A Review of Privacy-Preserving Data Sharing and Collaboration in IoT Environments

Raiyan Mustafa Mulla [1], Ishitha Saravan[1], Lilibeth Reales[1#] and Vikas Rao Naidu[1#]

[1]Middle East College, Muscat, Oman
[#]Advisor

ABSTRACT

A massive amount of data is being produced as the number of Internet of Things (IoT) devices used increases. To support new applications and services, this data can be shared and evaluated. Sharing sensitive data, however, presents serious privacy issues, especially in IoT contexts where data is frequently produced by personal devices. In this research, we suggest a privacy-respecting paradigm for cooperative data exchange in IoT situations. The suggested approach combines differential privacy approaches with safe multi-party computing to facilitate collaborative data sharing while preserving user privacy. Data security is maintained during computations thanks to multi-party computation, and differential privacy makes it challenging to locate a specific individual's data in a shared dataset. We analyzed several research and their implementation of each method to show the viability of our methodology. The findings demonstrate that the suggested framework may support data exchange and collaboration in IoT environments while preserving user privacy. This framework has a lot of potential to support brand-new services and applications in this industry. This tackles issues like preserving individual privacy while also enabling the study of massive datasets that come up when data is shared across many businesses. It can also be used in settings like smart homes or wearable technology when a lot of different personal gadgets are producing data. In conclusion, the paradigm we've suggested offers a way to share data collaboratively while yet protecting user privacy in IoT environments.

Introduction

Our way of life, our jobs, and how we interact with technology have all changed as a result of development and expansion in Internet of Things (IoT)'s devices. It has also seen substantial expansion in recent years on the worldwide market. Markets & Markets predicts that the industrial Internet of Things (IoT) market will develop at a compound yearly growth rate of 7.4% from 2020 to 2025, reaching a value of 110.6 billion USD (Rejeb et al., 2023). Additionally, it is anticipated that by 2030, there will be approximately 50 billion IoT devices in use globally, establishing an extensive network of interconnected devices. This generates enormous amounts of data that comes with several challenges, particularly in terms of privacy and security. The sensitive nature of IoT data has raised concerns regarding data privacy, and the potential for security breaches has made it difficult to ensure the safety of user information (Rejeb et al., 2022).

IoT devices regularly collect sensitive data, like personal data, which could be used improperly or exploited. Additionally, the massive amount of data being generated has the potential to compromise current security measures and expose system vulnerabilities (Lee & Ahmed, 2021). By addressing these challenges, the privacy and security of IoT data sharing must be guaranteed. It is typical practice for many parties, including people and businesses, to share data. This transaction may pose privacy hazards due to the potential for data sharing without the owner's knowledge or consent (Arora et al., 2019).

Some of the classic strategies used to protect data privacy in IoT include cryptographic procedures and data anonymization techniques. They have certain limitations and are not enough to address the security concerns. Due to

this, researchers have suggested differential privacy (DP) as a more practical privacy preservation method. To protect privacy, DP uses a variety of mathematical procedures to add the necessary amount of random noise (Kairouz et al., 2017). DP provides a formal degree of privacy assurance and is resistant to privacy violations. Researchers have presented the concept of differential privacy for privacy preservation in IoT, and major firms have already started adopting it in a number of IoT systems (Husnoo et al., 2021). Furthermore, Multiparty Computation (MPC) enables parties to compute data and arrive at a solution that is desired by both parties without disclosing any of the parties' personal information. Concerning issues requiring zero-knowledge proofs, Shamir's Key Sharing Algorithm has been used as an example. This paper shows the possibility of sharing IoT data and allowing collaborative work freely without any privacy concerns. This is achieved using differential privacy and Multiparty Computation(Hassan et al., 2020).

Literature Review

Lee and Ahmed discusses the integration of blockchain and IoT technologies to improve data security and privacy. The theoretical framework is centered on a general architecture to address trust difficulties between parties conducting business via blockchain. The goal of the project is to create an acceptable architecture that integrates blockchain technology and IoT systems to meet the objectives of both systems. The effectiveness of three models—the IoT generic layered model, IoT stretched model, and the layered cloud-edge model—in lowering the security susceptibility of IoT devices is compared in this article. In terms of improving security and privacy, the comparison reveals that the layered cloud-edge approach is the most successful, followed by the IoT stretched model and the IoT generic layered model. The paper makes the case that adequate infrastructure must be created in order to continuously improve IoT device security. The essay doesn't offer a thorough analysis of the literature on privacy issues with IoT devices. However, it underlines the need for appropriate infrastructure to improve user privacy and the growing concern regarding the security vulnerability of IoT devices. According to studies like (Ghazal et al., 2020), which are compatible with the conclusions of the paper, IT professionals should create proper IoT designs to lessen security vulnerabilities. Various threats that could have an impact on a company's operations are exposed as a result of the security vulnerabilities' rapid growth, according to other studies like (Liang et al., 2017). The article underlines that there is no ideal system for safeguarding user information and data. Other studies, like (Samie et al., 2019), which emphasize that IoT devices are susceptible to a number of cyber security threats that can impair their performance, support this conclusion. In addition, research like (Mendez et al., 2017) suggests that stronger security models need to be created in order to increase the security of IoT devices. In conclusion, the article provides some insights into the security and privacy concerns of IoT devices. It draws attention to the necessity of having the right infrastructure to improve data security and privacy. The study offers several insightful observations that are consistent with other research on the subject, despite the fact that it does not give an in-depth literature assessment on privacy aspects in IoT devices (Lee & Ahmed, 2021).

Husnoo and others gives an overview of privacy attacks on IoT-enabled critical infrastructure and suggests using differential privacy as a fix to protect data privacy while disclosing helpful aggregate database data. The notion of the Internet of Things (IoT), which enables the intelligent interconnected network of everything to allow interaction and exchange of information based on established protocols without requiring human involvement, is introduced at the beginning of the paper. The article goes on to describe the benefits of IoT-enabled systems in numerous industries, including healthcare, manufacturing, and transportation, as well as their rapid rise. The paper then identifies privacy issues that are challenging to discover in IoT-enabled critical infrastructure due to the increased architectural complexity and utilization of numerous heterogeneous components. With differential privacy and IoT-enabled CIs, the authors give a brief overview of some privacy attacks. Differential privacy (DP) is suggested by the authors as a means of protecting data privacy in IoT-enabled CIs. A statistical database's ability to protect individual privacy while revealing meaningful aggregate data about the database is measured using the formal framework known as data privacy (DP). The authors divide the currently used approaches for DP into two categories: methods that take into account

datasets and methods that do not. The next section of the paper examines noise addition strategies, which are ways to introduce noise to the data while still protecting its privacy. The Laplace Mechanism, Exponential Mechanism, and Gaussian Mechanism are the three noise adding mechanisms for DP. Future research directions are provided by the authors, who also talk about the difficulties and restrictions of DP. Overall, the study offers a thorough analysis of privacy assaults in IoT-enabled critical infrastructure and suggests using differential privacy as a defense against them. The work is well-organized and offers a comprehensive comprehension of the ideas covered. The authors cite a number of sources to back up their claims, which strengthens the authority of their writing. To better demonstrate the ideas covered, the article might have benefited from more in-depth examples and case studies (Husnoo et al., 2021).

The research paper titled " Differentially Private Secure Multi-Party Computation for Federated Learning in Financial Applications" by Byrd and Polychroniadou gives background information on the difficulties faced by contemporary financial firms while evaluating huge datasets across many devices. The authors note that consolidating data into a single database poses privacy issues and may exacerbate the possible repercussions of a data breach. The authors recommend federated learning as a strategy to allay these worries. In federated learning, each dataset is analyzed independently, and only the conclusions from each analysis are shared. The authors also discuss the concept of differential privacy, which can help thwart reverse engineering. According to the authors, boosting unpredictability can boost accuracy while preserving user privacy. In addition, the authors discuss secure multi-party computing (MPC), a novel strategy that guarantees anonymity without compromising accuracy. The authors ultimately introduce the idea of secure federated learning. According to this method, clients encrypt the model weights supplied during Step 2 of federated learning, but the server may still do the required computations on the encrypted data without knowing the original weights for any particular user. Recently, secure federated learning was constructed using the MPC technique (Byrd & Polychroniadou, 2020).

The work is presented in the article on multi-party computing (MPC) under differential privacy, where several parties share information to calculate some functions while maintaining privacy. The two privacy guarantee formulations that the authors contrast are differential privacy and secure function evaluation (SFE). They contend that differential privacy offers a higher guarantee of privacy protection than SFE since SFE has limitations in safeguarding sensitive information from powerful adversaries. The authors focus on a specific MPC problem with differential privacy, where each party may only access a single piece of data and attempts to compute a function that may differ from party to party. Computing a separate function is what the primary observer is focused on. The authors use an arbitrary cost metric to calculate the distortion between the true and calculated function values, and each party's information bit is subject to a different privacy restriction. The authors make a distinction between interactive and non-interactive communication protocols and demonstrate the precise superiority of a straightforward non-interactive randomized response protocol in maximizing accuracy for any given privacy level when each party holds one bit. As it holds for all sorts of functions, diverse privacy requirements, all forms of cost metrics, and both average and worst-case measures of accuracy, the authors assert that this optimality finding is quite generic. The authors distinguish between interactive and non-interactive communication protocols and show that, when each party possesses one bit, a simple non-interactive randomized response technique is preferable in terms of maximizing accuracy for any given privacy level. The authors claim that this optimality finding is highly broad because it holds for all sorts of functions, diverse privacy requirements, all forms of cost metrics, and both average and worst-case measures of accuracy.

In conclusion, the article describes a unique method for MPC under differential privacy and offers a thorough analysis of the related literature. The key contribution of the authors is evidence for the effectiveness of a non-interactive randomized response technique in optimizing accuracy for any given privacy level when each party has a single piece of information (Kairouz et al., 2017).

Lindell provides an introduction to the concept of secure multiparty computation (MPC) and its applications. It defines MPC as a technique that enables participants to carry out distributed computing tasks securely, even while malevolent actors are present. The article gives instances of how MPC might be used to address issues in the real world, like comparing DNA for cancer risk assessment and developing a trading platform that protects offers and bids' confidentiality. The article also mentions that MPC assures correctness and privacy, making sure that parties only

discover their output and that the computation is secure. The article gives a summary of the MPC's feasibility findings. It explains that even in the face of nefarious enemies, every distributed computing task may be securely computed. The number of participating parties and the number of potentially corrupted parties affects the viability of MPC. The page also includes a vocabulary note describing how secure function evaluation (SFE), which is frequently used interchangeably with MPC, differs from MPC. The article also mentions that some variations of MPC have its own names, like threshold cryptography and private set intersection (PSI). Overall, the paper offers a short and understandable introduction to the idea of MPC and its uses. It discusses the viability of MPC and the prerequisites for achieving secure protocols. Anyone with an interest in the subject of secure multiparty computation will find the article to be a helpful resource (Lindell, 2020).

Goyal & Saha discussed, the problem of privacy-preserving data aggregation in resource-constrained IoT systems, and a solution is suggested using ConcurrentTransmission (CT) based communication and the Shamir Secret Sharing (SSS) technique with the aid of the CT-based data sharing protocol MiniCast. The majority of the current PPDA solutions, according to the research, rely on homomorphic encryption (HE), which is unsuitable for Internet of Things (IoT) systems because it requires a lot of work. In contrast, SMPC-based solutions, which aim to achieve a cooperative solution for PPDA, rely more on inter-entity communication and data sharing than computation. However, because communication hardware consumes the most energy, IoT devices constantly work to reduce the amount of communication they need to function. In order to effectively implement the communication-intensive component of SMPC, the authors suggest employing CT-based communication and MiniCast. The article briefly describes SSS and MiniCast before outlining the key design factors to take into account while integrating the two systems. In a semi-honest adversarial situation, SSS achieves PPDA using polynomial interpolation over finite fields. The aggregation process occurs in two stages: the sharing phase and the reconstruction phase, and each node assumes a k-degree polynomial with coefficients. To achieve all-to-all/many-to-many data sharing, MiniCast enables numerous instances of the Glossy-based deluge to run concurrently in an interleaved manner. All transmissions in the chain of packets are scheduled according to a TDMA schedule by the protocol. The first-hop neighbors of the process' chosen initiator node transmit their packets, causing the transmission from the second hop to begin. The two rounds of SSS are said to directly correspond to two rounds of MiniCast, according to the authors. In the sharing phase, the chain size is increased to contain n2 sub-slots (packets) to allow a node to share n number of evaluated values meant for different nodes, and in the reconstruction phase, the nodes share the sum values for various public points, allowing the chain size of n to be sufficient. But in the phase of sharing, the chain size is O(n2). Additionally, the authors suggest using a low-degree polynomial to reduce the size of the overall chain during the sharing phase. This would allow the sharing phase to last only long enough to reach out to the required number of neighbors, rather than completing full network coverage (Goyal & Saha, 2022).

This paper addresses the challenges of preserving data confidentiality and privacy in federated learning (FL) systems. According to the authors, data confidentiality is often maintained using privacy-preserving methods such secure multi-party computation (MPC), homomorphic encryption (HE), and differential privacy (DP). They do note, however, that there is a drawback to using MPC to maintain data confidentiality in FL, as the fundamental requirement for all parties to produce and exchange secret shares of private data to all other parties inevitably results in high communication overhead, which exponentially rises with the number of parties in the membership list. To overcome this difficulty, the authors suggest a two-phase MPC-enabled FL framework that elects a portion of FL members from the entire membership list as the model aggregation committee members before using the MPC service to aggregate the local models of all FL parties. This work emphasizes the significance of maintaining data privacy and confidentiality in FL systems, as well as the necessity of scalable and effective privacy-preserving strategies, like MPC. The created two-phase MPC-enabled FL architecture provides a workable answer to the issue of high communication overhead, improving the scalability and efficiency of FL systems while safeguarding user privacy. The work generally offers valuable knowledge on developing privacy-preserving techniques for FL systems, particularly in addressing the problems of data privacy and security (Kanagavelu et al., 2020).

Privacy-Preserving Techniques

Anonymization

One strategy for protecting security is to eliminate actually recognizable data (PII) from information assortments. Personally identifiable information (PII) is information that can be used to identify a person, such as their name, address, phone number, or social security number. Anonymization allows organizations to continue using data while protecting the privacy of individuals whose personal information is being collected, processed, or distributed (Arora et al., 2019).

Anonymization techniques include data perturbation, data aggregation, and data masking. Data masking conceals sensitive information by using a pseudonym, such as a person's name, as a distinguishing identifier. The process of adding noise or unpredictability to the data to make it harder to identify specific people is known as data perturbation. Data aggregation is utilized in the healthcare industry to safeguard patient privacy while maintaining researchers' access to medical data. It is used in finance to help find and avoid fraud while also protecting the confidentiality of financial transactions. Researchers can examine user preferences and behavior on this social media platform while maintaining user anonymity. It is essential to comprehend that anonymity is not perfect and that there is always the possibility of someone being reidentified (Neves et al., 2023).

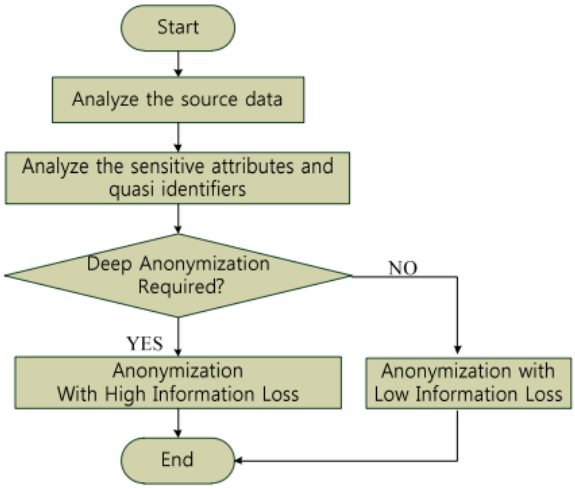

Figure 1. Proposed Scheme by (Jang, 2017)

Differential Privacy

It is a method for preserving personal information during data analysis. For the purpose of preventing the disclosure of private information about specific individuals, this method involves adding random noise to the data. Differential privacy makes sure that the results of a dataset query do not include any details about a specific data point's owner. In order to prevent the results of statistical queries from revealing information about any specific individual's data, this technique adds regulated levels of noise to the original data (Pettai & Laud, 2015).

Consider a dataset with information on the ages and incomes of several individuals. A hacker might be able to identify a specific person's data points if the data is insecure by comparing the exposed data with information that is already in the public domain. However, differential privacy introduces noise into the data prior to release, making it more difficult to pinpoint specific individuals in the dataset. This method aids in maintaining the data's statistical accuracy while protecting people's privacy (Husnoo et al., 2021).

As worries about data privacy have grown, differential privacy has gained popularity in recent years. This method has been used to safeguard sensitive information while still enabling data analysis in a number of different industries, including healthcare, banking, and social networks. Differential privacy does have some drawbacks and is not a panacea (Kairouz et al., 2017). When applying too much noise, data utility may be lost, lowering the accuracy of statistical queries. Therefore, when using differential privacy, it is crucial to strike a balance between privacy and data accuracy.

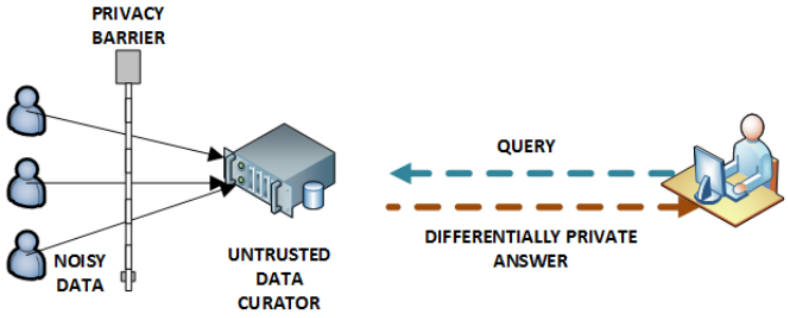

Figure 2. Local differential privacy threat model (Husnoo et al., 2021)

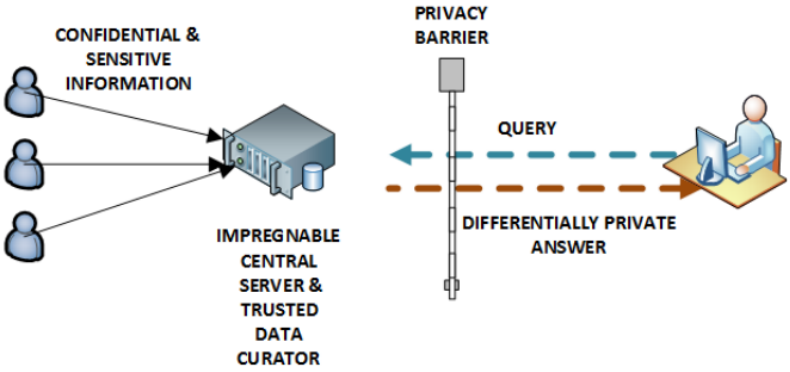

Figure 3. Central differential privacy threat model (Husnoo et al., 2021)

Secure Multi-Party Computation (MPC)

It is a method for computing a function while maintaining the privacy of each party's input on private data that is owned by different parties. MPC aims to make it possible to compute a joint function on multiple parties' private data without requiring any of the parties to disclose their private data to the other parties (Byrd & Polychroniadou, 2020).

Multiple parties participate in MPC and provide the computation with their individual inputs. Each party encrypts their data and shares it with the other parties rather than transmitting it to a third party for processing. In order to compute the function on the combined private data without disclosing their separate inputs, the parties perform computations on the encrypted data without decrypting it. Finally, without disclosing any personal information to the other parties, each party receives the computation's outcome (Geng et al., 2022).

MPC has the benefit of offering privacy guarantees to all parties involved in the calculation. This prevents any party from knowing more about the information of the other party than is necessary to compute the joint function and ensures that the information is not shared with unauthorized parties. MPC has a variety of uses, including secure voting systems, secure machine learning, and secure data analysis (Lindell, 2020).

The use of MPC in the healthcare sector is one instance. Let us say many hospitals wish to work together to create a new medicine. Due to privacy issues, each hospital possesses patient information that they are unable to share with others. The hospitals can compute statistical analyses on the pooled data while maintaining data privacy by using Secure MPC. This enables them to create a new medicine without invading the patients' privacy (Lindell, 2020).

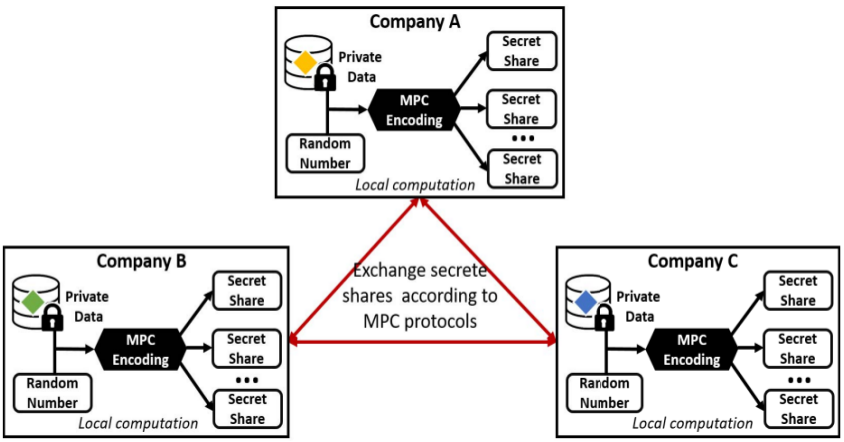

Figure 4. Secure Multi-Party Computation (Kanagavelu et al., 2020)

Federated Learning

This approach to distributed machine learning enables several devices or parties to cooperatively train a machine learning model without sharing their raw data with a central server. Instead, the model is sent to every device, where it is locally trained using that device's data. The device sends only the model updates—not the data—back to the central server when training is finished, where they are integrated to produce a new version of the model (Kanagavelu et al., 2020).

This technique protects users' privacy by ensuring that private information stays on their devices rather than being transferred to a centralized server. This shows that the user still has control over the data and that it is not shared with anybody else (Byrd & Polychroniadou, 2020). Federated learning can help to lessen issues brought on by data bias because it allows models to be trained on a number of data sets.

Healthcare is one area where federated learning has been put to use, allowing machine learning models to be trained on medical data without jeopardizing patient privacy. In the banking industry, it has also been applied to create fraud detection models without disclosing private consumer information (Kanagavelu et al., 2020).

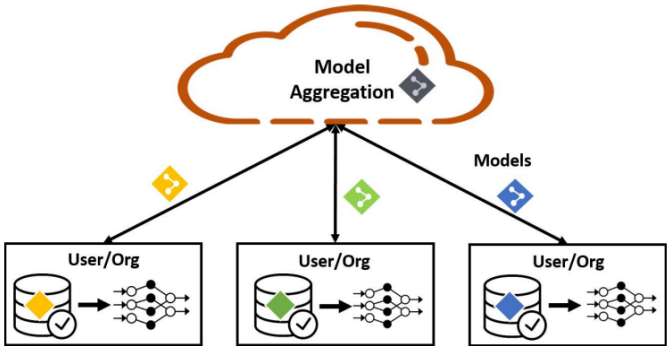

Figure 5. Federated Learning Architecture (Kanagavelu et al., 2020)

Results/Findings

A viable method of protecting privacy in IoT environments combines Differential privacy with Secure multi-party computation (MPC). While MPC ensures that no party has access to the private data of another during computation, differential privacy ensures that dataset queries do not yield any results that reveal any personally identifiable information. For IoT data sharing and collaboration, the combination of these two strategies delivers a higher level of privacy protection than either technique by itself. With this method, multiple parties can compute a joint function on their personal information without sharing that information with one another. MPC further offers privacy guarantees to all parties involved in the calculation in order to make sure that only authorized parties can access the data. This approach has produced favorable outcomes in a number of industries, including banking, social networks, and healthcare. In order to aggregate data from several organizations and safeguard patient privacy, secure MPC has been utilized in the healthcare sector. This has allowed for statistical analysis of the combined data. This has made it possible to develop new medications without violating patients' privacy. Differential privacy and Secure multi-party computing work well together to share and collaborate on data in IoT environments while maintaining privacy. It is suitable in many businesses where data privacy is a concern and delivers a high level of privacy protection.

Recommendation

Future research could dig deeper into the interaction between differential privacy and secure multi-party computation (MPC), examining the effectiveness of this combination in various IoT use cases and scenarios. The performance and scalability of these strategies can be improved, in particular, in large-scale IoT scenarios where several parties may need to share and process substantial amounts of data. To further increase privacy protection in IoT data sharing and cooperation, research can also look at ways to combine these methods with other privacy-preserving tools like homomorphic encryption and federated learning. In addition, research can look into how to assure compliance with data protection laws and standards as well as the practical consequences and difficulties of applying these techniques to real-world IoT applications including smart cities, industrial IoT and healthcare.

Conclusion

In conclusion, in the era of big data, privacy-preserving data sharing and collaboration in IoT environments is a crucial topic. Some privacy-preserving methods include anonymization, differential privacy, secure multi-party computation (MPC), and federated learning. These methods can be used to safeguard sensitive data and guarantee that people's privacy is upheld. The combination of differential privacy and secure multi-party computation (MPC), among many techniques, offers a potential way to protect privacy while yet enabling data sharing and cooperation. In order to prevent the results of a dataset query from revealing any information about the owner of a particular data point, differential privacy can be utilized to introduce random noise into the data. However, MPC makes sure that multiple parties can calculate a joint function on private data without revealing their unique inputs to the other parties. These two methods work together to create a powerful solution for protecting privacy in IoT contexts, allowing for secure data sharing and cooperation without jeopardizing people's private. The fact that each privacy-preserving method has its own drawbacks and trade-offs that must be properly taken into account means that none of them are flawless.

References

Arora, A., Bhushan, B., Kaur, A., & Saini, H. (2019). Security concerns and future trends of internet of things. In 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT) (pp. 1056-1060). New Delhi, India: HMR Institute of Technology and Management. https://ieeexplore-ieee-org.masader.idm.oclc.org/stamp/stamp.jsp?tp=&arnumber=8993222&tag=1

Byrd, D., & Polychroniadou, A. (2020). Differentially Private Secure Multi-Party Computation for Federated Learning in Financial Applications. In Proceedings of the International Conference on Artificial Intelligence and Financial Innovation (ICAIF '20), October 15–16, 2020, New York, NY, USA. https://arxiv.org/pdf/2010.05867.pdf

Ghazal, T. M., Afifi, M. A., & Kalra, D. (2020). Data Mining and Exploration: A Comparison Study among Data Mining Techniques on Iris Data Set. Journal of Talent Development and Excellence, 12(1), 3854-3861. http://scholar.google.ae/citations?user=r3JPWucAAAAJ&hl=en

Geng, T., Njilla, L., & Huang, C.-T. (2022). Delegated Proof of Secret Sharing: A Privacy-Preserving Consensus Protocol Based on Secure Multiparty Computation for IoT Environment. Network, 2(1), 66–80. MDPI AG. Retrieved from http://dx.doi.org/10.3390/network2010005

Goyal, H., & Saha, S. (2022). Multi-Party Computation in IoT for Privacy-Preservation. In 2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS) (pp. 1-10). IEEE. doi: https://doi.org/10.1109/ICDCS54860.2022.00133

Hassan, M. U., Rehmani, M. H., & Chen, J. (2020). Differential Privacy Techniques for Cyber Physical Systems: A Survey. IEEE Communications Surveys & Tutorials, 22(1), 746-789. doi: https://doi.org/10.1109/COMST.2019.2944748

Husnoo, M. A., Anwar, A., Chakrabortty, R. K., Doss, R., & Ryan, M. J. (2021). Differential Privacy for IoT-Enabled Critical Infrastructure: A Comprehensive Survey. IEEE Access, 9, 153276-153304. doi: https://doi.org/10.1109/ACCESS.2021.3124309

Jang, S.-B. (2017). A study of performance enhancement in big data anonymization. In 2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT) (pp. 1-4). Kuta Bali, Indonesia: IEEE. doi: https://doi.org/10.1109/CAIPT.2017.8320669.

Kairouz, P., Oh, S., & Viswanath, P. (2017). Secure multi-party differential privacy. https://kairouzp.github.io/nips_2015.pdf

Kanagavelu, R., Li, Z., Samsudin, J., Yang, Y., Yang, F., Goh, R. S. M., Cheah, M., Wiwatphonthana, P., Akkarajitsakul, K., & Wang, S. (2020). Two-phase multi-party computation enabled privacy-preserving federated learning. In 2020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID). Institute of Electrical and Electronics Engineers (IEEE). DOI: https://doi.org/10.1109/CCGrid49817.2020.00043

Lee, C. C. K., & Ahmed, G. (2021). Improving internet privacy, data protection and security concerns. International Journal of Technology, Innovation and Management (IJTIM), 1(1). http://research.skylineuniversity.ac.ae/id/eprint/152/1/19.pdf.

Liang, X., Zhao, J., Shetty, S., & Li, D. (2017, October). Towards data assurance and resilience in IoT using blockchain. In MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM) (pp. 261-266). IEEE. https://doi.org/10.1109/MILCOM.2017.8170858

Lindell, Y. (2020). Secure multiparty computation (MPC). UnboundTech and Bar-Ilan University. Retrieved from https://eprint.iacr.org/2020/300.pdf

Mendez, D. M., Papapanagiotou, I., & Yang, B. (2017). Internet of things: Survey on security and privacy. arXiv preprint arXiv:1707.01879. https://doi.org/10.1109/COMST.2018.2803740

Neves, F., Souza, R., Sousa, J., Bonfim, M., & Garcia, V. (2023). Data privacy in the Internet of Things based on anonymization: A review. Journal of Computer Security, 31(3), 449-480. DOI: https://doi.org/10.3233/JCS- 210089

Pettai, M., & Laud, P. (2015). Combining Differential Privacy and Secure Multiparty Computation. https://eprint.iacr.org/2015/598.pdf

Rejeb, A., Rejeb, K., Treiblmaier, H., Appolloni, A., Alghamdi, S., Alhasawi, Y., & Iranmanesh, M. (2023). The Internet of Things (IoT) in healthcare: Taking stock and moving forward. Internet of Things, 22, 100721. https://doi.org/10.1016/j.iot.2023.100721

Rejeb, A., Rejeb, K., Simske, S., Treiblmaier, H., & Zailani, S. (2022). The big picture on the internet of things and the smart city: a review of what we know and what we need to know. Internet of Things, 19, 100565. https://doi.org/10.1016/j.iot.2022.100565

Samie, F., Bauer, L., & Henkel, J. (2019). From cloud down to things: An overview of machine learning in Internet of Things. IEEE Internet of Things Journal, 6(3), 4921-4934. https://doi.org/10.1109/JIOT.2019.2893866