov Optimization. *KSII Transactions on Internet & Information Systems*, *16*(8).

Boopathi, M., Gupta, S., Zabeeulla, A.M., Gupta, R., Vekriya, V. and Pandey, A.K., 2023. Optimization algorithms in security and privacy-preserving data disturbance for collaborative edge computing social IoT deep learning architectures. *Soft Computing*, pp.1-13.

Wang, Y., Su, Z., Luan, T.H., Li, J., Xu, Q. and Li, R., 2023. SEAL: A Strategy-Proof and Privacy-Preserving UAV Computation Offloading Framework. *IEEE Transactions on Information Forensics and Security*.

Zheng, J., Li, K., Mhaisen, N., Ni, W., Tovar, E. and Guizani, M., 2022. Exploring Deep-Reinforcement-Learning-Assisted federated learning for Online Resource Allocation in Privacy-Preserving EdgeIoT. *IEEE Internet of Things Journal*, *9*(21), pp.21099-21110.

Wang, N., Chau, S.C.K. and Zhou, Y., 2021. Privacy-preserving energy storage sharing with blockchain and secure multi-party computation. *ACM SIGENERGY Energy Informatics Review*, *1*(1), pp.32-50.

Oskouei, M.Z., Mohammadi-Ivatloo, B., Abapour, M., Shafiee, M. and Anvari-Moghaddam, A., 2021. Privacy-preserving mechanism for collaborative operation of high-renewable power systems and industrial energy hubs. *Applied Energy*, *283*, p.116338.

He, X., Jin, R. and Dai, H., 2019. Peace: Privacy-preserving and cost-efficient task offloading for mobile-edge computing. *IEEE Transactions on Wireless Communications*, *19*(3), pp.1814-1824.

Hua, W., Umar, M., Zhang, Z. and Suh, G.E., 2020. GuardNN: Secure Accelerator Architecture for Privacy-Preserving Deep Learning. *arXiv preprint arXiv:2008.11632*.

Qin, Z., Liu, D., Hua, H. and Cao, J., 2021. Privacy preserving load control of residential microgrid via deep reinforcement learning. *IEEE Transactions on Smart Grid*, *12*(5), pp.4079-4089.

Tajalli, S.Z., Kavousi-Fard, A., Mardaneh, M. and Karimi, M., 2023. A multi-agent privacy-preserving energy management framework for renewable networked microgrids. *IET Generation, Transmission & Distribution*.

Yang, Q. and Wang, H., 2021. Privacy-preserving transactive energy management for IoT-aided smart homes via blockchain. *IEEE Internet of Things Journal*, *8*(14), pp.11463-11475.

Zhang, H. and Zeng, K., 2019, April. Pairwise markov chain: A task scheduling strategy for privacy-preserving sift on edge. In *IEEE INFOCOM 2019-IEEE Conference on Computer Communications* (pp. 1432-1440). IEEE.

Wang, N., Chau, S.C.K. and Zhou, Y., 2021, June. Privacy-Preserving Energy Storage Sharing with Blockchain. In *Proceedings of the Twelfth ACM International Conference on Future Energy Systems* (pp. 185-198).

Kim, Y., Venkatesha, Y. and Panda, P., 2022, June. Privatesnn: privacy-preserving spiking neural networks. In *Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 36, No. 1, pp. 1192-1200).

Hua, W., Umar, M., Zhang, Z. and Suh, G.E., 2022, July. Guardnn: secure accelerator architecture for privacy-preserving deep learning. In *Proceedings of the 59th ACM/IEEE Design Automation Conference* (pp. 349-354).

Xie, C., Daghero, F., Chen, Y., Castellano, M., Gandolfi, L., Calimera, A., Macii, E., Poncino, M. and Pagliari, D.J., 2023. Efficient Deep Learning Models for Privacy-preserving People Counting on Low-resolution Infrared Arrays. *IEEE Internet of Things Journal*.

Long, Y., Chen, Y., Ren, W., Dou, H. and Xiong, N.N., 2020. Depet: A decentralized privacy-preserving energy trading scheme for vehicular energy network via blockchain and k-anonymity. *IEEE Access*, *8*, pp.192587-192596.

Lee, S., Xie, L. and Choi, D.H., 2021. Privacy-preserving energy management of a shared energy storage system for smart buildings: A federated deep reinforcement learning approach. *Sensors*, *21*(14), p.4898.