A Comparative Analysis of Machine Learning Models Deployed for the Device Identification Mechanism

Manuel Cruz*

Department of Computer Science, Institute for Machine Learning, Zurich, Switzerland

Corresponding author: Manuel Cruz, Department of Computer Science, Institute for Machine Learning, Zurich, Switzerland , Email: manuelcruz98@hotmail.com

Received date: December 23, 2022, Manuscript No. IPACSIT-23-15955; **Editor assigned date:** December 27, 2022, PreQC No. IPACSIT-23-15955 (PQ); **Reviewed date:** January 10, 2023, QC No. IPACSIT-23-15955; **Revised date:** January 17, 2023, Manuscript No. IPACSIT-23-15955 (R); **Published date:** January 23, 2023, DOI: 10.36648/ 2349-3917.11.1.4

Citation: Cruz M (2023) A Comparative Analysis of Machine Learning Models Deployed for the Device Identification Mechanism. Am J Compt Sci Inform Technol Vol .11 No.1:004.

Description

IoT reliability and viability are of the utmost concern because data collection poses a security and privacy risk. Device identification, which makes use of a wide range of machine learning algorithms to identify IoT devices, is the first approach. Device identification is carried out with the help of Logistic Regression, K-Nearest Neighbor, Support Vector Classifier, Random Forest, Gradient Boosting, AdaBoost, Light Gradient Boosting Machine, Extreme Gradient Boosting Convolution Neural Networks, and Long Short Term Memory algorithms. Multiple statistical measures have been used to evaluate these models' performance, and we find that LSTM performs better than any other baseline model. A blockchain-based architecture for smart homes to guarantee transparency and data protection is the second approach proposed for ensuring the IoT environment's viability. Smart retail, drone traffic monitoring, autonomous delivery robots, medical surgery robots, and other innovations have emerged as a result of the IoT and AI collaboration. Better risk management improves IoT scalability, reduces costs, and eliminates downtime thanks to the AI-IoT combination. The cyber risk landscape dramatically shifts as the number of IoT devices rises, as numerous devices become vulnerable and are exposed. As a result, resilience and survivability are essential for IoT growth and scalability. There have been numerous reports of hijacked cameras compromising control systems and hacking medical devices over the past few decades. Because it is made up of operating systems, network stacks, firmware, protocols, security tools, and other components, the Internet of Things ecosystem is susceptible to threats and cyberattacks.

IoT Ecosystem's Resilience and Viability

As a result, device identification is difficult. It is necessary to ensure the IoT ecosystem's resilience and viability in order for it to function continuously and smoothly. Device identification is one strategy for improvised security, and security is one important aspect of the same. It is much simpler to authenticate users and processes over the Internet of Things network if devices are identified. Trust, privacy, safety, and integrity are essential aspects of security that are ensured by device identity. After authentication and trust are established when devices, services, and users connect to the network, secure communication and transactions can take place. There is a lot of data generated and shared when devices connect. Most of this data is private and must comply with regulations. To maintain data privacy, identified devices can guarantee encrypted and safe communication. In the event of a cyberattack, identified devices are simpler to locate, ensuring the system's overall safety. Finally, the legitimacy of the firmware and software on a device depends on the device's identity. As a result, device identification is an essential component of Internet of Things security, contributing to its resilience and viability. IoT device identifiers are used to identify network members or devices. Information that is shared between devices is obtained using a unique identifier. The identifier helps locate other Internet of Things devices and shows the identity characteristics. This is crucial for figuring out how many devices are in the IoT environment and how big it is.

IoT Information Examination and Shrewd Agreements

IoT has played a significant role in monetary transactions and financial services over the past few years. Because of this, IoT devices are easy prey for cybercriminals because they store personal information and make it easier to make financial transactions. It's possible that the data that doesn't come from financial institutions isn't properly secured or is left exposed. As a result, improvising security is essential. Another way to ensure the IoT's survival is to comprehend the potential flaws and address security issues. Using smart contacts, further information could be gathered from IoT devices to determine the accuracy of payments. In the Internet of Things, smart contracts can automate a number of processes and build trust between users and devices while enabling high levels of coordination and authority. Blockchain-based applications known as smart contracts, which are known to eliminate administrative overhead, are self-executing applications. They can affirm the exchanges that have occurred and execute pre-decided conditions. Subsequently IoT information examination and shrewd agreements are being conveyed in various fields, in this manner establishing a generally speaking dependable climate. IoT device identification is the first strategy. To identify IoT devices based on their characteristics, we employ a number of machine learning models and evaluate the models using statistical parameters like accuracy, precision, recall, and so forth. We propose smart contract-based security architecture for a trust-based, resilient IoT environment to address the security concerns associated with financial services. Data becomes more appealing to cybercriminals as more devices become connected to the internet. Vulnerabilities, cyber-attacks, and risks are constant and widespread in IoT. From toasters to bots, connected objects may be compromised without adequate security. Additionally, a great deal of the data generated by intelligent home data may be private. Therefore, it is necessary to devise strategies to secure the IoT environment in order to guarantee its viability and dependability.