International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 08 | August - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

Based Attack Detection on Machine Learning Algorithm

Mr.T.Senthil Kumar[1], Ms.R.Nithyasri[2] , Ms.R.Ranjani [3],Ms.A.Saktheswari[4]

1Assistant Professor, Depar. of Information Technology,Hindusthan Institute of Technology, Coimbatore, Tamil Nadu,India

2,3,4 Student, Dept. of Information Technology,Hindusthan Institute of Technology,Coimbatore Tamil Nadu, India

Abstract-Due to increased digitization and the advent of new technologies such as the Internet of Things, the use of machine learning (ML) algorithms is rapidly expanding (IoT). ML algorithms are being used in healthcare, IoT, engineering, finance, and other fields in today's digital world. However, in order to predict/solve a specific problem, all of these algorithms must be taught. There's a good chance that the training datasets have been tampered with, resulting in skewed findings. As a result, we have proposed a blockchain-based approach to protect datasets generated by IoT devices for E-Health applications in this article. To address the aforementioned issue, the proposed blockchain-based solution makes use of a private cloud. For assessment, we created a solution that dataset owners can use to secure their data.

I.INTRODUCTION

Machine learning (ML) and related applications have been widely employed. This widespread adoption has resulted in a reliance on machine learning-based forecasts, which has an impact on the judgments made [1]. The accuracy of the datasets used to train machine learning algorithms serves as the foundation for making such predictions and making appropriate decisions. However, if the dataset is tampered with, the ML algorithms' training results would be diluted, resulting in slanted and prejudiced choices. As an example, tampering of customer survey research and product review related data could lead to biased product recommendation in e-commerce platform. [2]. Also, the ML algorithm could be interfered with, resulting in favourable decisions, particularly in the healthcare sector. The ability of machine learning algorithms to process data and identify data patterns makes them more vulnerable to numerous forms of attacks. The authors of [3] devised

poisoning and evasion attacks with the goal of minimising classification generalisation mistakes. As a result, a deceptive model was created, resulting in skewed measurement values in categorization. During the testing phase, evasion is one of the most widely used assaults, in which faked but normal-appearing inputs are fed into the ML system. When these inputs are processed, the model invariably classifies them incorrectly. As a result, the data is misclassified or, in some situations, idea drift occurs, in which the system is constantly retrained, resulting in poor performance [4]. Training data is manipulated in the event of a poisoning assault. This altered data has a negative impact on the classification model's accuracy when fed into it. The classifier function can be skewed in some cases of this type of attack, resulting in favourable results for the attacker [5], [6]. With the growth of technologies such as IoT, Internet of Medical Things, Federated Learning, and others, the amount of digital data generated by IoT-based devices in the healthcare industry is rapidly increasing. The use of machine learning algorithms aids clinicians in quickly diagnosing patients. As a result, a blockchain-based solution to securing medical datasets generated by IoT devices in healthcare applications is provided in this research.

The main contribution of this article includes:

- The data generated from the sensors in the IoTsystem and ML algorithms are stored securelyin a private cloud using AES encryption.
- Identifying tampering of datasets and ML algorithms using blockchain.

The organisation of the paper is as follows Section 2 presents state-of-the-art technologiesfor securing ML datasets from potential attackers.In section 3, proposed framework is discussed .Section 4 contains experimental results and the article is finally concluded with section 5. Recent Developments Recent research emphasise the vulnerability of ML algorithms to adversarial assaults in which non-traceable changes are made in the input data, resulting in erroneous output predictions that deceive the ML method utilised. In [7], the authors identify and analyse the many types of adversarial attacks launched in real-time circumstances, as well as provide feasible defence mechanisms to counter such attacks. Adversarial pictures add adversarial noise, which is used to train machine learning models that are subjected to black box attacks. The detectors aid in detecting hostile alterations in the original image. The concerns related to adversarial attacks are most prevalent in the classification of image objects collected by cell phone cameras, where even the Google inception model is vulnerable to such attacks. The Robust Physical Perturbation technique is used in a scenario in which imposters produce counterfeit road sign

posters and replace them with the real thing. Similar disparate tactics have been observed in cyberspace attacks. For categorization and prediction, robot visual pictures as well as three-dimensional object photos are supplied into ML systems [8], [9]. Intrusion detection is one of the most intriguing blockchain applications. In the case of cryptocurrency and smart contracts, the implementation of intrusion detection with the intersection of blockchain provides a wide range of possibilities [10]. Blockchain has numerous potential uses in the energy sector, as evidenced by peer-to-peer energy trading, IoT applications using blockchain, decentralised markets, electric vehicle charging, and e-mobility [11]. Ethereum and Hyperledger are two non-financial blockchain

applications. The authors of [12] discovered that Binary Neural Networks (BNN) are more robust than full precision networks. As a result, when paired with BNN, input discretization or dimensionality reduction of the input parameters makes the model more resilient against adversarial attacks

- Adversarial Attack on training data: Adversarial training using Brute Force, Data compression as a counter-measure, Imaging Mechanism, Randomization of Data
- Adversarial Attack for network model Deep Contractive Network, Regularization and Masking of the Gradient, Defensive Filtration, Bioinspired Defence Mechanism
- Poisoning Attack: Sanitization of Data, Micromodel based defence, Strong Intentional Perturbations,Human in the Loop (HITL) model, TRIM algorithm

Some of the limitations of the existing defence mechanisms include:

- The existing defence mechanisms deal with specific type of attacks and hence fail to adapt to newer attacks.
- The defence mechanisms such as Brute force method consumes excessive computational resources.

The present work emphasizes on elimination of these limitations using the proposed blockchain based approach

II.Blockchain Fragmentation

Blockchain is a technology that stores and manages a list of timestamped immutable data records in blocks by groups of computing entities. The blocks

are linked together using cryptographic hashes of the previous block. Each block comprises three components: the timestamp, the hash of the previous block, and transaction data. As a result, if any modifications to transactions are required, they must be consistently updated in all of the blocks that comprise the blockchain using the consensus mechanism [13]. This assures the blockchain's immutability, establishing blockchain as the best tool for dealing with all forms of ML algorithm attacks. Blockchain technology have been effectively applied in cryptocurrencies, supply chain management, asset management, health care, digital ID maintenance, and many other applications [14], [15]. With today's world reliant on data-centric analysis, which necessitates precise ML algorithms, it is critical to maintain defence against all possible assaults. There is an urgent need to develop a model that is strong enough to withstand all types of attacks on datasets and ML algorithms. This serves as the primary impetus for the current work. The datasets and the ML algorithm are saved in an encrypted format in the private cloud in this work. Any user who wishes to utilise this dataset or ML method will be assigned a block id as well as the dataset's hash. After receiving this id, the user can utilise the ML algorithms to perform predictive analysis on the datasets. A new hash will be created at the user end after this process is completed.This user-generated hash will be compared to the blockchain's hash. If the hashes match, it is safe to assume that the datasets and ML algorithms have not been tampered with.

III.Architecture Proposal

Figures 1 and 2 depict the proposed work's architecture diagram. Figure 1 depicts the data handling and storage procedure in a private cloud. The encrypted fragments of the data sets and ML algorithms are stored in the private cloud. When a user makes a download request, the data is decrypted and defragmented. Figure 2 depicts a hybrid blockchain in which the administrator creates the blocks, representing the private blockchain, and the user has view and access to the blocks, representing the public blockchain.

Figure 1.Storage of Fragmented dataset in Private cloud

The main goal of adopting a private cloud is to provide the owner complete control over the data. The private cloud is used by the owner to limit access to permitted users and prevent unwanted

access. The overall goal of safeguarding the dataset is substantially improved with this level of access control. The dataset is saved in the cloud as blocks.

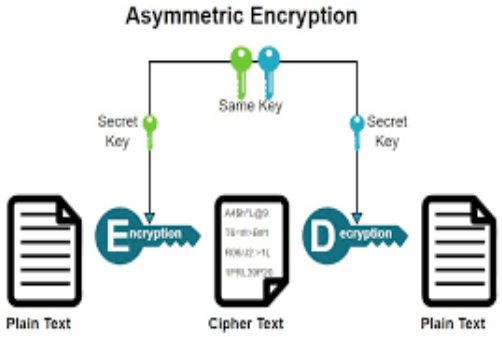

Figure 2.Concept of cryptography in Blockchain

To boost security, encrypted fragments are used. When a dataset download request is made, the fragments are decrypted and the original dataset file is returned to the user. The user can then utilise the public blockchain to compare the hash of the downloaded file to the computed hash to ensure file integrity. This aids in establishing and justifying the dataset's integrity to any third parties. The admin is in charge of adding the dataset name and file hash to the blockchain.This is accomplished using the admin private key's specific private blockchain access, which allows him to add a dataset hash as a block to the blockchain, making it publicly viewable and thereby ensuring the file's integrity.This type of blockchain-based integrity check adds a new dimension to existing types of security and can serve as a stepping stone to more futuristic ideas of automated security. The hybrid blockchain can be used to combine the benefits of both private and public blockchains to achieve a desired result. We introduce the concept of full authority to the data owner while without restricting public access to the data.

IV.Experiments and Results

The following software was used to imitate the experimentation in this study. We utilised 7Zip, an open source file archiver, to fragment the files. Google Cloud Platform hosts the private cloud. With the help of Remix IDE (Ethereum), a blockchain is mimicked using a smart contract written in Solidity. The Medical Cost Dataset from Kaggle is used in this experiment. There are 1338 rows of data in this collection, with 7 attributes. The dataset was separated into many fragments before being stored in the private cloud using the open source archiever programme 7zip. These fragments are then encrypted with AES encryption and a 256-bit key size before being transferred to a Google Cloud Virtual Private Cloud (VPC). The administrator can generate a hash of the datasets and the machine learning algorithm and store it in a blockchain. In this work, the linear regression algorithm is employed for experimentation purposes. The sample logs that were created.

To manage the blocks in the blockchain, a simulation of the deployed contracts is run. If a user wants to test the correctness of the ML algorithm on the dataset, he can ask the administrator for permission. The dataset will be defragmented and the dataset and ML algorithm will be downloaded once the user submits a private key. The user can compute the hash of the downloaded file and compare it to the public blockchain access following the steps below.

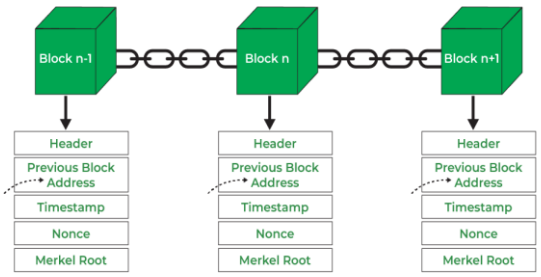

Figure 3. Log of the Blocks created in Blockchain

This allows the user to experiment with machine learning methods on a dataset. After the trial, any third party can check the results for originality by comparing the created hash to the public blockchain hash. If the hashes match, the dataset and machine learning technique are both safe.

V.Conclusion and Future Scope

We successfully created a blockchain-based system to detect assaults on machine learning algorithms and medical datasets in this work. Using the same principle to fuel the requirement to secure an organization's datasets would mean that the private blockchain would require verification from a large number of senior officials, with a consensus awaiting. A feasibility analysis of the various consensus for such a huge scenario, taking into account processing power, time, and resources for data block creation and mining, could be quite useful. Decentralized storage, such as the Inter Planetary File System (IPFS) or SWARM, could be used as a comprehensive decentralised solution to keep the dataset more secure and not on a single organisation. Using decentralised storage to secure the dataset could be a stepping stone to the future of decentralisation, a glimpse into web 3.

REFERENCES

[1] Mahdavinejad, Mohammad Saeid, Mohammadreza Rezvan, Mohammadamin Barekatain, Peyman Adibi, Payam Barnaghi, and Amit P. Sheth, ”Machine learning for Internet of Things data analysis: A survey,” Digital Communications and Networks., vol. 4, no. 3, pp. 161–175, 2018.

[2] Zhang, Yun, Xiaohua Li, Jili Fan, Tiezheng Nie, and Ge Yu, ”A Blockchain Based Secure E-Commerce Transaction System,” Prof.

International Conference on Web Information Systems and Applications, pp. 560–566, 2019.

[3] Kwon, Hyun, Yongchul Kim, Ki-Woong Park, Hyunsoo Yoon, and Daeseon Choi, Daeseon, ”Multi-targeted adversarial example in evasion attack on deep neural network”, IEEE Access, vol. 6, pp. 46084–46096, 2018.

[4] Bhagoji, Arjun Nitin, Daniel Cullina, Chawin Sitawarin, and Prateek Mittal, ”Enhancing robustness of machine learning systems via data transformations, proc. 52nd Annual Conference on Information Sciences and Systems (CISS), pp. 1–5, 2018.

[5] Jagielski, Matthew, Alina Oprea, Battista Biggio, Chang Liu, Cristina Nita-Rotaru, and Bo Li, ”Manipulating machine learning: Poisoning attacks and countermeasures for regression learning”, proc. 2018 IEEE Symposium on Security and Privacy (SP), pp. 19–35, 2018.

[6] Suciu, Octavian, Radu Marginean, Yigitcan Kaya, Hal Daume III, and Tudor Dumitras, ”When does machine learning {FAIL}? generalized transferability for evasion and poisoning attacks,” proc. 27th {USENIX} Security Symposium ({USENIX} Security 18), pp. 1299–1316,2018.

[7] Akhtar, Naveed, and Ajmal Mian, ”Threat of adversarial attacks on deep learning in computer vision: A survey,” IEEE Access, vol. 6, pp. 14410–14430, 2018.

[8] G. Rossini and D. Rossi, “Evaluating ccn multi-path interest forwarding strategies,” Computer Commun., 2013.

[9] S. Podlipnig and L. Bo¨szo¨rmenyi, “A survey of web cache replacement strategies,” ACM Computing Surveys, 2003.

[10] M. A. M. Hail, M. Amadeo, A. Molinaro, and S. Fischer, “On the performance of caching and forwarding in information-centric network- ing for the iot,” in International Conference on Wired/Wireless Internet Communication. Springer, 2015.

[11] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, “Networking named content,” in 5th international conference on Emerging networking experiments and technologies. ACM, 2009.

[12] J. Wang, “A survey of web caching schemes for the Internet,” ACM SIGCOMM Computer Comm. Review, 1999.

[13] M. Amadeo, C. Campolo, J. Quevedo, D. Corujo, A. Molinaro, A. Iera, R. L. Aguiar, and A. V. Vasilakos, “Information-centric networking for the internet of things: Challenges and opportunities,” IEEE Netw., 2016.

[14] E. Baccelli, C. Mehlis, O. Hahm, T. C. Schmidt, and M. Wa¨hlisch, “Information Centric Networking in the IoT: Experiments with NDN in

the Wild," in 1st ACM Conf. on Information-Centric Networking, 2014.

[15] M.-O. Pahl and G. Carle, "Crowdsourced Context-Modeling as Key to Future Smart Spaces," in NOMS, 2014.

[16] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. B. Ohlman, "A Survey of Information-Centric Networking," IEEE Communications Magazine, no. July, 2012.

[17] G. Xylomenos, C. N. Ververidis, V. A. Siris, N. Fotiou, C. Tsilopoulos, X. Vasilakos, K. V. Katsaros, and G. C. Polyzos, "A Survey of information-centric networking research," IEEE Communications Sur- veys and Tutorials, 2014.

[18] M. Zhang, H. Luo, and H. Zhang, "A survey of caching mechanisms in information-centric networking," IEEE Comm. Surveys and Tut., 2015.

[19] I. Psaras, W. K. Chai, and G. Pavlou, "Probabilistic in-network caching for information-centric networks," in 2nd edition of ICN workshop on Information-centric networking. ACM, 2012.

[20] Z. Zhou, D. Zhao, X. Xu, C. Du, and H. Sun, "Periodic query optimiza- tion leveraging popularity-based caching in wireless sensor networks for industrial iot applications," Mobile Networks and Applications, 2015.

[21] M. Meddeb, A. Dhraief, A. Belghith, T. Monteil, K. Drira, and S. Alah- madi, "Cache Freshness in Named Data Networking for the Internet of Things," The Computer Journal (Oxford), 2018.

[22] D. Niyato, D. I. Kim, P. Wang, and L. Song, "A novel caching mechanism for Internet of Things (IoT) sensing service with energy harvesting," IEEE International Conf. on Communications (ICC), 2016.