Machine Learning and the Trusted Internet of Things (IoT)

Aine Mac Dermott[1], Patrick C. K. Hung[2]

[1] School of Computer Science and Mathematics, Liverpool John Moores University, UK
[2] Faculty of Business and IT, Ontario Tech University, Canada

A.M.MacDermott@ljmu.ac.uk, patrick.hung@ontariotechu.ca

Abstract

Machine learning employs computational methods from advanced analytics that use statistical algorithms to find patterns in datasets. The Internet of Things (IoT) represents the seamless merging of the real and digital world, with new devices being created that store and pass around data. These machine learning models are updated and refined by continually feeding in new user data (as features) and their feedback (as labels) from the IoT devices. Trust is a decision-making process and is always considered a binary decision. More specifically, trust is treated as a performance requirement in the Software Development Life Cycle (SDLC) that refers to a system's specific capabilities. Machine learning techniques are being applied to the IoT environment to facilitate performance and efficiency with the concept of edge computing. However, current machine learning models may threaten IoT environments' security, privacy, and trust. Fortunately, future machine learning models, utilizing trust, may mitigate or even offset these current issues. There are two levels. First, the static trust computation at this level focuses on static attributes associated with a device. Second, the dynamic trust computation uses an initial trust level gained by a device or obtained from a recommender along with keeping track of all the interactions that are happening in between the devices. There is a need for well-defined trust models for IoT applications, where the trust score is a performance metric based on functional properties relevant to the collaboration context.

1 Proposal

1.1 Synonyms

Machine Learning, Security, Privacy, Internet of Things (IoT), Trust

1.2 Definition

Machine learning employs computational methods from advanced analytics that use statistical algorithms to find patterns in datasets. In recent years, machine learning has been used for data processing and analysis to build descriptive and discriminative models, providing insights to businesses and policymakers for making intelligent decisions. The Internet of Things (IoT) represents the seamless merging of the real and digital world, with new devices being created that store and pass around data. The prevalent usage of mobile, wearable, and IoT devices has encouraged the amplified amount of generated data. Understanding how these devices interact and how the data created by said devices will flow through a system can create meaningful insights and provide useful analytical data. These machine learning models are updated and refined by continually feeding in new user data (as features) and their feedback (as labels) from the IoT devices. Future IoT services aim to make decisions autonomously without human intervention. In this regard, trust has been recognized as a key component for processing and handling data and complying with the services, business, and customer needs. The trusted IoT is focused on secure authentication, data encryption, and transaction uniqueness with this mass of devices, with the ultimate objective being where all physical and virtual "things," "people, processes, machines," can securely exchange data and value at global scales with business models based on privacy and trust.

1.3 Motivation and Background

Machine learning has been used in recent years for data processing and analysis, providing insights to businesses and policymakers for making intelligent decisions (Mitchell, 1997). Machine learning employs software tools from advanced analytics that use statistical algorithms to find patterns in datasets. Machine learning algorithms are generally classified into two categories: (1) Supervised learning: The data is labeled and trained according to their classes, such as malicious and legitimate, to the algorithms as mathematical models. (2) Unsupervised learning: The data is not labeled or trained, but the algorithms determine the degree of data coherence to create classes according to the quality of data coherence and data modularity (Zeadally et al., 2020). More recently, deep learning technology promises to revolutionize this processing further, leading to better and more accurate results (Lecun et al., 2015). Deep learning employs software tools from advanced analytics disciplines such as data mining, predictive analytics, text mining, and machine learning based on a set of algorithms that attempt to model high-level abstractions in data by using multiple processing layers with complex structures or non-linear transformations. The processing and analysis of deep learning applications present methodological and technological challenges; however, they also present us with significant opportunities.

The Merriam-Webster definition of "Trust" is described as follows: "A trust is a reliance on someone or things for a specific context." In this particular context, trust is a decision-making process and is always considered a binary decision. More specifically, trust is treated as a performance requirement in the Software Development Life Cycle

(SDLC) that refers to a system's specific capabilities. Modeling trust can benefit the entire SDLC by balancing the need for trust against Quality of Service (QoS), such as system performance, cost, and schedule. (Tucker, 2019). Trust modeling, reasoning, and management can be applied to a distributed environment to enhance its security and reduce a system's dependence on other services. Trust associates integrity with interactions among the device and increasing the human-to-human trust relationship, device-to-device trust relationship, and human-to-device trust relationship (Patel et al., 2019). Jayasinghe et al. (2019) define trust as a "qualitative or quantitative property of a trustee, evaluated by a trustor as a measurable belief, subjectively or objectively, for a given task, in a specific context, for a specific period." and also notes that a "Trust model comprises three entities: Knowledge, Experience, and Reputation. Each trust model is a collective representation of several trust attributes. Each trust attribute represents the trustworthiness feature of a trustee." In the trusted IoT, privacy needs to be by design, resulting in compliance via adaptive algorithms and trust in the connected nodes.

With this in mind, Machine learning techniques are being applied to the IoT environment to facilitate performance and efficiency with the concept of edge computing. However, current machine learning models may threaten IoT environments' security, privacy, and trust. Fortunately, future machine learning models, utilizing trust, may mitigate or even offset these current issues.

1.4 Structure of Learning Systems

The IoT consists of large-scale and heterogeneous entities (devices), which results in difficulties in providing trustworthy services. Data security and privacy issues are an increasing concern due to the wealth of data collected, stored, and processed on these IoT-based devices. Depending on the nature of the device, this data can take the form of personalized, location specific, or user-centric information. The highly diverse IoT application domains, resource constrained IoT devices, and heterogeneity of both devices and platforms hinder the development of a standard IoT trust framework (MacDermott, 2020). Developing a trust ontology (or taxonomy) is needed to formally represent the requirement for trust among IoT devices and apply feasible measures to overcome potential risks. In focusing more specifically on trust, there are two levels. First, the static trust computation at this level focuses on static attributes associated with a device. Second, the dynamic trust computation uses an initial trust level gained by a device or obtained from a recommender along with keeping track of all the interactions that are happening in between the devices.

For example, behavioral evidence includes specific characteristics related to the device's personal properties (Patel et al., 2019). Establishing trust in IoT is challenging due to the volume of diversified influential factors from the cyber-physical-systems (Jayasinghe et al., 2019). The IoT landscape is fragmented: the diversity, volatility, and ubiquity make the task of processing, integrating, and interpreting real-world IoT data an additional challenge. To develop interoperable IoT applications that can detect events in the real world and respond accordingly, deducing knowledge from gathered raw data is a prerequisite (MacDermott et al., 2020). Machine learning and data science will have positive impacts, but this utilization will require deep learning and training of data to understand the underlying devices.

In addition, Jayasinghe et al. (2019) presented a machine learning-based trust computational model for IoT to analyze the trust attributes extracted before and predict prospective transactions' trustworthiness based on Support Vector Machine (SVM). The model is realized based on unsupervised learning techniques with trained datasets by two different labels: trustworthy and untrustworthy.

Furthermore, Tucker (2018) presented a computational trust model to extract key trust features from IoT by a graph-based modeling methodology. The model is based on a machine learning-based scheme to aggregate the trust attributes for obtaining a single trust score for complex intersystem trust relationships for the IoT domain.

More recently, Nassar (2020) has proposed the use of blockchain technology and semantic methodologies to enhance security, trust, authentication, and interoperability in medical and healthcare federated frameworks. The "DITrust Chain Model" is designed to generate reliable cooperative IoT eco-systems (or zones) with reliable mutual information integration between its members. Trust and reliability between members are assessed using hashing and signed exchanged messages.

Qolomany (2020) has also presented trust-based cloud machine learning models for IoT and Industrial IoT services. Their approach evaluates the level of trustworthiness of machine learning models built by different service providers. It uses an intelligent polynomial-time heuristic to maximize trustworthiness while respecting the given reconfiguration budget/rate.

1.5 Cross References

Machine Learning with Privacy, Privacy-Preserving Speech Recognition

1.6 Conclusion

Machine learning requires a large amount of training data for algorithm performance and accuracy. The models and algorithms themselves can be subject to attacks, and the data collected can contain sensitive or confidential information about individuals and organizations. If malicious users were able to recover data used to train these models, the resulting information leakage could create serious issues. Furthermore, if the model's inner parameters are considered proprietary information, access to the model could present further privacy problems. However, the following preventative measures are used to deter malicious users from learning such parameters (De Cristofaro, 2020). For example, the removal of private data from a record - 'anonymization' and 'pseudonymization' – and the replacement of sensitive entries with artificially generated ones (while still allowing re-attribution using a look-up table) are currently the most widely used privacy preservation techniques for medical datasets (Kaisis, et al. 2020). A further example is Differential Privacy (DP), which helps companies collect and share aggregate information about user habits while maintaining individual users' privacy. The primary premise of DP involves making sure that a data subject is not adversely affected by their entry or participation in a database while maximizing utility and data accuracy for the queries. Ensuring data privacy is crucial for numerous applications, including maintaining sensitive information integrity and eliminating the opportunity for adversaries to track users based on Personally Identifiable Information (PII).

The IoT is rapidly becoming an Internet "Web of Things," and there is an increasing need for technologies to expand at the same rate. Data is the most valuable asset in this interconnected paradigm and ensuring trust and protecting privacy becomes increasingly difficult as the IoT becomes more prevalent in the future. Such an increase in connectivity and data collection results in less control, both the data and the connected devices. As such, there is a need for well-defined trust models for IoT applications, where the trust score is a performance metric based on functional properties relevant to the collaboration context.

Recommended Reading

Abou-Nassar EM, Iliyasu AM, El-Kafrawy PM, Song O, Bashir AK, El-Latif AAA (2020) DITrust chain: towards Blockchain-based trust models for sustainable healthcare IoT systems. IEEE Access 8:111223–111238

De Cristofaro E (2020) An overview of privacy in machine learning. arXiv preprint arXiv:2005.08679

Jayasinghe U, Lee GM, Um T, Shi Q (2019) Machine learning based trust computational model for IoT services. IEEE Trans Sustain Comput 4(1):39–52

Kaissis GA, Makowski MR, Rückert D et al (2020) Secure, privacy-preserving and federated machine learning in medical imaging. Nat Mach Intell 2:305– 311

Lecun Y, Bengio Y, Hinton G (2015) Deep learning. Nature 521(7553):436–444

MacDermott Á, Carr J, Shi Q, Baharon MR, Lee GM (2020) Privacy preserving issues in the dynamic internet of things (IoT), the 2020 IEEE international symposium on networks, computers and communications (ISNCC), pp 1–6

Mitchell TM (1997) Machine learning, 1st edn. McGraw Hill, New York

Patel M, Bhattacharyya S, Alfageeh A (2019) Formal trust architecture for assuring trusted interactions in the internet of things, 2019 IEEE 10th annual ubiquitous computing, Electronics & Mobile Communication Conference (UEMCON), New York, pp 0033–0039

Qolomany B, Mohammed I, Al-Fuqaha A, Guizani M, Qadir J (2021) Trust-based cloud machine learning model selection for industrial IoT and Smart City services. IEEE Internet Things J 8(4):2943–2958

Sagar S, Mahmood A, Sheng QZ, Zhang WE (2020) Trust computational heuristic for social internet of things: a machine learning-based approach, 2020 IEEE international conference on communications (ICC), Dublin, pp 1–6

Tomsett R, Chan K, Chakraborty S (2019) Model poisoning attacks against distributed machine learning systems, proceedings volume 11006, artificial intelligence and machine learning for multi-domain operations applications; 110061D

Tucker S (2018) Engineering trust: a graph-based algorithm for modeling, validating, and evaluating trust, 2018 17th IEEE international conference on trust, security and privacy in-computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE), New York, pp 1–9

Zeadally S, Adi E, Baig Z, Khan IA (2020) Harnessing artificial intelligence capabilities to improve cybersecurity. IEEE Access 8:23817–23837