TRUSTWORTHYPRIVACY PRESERVING FRAMEWORK FOR MACHINE LEARNING IN INDUSTRIAL IOT SYSTEMS

Rashmi HC[1], Sevanthi T Sanjeev[2], Roja Naidu M[3], Sheethal TS[4]
Assistant professor[1]
[3,2,3,4]Department of Information Science and Engineering SSIT, Tumkur
[1]rashmihc@ssit.edu.in, [2]sevanthitsanjeev7544@gmail.com,
[3]Tumkurrojamanjunath9937@gmail.com, [4]sheethalsheethal20@gmail.com

Abstract

Industrial internet of things (IIoT) is transforming many leading industries like transportation, mining, agriculture, energy and healthcare. Machine learning algorithms are used for securing platforms for IT systems. The IOT network unit nodes usually resource in an unusual way by making them more liable to cyber attacks. IIoT systems demands different scenarios in real world one among them is providing security and the causes that surround them in real world aspects. It includes a framework called PriModChain causes privacy and trustworthiness on IIoT data by combining differential privacy, Ethereumblockchain and federated Machine learning. Thus, security will be compromised and we use PriMod chain for providing privacy and other compliances and developed using Pythonwith socket programming on basic computer.

Introduction

The Industrial internet of things (IIoT) uses actuators and sensors along with computing interacting abilities to make decisions by changing the way of collecting data, exchanging data and analyzing the data. Machine learningplays a major role in Industry 4.0 i.e also referred to asIndustrial Internet, activate predictive analytics and uncovering necessary insights to transform industries. By using the advancement of computing and interacting technologies, Machine learning activates the analysis of huge quantities of data like produced by an IIoT based system and uses the extracted information to help real-time decision making in complex situations.Three examples of deep learning in IIoT based Industry 4.0 systems are Fault detection and isolation in industrial processes, real-time qualitymonitoring in additive manufacturing and automatic fruit classification.

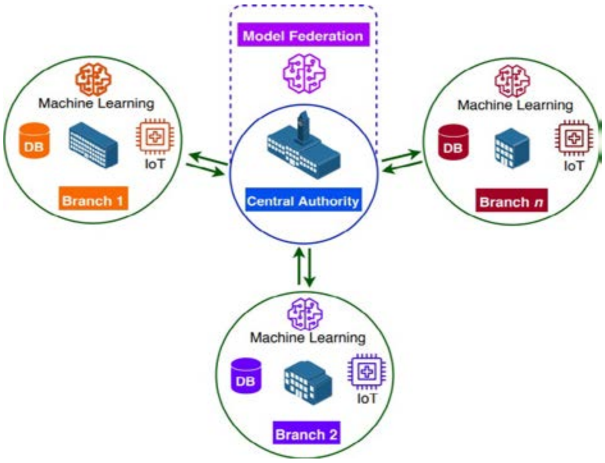

Figure 1: Model knowledge sharing in IIoT-based Industry 4.0

A collection of highly geographically sorted entities which is composed by large scale IIoT based industry setup is as shown in figure 1. As depicted in figure, In IIoT systems like open banking, smart healthcare, data and Machine learning models are trained insight the local boundaries have to be interacted with the specific users to produce organization wide knowledge. To increase the business value against their opponent, vendors have restricted their discernments on product development and improvements within organizationalboundaries. However, Industries like open banking and smarthealthcare are hugely complicated withhuman specific tactful private data. This complication makes IIoT based

Industrysetting quite demanding in the processes of dispensing the data acquisition. Machine learning models that instructed on tactful data can disclose sensitive or private data to advance adversaries. An attack called "man in the middle" supervised by an adversary can effect changes to the actual Machine learning knowledgefetched by the source. To memorize the confidential information malicious algorithms are executed by contributing them as a part of fundamental training processes. Memorized information can be later drawn out and estimated by theadversaries, hence acquiring confidential information to opponency privacy.Membership inference and Model inversion are the two privacy inference attacks that show more vulnerability of machine learning models trained on confidential information. Thereby privacy and trustworthiness are required elements of machine learning in IIoT systems.

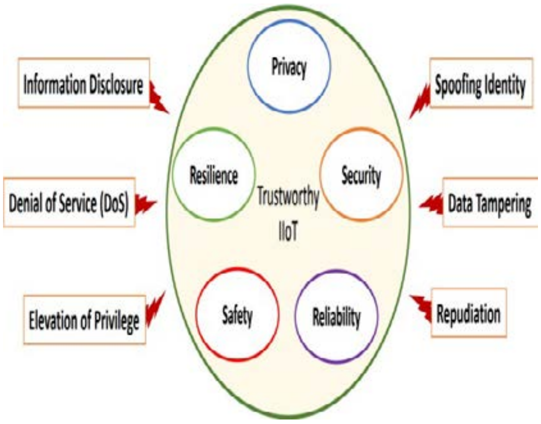

Figure 2: Five pillars of a trustworthy IIoT system vs. STRIDE model of threats.

The five pillars or parameters of trustworthiness in IIoT system is depicted in figure 2. By administering these five parameters can assure a safe and trustworthy IIoT based system can keep away from threats such as tampering denial of service, spoofing, elevation of privilege and repudiation are recognized by the STRIDE threat mode.Privacy and trust issues of machine learning in IIoT systems are addressed by a framework called PriModChain which is the abbreviation of Privacy- preserving trustworthy machine learning model training and sharing framework based in blockchain. This PriModChain combines smart contracts, differential privacy, Ethereumblockchain and federated learning. This also uses the interplanetary file system for off-chain data administration. The preferred framework called PriModChain uses federated learning to cause a global portrayal of the dispensed machine learning knowledge in dispensed IIoT habitat. Federated learning gives the ability of training machine learning model in case of static data and data streams. Model owners were not left by original models; federated learning gives a limited extent of privacy in its default.

Background

A. Differential privacy

Differential privacy is a privacymodel which gives a secure level of privacy by minimizing the possibilities of each and every independent record recognition. In a data item how much information can be obtained for third party analysis is limited by differential privacy. These limits are defined by epsilon and delta frequently. In differential privacy there are two mechanisms which are commonly used perturbation they are Laplace and Gaussian.

B. Federated Learning

Federated learning is a technique in machine learning which trains an algorithm over several broadcasted edge device or servers which is storing local data without swapping them. Based on the datasets machine learning models has been built by using an approach called federated learning which are issued over numerous environment.

C.Block chains, Ethereum, and SmartContracts.

A Blockchain is a connection of nodes that are chained using cryptographic algorithms. The block of data is feed into corresponding blocks which will be in encrypted using cryptographic principles and will automatically become transparent and flexibility to attack.

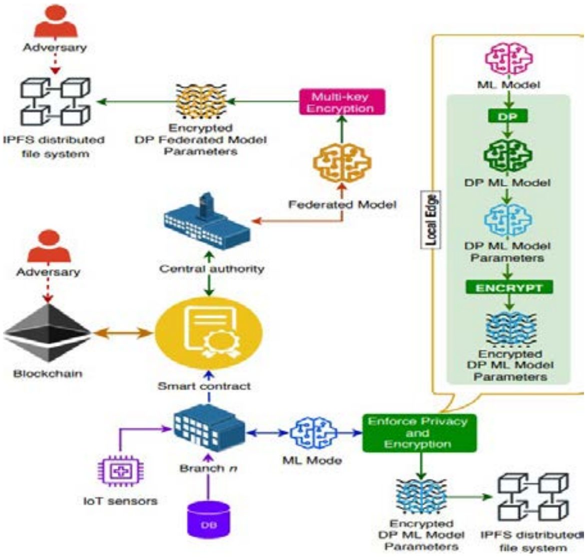
Adversary
IPFS distributed file system
Encrypted DP Federated Model Parameters
Multi-key Encryption
Federated Model
Central authority
Adversary
Blockchain
Smart contract
Local Edge
ML Model
DP
DP ML Model
DP ML Model Parameters
ENCRYPT
Encrypted DP ML Model Parameters
IoT sensors
Branch n
DB
ML Mode
Enforce Privacy and Encryption
Encrypted DP ML Model Parameters
IPFS distributed file system

Figure 3: Modular arrangement of the main components of the proposed framework.

R22,R 19:-Conclusion

A new framework named PriModChain is used for trustworthy machine learning and sharing in IIoT.PriModChainincludes interplanetary file system, block chain, differential privacy and trustworthiness on Machine learning in IIoT. The integration of all these technologies introduces low latency, secure P2P content delivery with reliability, privacy, security and flexibility. This enables to direct future to investigate different approaches to improve efficiency and reduce latency.

References

1. R. Iqbal, T. Maniak, F.Doctor, and C. Karyotis, “Fault detection and isolation in industrial processes using deep learning approaches,” IEEE Transactions on Industrial Informatics.

2. S. A. Shevchik, G. G.Masinelli, C. Kenel, C. Leinenbach, and K. Was- mer, “Deep learning for in situ and real-time quality monitoring in additive manufacturing using acoustic emission,” IEEE Transactions on Industrial Informatics, 2019.

3. M. S. Hossain, M.Al-Hammadi, and G. Muhammad, “Automatic fruit classification using deep learning forindustrial applications,” IEEE Transactions on Industrial Informatics, vol. 15, no. 2, pp. 1027–1034, 2018. 4. R. S. Peres, A. D. Rocha, P. Leitao, and J. Barata,“Idarts– towards intelligent data analysis and real-time supervision for industry 4.0,” Computers in Industry, vol. 101, pp. 138–146, 2018

5. K. Talwar, and L. Zhang, “Deep learning with differential privacy,” in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security.ACM, 2016, pp.308–318.

6. R. Shokri, M. Stronati, C. Song, and V.Shmatikov, “Membership inference attacks againstmachine learning models,” in Security and Privacy (SP), 2017 IEEE Symposium on. IEEE, 2017, pp. 3–18.

7. R. Shokri, M. Stronati, C. Song, and V. Shmatikov, “Membership inference attacks againstmachine learning models,” in Security and Privacy (SP), 2017 IEEE Symposium on. IEEE, 2017, pp. 3–18.

8. Song, T. Ristenpart, andV.Shmatikov, “Machine learningmodels that remember too much,” in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2017, pp. 587–601.

9. M. Fredrikson, S. Jha, and T. Ristenpart, “Model inversion attacks that exploit confidence information andbasiccountermeasures,” in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015, pp. 1322–1333.

10. J. Benet, “Ipfs-content addressed, versioned, p2p file system,” arXivpreprint arXiv:1407.3561,2014.

11. V.Gatteschi,F.Lamberti, C.Demartini, C.Pranteda, and V.Santamar´ıa, “Blockchain and smart contracts for insurance: Is the technology matureenough?” Future Internet, vol. 10, no. 2, p. 20,2018.

12. H. B.McMahan, E. Moore, D. Ramage, S. Hampson etal.,“Communication-efficient learning of deep networks from decentralized data,” arXiv preprint arXiv:1602.05629, 2016

13. C. J. Cremers, “The scythertool: Verification, falsification,andanalysis of security protocols,” in International Conference on Computer AidedVerification.Springer, 2008, pp. 414–418.

14. Lowe, “A hierarchyofauthentication specifications,” in Proceedings 10th Computer Security Foundations Workshop. IEEE, 1997, pp. 31–43.

15. C. Cremers and S. Mauw, “Security properties,”in Operational Seman- tics and Verification of Security Protocols. Springer, 2012, pp. 37–65.

16. Boyes, B. Hallaq, J.Cunningham, and T. Watson, “The industrial internet of things (iiot):An analysis framework,”Computers in Industry, vol. 101,pp.1-12, 2018.

17. Sedgewick, “Framework for improving critical infrastructure cyber-security,version1.0,”Tech.Rep.

18. J. Benet, “Ipfs-content addressed, versioned, p2p file system,” arXivpreprint arXiv:1407.3561,2014.

19. V. Gatteschi,F.Lamberti, C. Demartini, C. Pranteda, and V. Santamar´ıa, “Blockchain and smart contracts for insurance: Is the technology matureenough?” Future Internet, vol. 10, no. 2, p. 20,2018.

20. H. B.McMahan, E. Moore, D. Ramage, S. Hampson etal.,“Communication-efficient learning of deep networks from decentralized data,” arXiv preprint arXiv:1602.05629, 2016.

21. C. J. Cremers, “The scythertool: Verification, falsification,and analysis of security protocols,” in International Conference on Computer AidedVerification. Springer, 2008, pp. 414–418.

22. Lowe, “A hierarchyof authentication specifications,” in Proceedings 10th Computer Security Foundations Workshop. IEEE, 1997, pp. 31–43.

23. C. Cremers and S. Mauw, “Security properties,”in Operational Seman- tics and Verification of Security Protocols. Springer, 2012, pp. 37–65.

24. Boyes, B. Hallaq, J.Cunningham, and T. Watson, “The industrial internet of things (iiot):An analysis framework,” Computers in Industry, vol. 101, pp. 1–12,2018.