A NEW APPROACH IN INDUSTRIAL IOT SYSTEMS WITH TRUSTWORTHY PRIVACY PRESERVING FRAMEWORK FOR MACHINE LEARNING

B. Kavitha, M.C.A., Lecturer, Department of Computer Science, Sri Durga Malleswara Siddhartha Mahila Kalasala, Vijayawada.

A. Aruna, M.Sc.(IS), Lecturer, Department of Computer Science, Triveni DegreeCollege, Vijayawada

ABSTRACT:

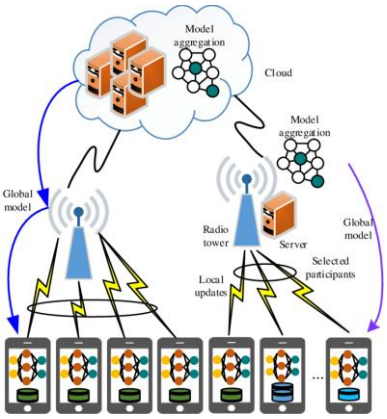
In this paper, The regulations for the data privacy-preserving create an appropriate scenario to focus on privacy from the perspective of the use or data exploration that takes place in an organization. IIoT is a major driving force for Industry 4.0, which heavily utilizes machine learning (ML) to capitalize on the massive interconnection and large volumes of IIoT data. However, ML models that are trained on sensitive data tend to leak privacy to adversarial attacks, limiting its full potential in Industry 4.0. This article introduces a framework named PriModChain that enforces privacy and trustworthiness on IIoT data by amalgamating differential privacy, federated ML, Ethereum blockchain, and smart contracts. The feasibility of PriModChain in terms of privacy, security, reliability, safety, and resilience is evaluated using simulations developed in Python with socket programming on a general-purpose computer. We used Ganache_v2.0.1 local test network for the local experiments and Kovan test network for the public blockchain testing.

KEYWORDS: Industries,Privacy,Machine learning,Data models.

INTRODUCTION

However, collecting and analyzing data has incurred serious privacy issues since such data contain various sensitive information of users. Even worse is that, driven by advanced data fusion and analysis techniques, the private data of users are more vulnerable to attack and disclosure in the big data era. For example, the adversaries can infer the daily habits or behavior profiles of family members (e.g., the time of presence/absence in the home, certain activities such as watching TV, cooking) by analyzing the usage of

 DOI : 10.36893.DRSR.2021.V08I14.18-22 Copyright @ 2021 Authors

appliances, and even obtain = identification information, social relationships, and attitudes towards religion 

From the perspective of privacy-preserving techniques, differential privacy (DP) [**22**] was proposed for more than ten years and recognized as a convincing framework for privacy protection, which also refers to global DP (or centralized DP). (Without loss of generality, DP appears in the rest of this article refers to global DP (i.e., centralized DP).) With strict mathematical proofs, DP is independent of the background knowledge of adversaries and capable of providing each user with strong privacy guarantees, which was widely adopted and used in many areas [**23**,**24**]. However, DP can be only used to the assumption of a trusted server. In many online services or crowdsourcing systems, the servers are untrustworthy and always interested in the statistics of users' data.

PROBLEM DEFINITION

Collecting and analyzing massive data generated from smart devices have become increasingly pervasive in crowdsensing, which are the building blocks for data-driven decision-making. However, extensive statistics and analysis of such data will seriously threaten the privacy of participating users. Local differential privacy (LDP) was proposed as an excellent and prevalent privacy model with distributed architecture, which can provide strong privacy guarantees for each user while collecting and analyzing data. LDP ensures that each user's data is locally perturbed first in the client-side and then sent to the server-side, thereby protecting data from privacy leaks on both the client-side and server-side. This survey presents a comprehensive and systematic overview of LDP with respect to privacy models, research tasks, enabling mechanisms, and various applications. Specifically, we first provide a theoretical summarization of LDP, including the LDP model, the variants of LDP, and the basic framework of LDP algorithms. Then, we investigate and compare the diverse LDP mechanisms for various data statistics and analysis tasks from the perspectives of frequency estimation, mean estimation, and machine learning. Furthermore, we also summarize practical LDP-based application scenarios.

DOI : 10.36893.DRSR.2021.V08I14.18-22
Copyright @ 2021 Authors

LITERATURE SURVEY

- **Bin Jiang,Jianqiang Li,Guanghui Yue, Houbing Song**

Development of Internet of Things (IoT) brings new changes to various fields. Particularly, industrial Internet of Things (IIoT) is promoting a new round of industrial revolution. With more applications of IIoT, privacy protection issues are emerging. Specially, some common algorithms in IIoT technology such as deep models strongly rely on data collection, which leads to the risk of privacy disclosure. Recently, differential privacy has been used to protect user-terminal privacy in IIoT, so it is necessary to make in-depth research on this topic. In this paper, we conduct a comprehensive survey on the opportunities, applications and challenges of differential privacy in IIoT. We firstly review related papers on IIoT and privacy protection, respectively. Then we focus on the metrics of industrial data privacy, and analyze the contradiction between data utilization for deep models and individual privacy protection. Several valuable problems are summarized and new research ideas are put forward. In conclusion, this survey is dedicated to complete comprehensive summary and lay foundation for the follow-up researches on industrial differential privacy.

- **M. Parimala, Swarna Priya, Quoc-Viet Pham**

Industrial Internet of Things (IIoT) lays a new paradigm for the concept of Industry 4.0 and paves an insight for new industrial era. Nowadays smart machines and smart factories use machine learning/deep learning based models for incurring intelligence. However, storing and communicating the data to the cloud and end device leads to issues in preserving privacy. In order to address this issue, federated learning (FL) technology is implemented in IIoT by the researchers nowadays to provide safe, accurate, robust and unbiased models. Integrating FL in IIoT ensures that no local sensitive data is exchanged, as the distribution of learning models over the edge devices has become more common with FL. Therefore, only the encrypted notifications and parameters are communicated to the central server. In this paper, we provide a thorough overview on integrating FL with IIoT in terms of privacy, resource and data management. The survey starts by articulating IIoT characteristics and fundamentals of distributive and FL. The motivation behind integrating IIoT and FL for achieving data privacy preservation and on-device learning are summarized. Then we discuss the potential of using machine learning, deep learning and blockchain techniques for FL in secure IIoT. Further we analyze and summarize the ways to handle the heterogeneous and huge data. Comprehensive background on data and resource management are then

DOI : 10.36893.DRSR.2021.V08I14.18-22
Copyright @ 2021 Authors

presented, followed by applications of IIoT with FL in healthcare and automobile industry. Finally, we shed light on challenges, some possible solutions and potential directions for future research.

- **Hugh Boyes,Bil Hallaq,Joe Cunningham**
- Historically, Industrial Automation and Control Systems (IACS) were largely isolated from conventional digital networks such as enterprise ICT environments. Where connectivity was required, a zoned architecture was adopted, with firewalls and/or demilitarized zones used to protect the core control system components. The adoption and deployment of 'Internet of Things' (IoT) technologies is leading to architectural changes to IACS, including greater connectivity to industrial systems. This paper reviews what is meant by Industrial IoT (IIoT) and relationships to concepts such as cyber-physical systems and Industry 4.0. The paper develops a definition of IIoT and analyses related partial IoT taxonomies. It develops an analysis framework for IIoT that can be used to enumerate and characterise IIoT devices when studying system architectures and analysing security threats and vulnerabilities. The paper concludes by identifying some gaps in the literature.

PROPOSED APPROACH

The increasing number of sanctions for privacy violations motivates the systematic comparison of three known machine learning algorithms in order to measure the usefulness of the data privacy preserving. The scope of the evaluation is extended by comparing them with a known privacy preservation metric. Different parameter scenarios and privacy levels are used. The use of publicly available implementations, the presentation of the methodology, explanation of the experiments and the analysis allow providing a framework of work on the problem of the preservation of privacy. We verify the proposed security protocol using Scyther_v1.1.3 protocol verifier.

CONCLUSION

In this paper, proposed a unique s the concepts of smart contracts, blockchain, federated learning, differential privacy, and interplanetary file system (IPFS) to enforce privacy and trustworthiness on ML in IIoT. Federated learning is used as the global ML model federation and sharing approach, while differential privacy enforces privacy on the ML models. The integration of smart contracts and the Ethereum blockchain introduce traceability, transparency, and immutability to the framework. IPFS introduces immutability, low latency, and fast decentralized archiving with secure P2P content delivery.

DOI : 10.36893.DRSR.2021.V08I14.18-22
Copyright @ 2021 Authors

The proposed framework was tested for its feasibility in terms of privacy, security, reliability, safety, and resilience.

REFERENCES:

1. Shu, J.; Jia, X.; Yang, K.; Wang, H. Privacy-Preserving Task Recommendation Services for Crowdsourcing. *IEEE Trans. Services Comput.* **2018**,
2. Wang, T.; Zhao, J.; Yu, H.; Liu, J.; Yang, X.; Ren, X.; Shi, S. Privacy-preserving Crowd-guided AI Decision-making in Ethical Dilemmas. In Proceedings of the 28th ACM International Conference on Information and Knowledge Management, Beijing, China, 3–7 November 2019; pp. 1311–1320.
3. Zhao, J.; Jung, T.; Wang, Y.; Li, X. Achieving differential privacy of data disclosure in the smart grid. In Proceedings of the IEEE INFOCOM 2014—IEEE Conference on Computer Communications, Toronto, ON, Canada, 27 April–2 May 2014; pp. 504–512.
4. Chen, R.; Li, H.; Qin, A.K.; Kasiviswanathan, S.P.; Jin, H. Private spatial data aggregation in the local setting. In Proceedings of the 2016 IEEE 32nd International Conference on Data Engineering (ICDE), Helsinki, Finland, 16–20 May 2016; pp. 289–300
5. M. Abadi et al., "Deep learning with differential privacy", *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, pp. 308-318, 2016.
6. C. Song, T. Ristenpart and V. Shmatikov, "Machine learning models that remember too much", *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, pp. 587-601, 2017.
7. S. Wang et al., "Adaptive federated learning in resource constrained edge computing systems", *IEEE J. Sel. Areas Commun.*, vol. 37, no. 6, pp. 1205-1221, 2019.
8. M. S. Ali, K. Dolui and F. Antonelli, "IoT data privacy via blockchains and IPFS", *Proc. 7th Int. Conf. Internet Things*, pp. 1-7, 2017.
9. C. J. Cremers, "The Scyther tool: Verification falsification and analysis of security protocols", *Proc. Int. Conf. Comput. Aided Verification.*, pp. 414-418, 2008.
10. J. Wan et al., "A blockchain-based solution for enhancing security and privacy in smart factory", *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3652-3660, Jun. 2019.

DOI : 10.36893.DRSR.2021.V08I14.18-22
Copyright @ 2021 Authors