Cloud Base of Carrying System Using Cyber Security and Artificial Intelligence

Nikata B. Shingote[1] Prof. Monika D. Rokade[2]
[1,2]Sharadchandra Pawar College of Engineering, otur, Maharashtra, India

Abstract— The Internet of Things (IOT) is of great significance in the transportation industry. Autonomous vehicles (AV) are designed to improve daily activities, such as delivering packages, improving traffic and cargo transportation. Autonomous vehicles are not limited to ground vehicles, but also include air and sea vehicles with a wide range of applications. The Internet of Things system composed of a series of audio and video has been called the Internet of Transportation System. Although such IOT systems manage large amounts of sensor data, much of the data is also sent to the cloud for offline analysis. Video and audio and the potential for improvements that can be brought to the transportation industry are huge, but security and privacy issues have brought new challenges, and these challenges must be resolved as we move forward. In addition, artificial intelligence technology has also become crucial for such IOT systems to be able to intelligently manage video and audio. This article discusses the AI and security of the cloud-based transportation system Internet.

Keywords: Network Security, Artificial Intelligence, Artificial Intelligence, Cloud Transportation Internet

I. INTRODUCTION

In recent years, AV has exploded. The company has invested heavily in audiovisual equipment. Audiovisual equipment uses various sensors (for example, cameras, GPS, inertial measurement unit [IMU], LIDAR, RADAR, and ultrasonic sensors) to evaluate its environment. Audiovisual and its potential for improvement in the transportation industry are huge, but security and privacy issues have brought new challenges that need to be resolved. Sensors are susceptible to malicious tampering (for example, IMUs are susceptible to acoustic interference, while GPS receivers are susceptible to spoofing signals). Beforethe vehicle acts on it, the accuracy of the sensor signal should be verified [1]

The Internet of Things system consisting of a series of audio and video has been called the Internet of Transportation Systems. The Internet of the transportation system is vulnerable to attacks (just like any cyber-physical system). Streaming data is being collected from such systems, including self-driving cars and future driverless cars. With the electrification of transportation systems, they need to save energy. Security threats to such systems can cause huge damages, including accidents, loss of life, and being trapped on remote highways due to attacks on energy management.

Data science/machine learning technology is being used to analyze audiovisual data, and the challenge is to apply streaming analysis/learning technology to transportation data. For example, how to apply ML technology to a large amount of sensor data sent by AV? [2].

The Internet of the transportation system will also rely to a large extent on data science/AI/ML (machine learning) technologies to achieve various applications, including optimal directions, unmanned driving, etc. The opponent will learn the machine learning model we use and try to frustrate our model [3]. Finally, although the Internet of the transportation system collects a lot of data, the privacy of individuals must be protected. We envision that many data sharing and analysis will be performed using services running in the cloud integrated with the transportation system Internet [4].

This article explores how to integrate artificial intelligence, security, and cloud technology to develop intelligent transportation systems. We will first discuss the integration of cyber security and AI in the second II. Next, in the III part, we will discuss how to use the secure cloud to conduct data analysis on the Internet of the transportation system. The IV part discusses the security and privacy of the Internet of the transportation system. The V part discusses how to integrate various components (such as AI, cloud security) to provide a smart and secure transportation system Internet. Chapter 6 discusses the future direction.

II. INTEGRATION OF CYBER SECURITY AND ARTIFICIAL INTELLIGENCE

The integration of cyber security and AI involves three aspects. One is to apply AI to network security, the second is to use AI for network security, and the third is to detect privacy attacks caused by AI. In the mid-1990s, research on the application of AI to network security began. The idea is to apply ML technology to detect unauthorized intrusions. This research was expanded in the 2000s to include malware analysis and insider threat detection [5]. A large amount of attack data is being collected. This data must be analyzed so that malicious attacks can be detected. In addition, we also need to predict how the malware will mutate so that attacks can be prevented [6]. In addition, streaming data is being analyzed to detect malicious insiders.

The second area is to ensure the safety of AI technology. In the past decade, this field (now known as adversarial machine learning) has become very important. From healthcare to audio and video, we are increasingly relying on ML technology in all aspects of our lives. These machine learning techniques can be attacked and can lead to 8 catastrophic situations. Therefore, we need to check the type of attack and adapt Machine learning technology. For example, in our work, we checked support vector machines (SVM) and adopted SVM technology to detect certain attacks. The opponent will understand our model and adapt to its behavior. Our adversarial support vector machine technology understands the behavior of the adversary and adjusts itself so that it can detect an attack. Over time, it became a game between our opponents and us.

The desired aspect is the privacy violation that may occur when ML technology is used. For example, it is now possible to integrate large amounts of data and analyze the data to obtain various attributes of individuals. This may result in damage to personal privacy. Many privacy Awareness machine learning (data mining) technology has

been developed [7]. The challenge is to implement appropriate strategies so that we can perform strategically aware data collection, storage, integration, analysis and sharing [8].

III. THE INTERNET OF THINGS BASED ON THE SECURER CLOUD

As mentioned earlier, we envision that much of the data collected from the AV will be sent to the cloud for further processing, including performing analysis. That is, various ML technologies can be used to analyze massive amounts of data including attack data in the cloud. Therefore, it is very important to ensure the security of the cloud itself, especially when safety-critical operations must be performed.

We have designed and developed a layered architecture for secure cloud [9]. At the lowest level is VNM (Virtual Network Monitor). Then, we perform the VMM layer (virtual machine monitor) of the virtual machine self-check. On top of this is a cloud storage layer based on technologies such as HADOOP/ MAPREDUCE. Data can be encrypted, which means that the encrypted data must be queried and analyzed. Above this layer is the query layer for querying cloud data. Finally, we have the application layer. In our example, the applications are those that support the Internet of the transportation system.

IV. THE SECURITY AND PRIVACY OF THE INTERNET IN THE TRANSPORTATION SYSTEM

One method for Internet security and privacy in transportation systems is to use Physically Based Anomaly Detection (PBAD) algorithms to establish reference monitors for ground and airborne AVs [1]. The algorithm will consist of three parts: (i) building a physical invariant model of AV offline; (ii) implementing online tools to monitor expected and observed behavior to detect abnormalities; and (iii) if there is a significant residual difference, then The alarm is issued between two executions. This technology has been applied to the ground and Ariella AV. Below we provide more detailed steps.

A. Offline preprocessing:

AV invariance is calculated using well-known nonlinear models for aircraft and ground vehicles. The accelerometer, gyroscope and magnetometer sensor data on the x, y, and z axes are used for the aircraft. Ground vehicles use vehicle position and steering angle. (Ii) Online stage: The extended Kalman filter (EKF) is used to predict the physical behavior of AV by estimating unknown parameters in the input of the noise sensor. Algorithm partition Divided into two parts, estimates can be predicted and corrected before being compared with sensor data. (Iii) Anomaly detection: Then use the CUSUM algorithm to detect persistent attacks. If the remaining difference is greater than a predefined threshold, an alert will be issued.

In addition to the safety of individual vehicles, the transportation sector can also benefit greatly from the supporting infrastructure that enables communication between vehicles, motion sensors on lamp posts, and surveillance cameras (to name a few) It can help identify traffic jams, divert vehicles and increase vehicle safety. From the user's point of view, all the information required by such systems will cause privacy issues, and this information may lead to the disclosure of private information, such as vehicle identification and driving styles. As the advancement of the Internet of Things becomes more prominent in daily activities, legislators, engineers, and scientists should keep privacy issues in mind. This will help improve public perception, reduce consumer hesitation, and increase the adoption rate of high-tech [4].

V. INTEGRATING AI AND SECURITY FOR THE INTERNET OF CLOUD-BASED TRANSPORTATION SYSTEMS

Data science/machine learning techniques are being used to analyze data, and the challenge is to apply streaming analysis/learning techniques to transportation data. The main problem is to understand the nature of complex transportation data, and to adopt flow analysis technology and apply it to the large amount of heterogeneous sensor data collected. Such data usually emits data streams. Therefore, many stream-based machine learning techniques need to be checked [10]. In addition, deep learning-based technologies developed for IOT systems need to be studied [11].

The Internet of the transportation system will rely heavily on data science/artificial intelligence/machine learning technology to achieve various applications, including the best direction, unmanned driving, etc. The opponent will learn the model used by the vehicle and the data used in model training. The opponent will try to stop the learning process of the vehicle. Therefore, the learning algorithm must be adapted to thwart the opponent's actions. In the end, it becomes a game between the opponent and the vehicle's machine learning algorithm [3].

Although the transportation Internet system collects a large amount of data, it is necessary to protect personal privacy. As more and more sensor data is collected, the storage on the AV will not be enough to store all the data. We envision an encrypted cloud storage component where older data and/or less frequently accessed data will be pushed to the cloud. According to the access control policy, local applications running on the AV will be allowed to access certain collected data. When necessary, these AVs will be allowed to access certain encrypted data stored in the cloud through a simple query interface. We envision that many data sharing and analysis will be performed using services Outsource some running in the cloud [8].

Another direction to enhance security while ensuring high-performance computing is trusted analysis [12]. The calculation of big data may require a lot of computing resources, and organizations (for example, automobile companies) may use third-party services to9 Calculations are cost-effective. When a third-party server is used for calculation, the data is inherently available in an untrusted environment, for example, observed by an intermediary during data transmission, or an insider threat from an adversary in a third-party location performing the calculation. In these cases, data owners may need to protect their data and require encryption guarantees about the data security of these third-party services and the integrity of the calculated output. We are using advancements in embedded hardware technologies (such as Intel SGX) to conduct

research on secure encrypted stream data processing and trustworthy analysis to support a trustworthy execution environment (TEE). We need to explore the application of TEE in transportation and infrastructure Internet.

VI. SUMMARY AND DIRECTION

This article discusses the characteristics of the Inter prise of tracks and develop ML technology to detect and prevent attacks. We must also study how to deal with the ML technology attacks required to develop intelligent transportation systems. Finally, we need to determine the type of data to be sent to the secure cloud for analysis We have only made a fuss in protecting the Internet of the transportation system. We must understand the various types of tracks and develop ML technology to detect and prevent attacks. We must also study how to deal with attacks on the ML technology required for the development of intelligent transportation systems. Finally, we need to determine the type of data to be sent to the secure cloud for analysis.

REFERENCES

[1] R. Quinonez, J. Giraldo, L. Salazar, E. Bauman, A. Cardenas, Z. Lin, Securing Autonomous Vehicles with a Robust Physics-Based Anomaly Detector. 29th USENIX Security Symposium (USENIX Security 20). Boston, MA, August 2020.
[2] M. Masood, L. Khan, and B. Thuraisingham, Data Mining Applications in Malware Detection, CRC Press 2011.
[3] Y. Zhou, M. Kantarcioglu, B. M. Thuraisingham, B. Xi, Adversarial support vector machine learning. ACM KDD 2012: 1059-1067
[4] B. M. Thuraisingham, SecAI: Integrating Cyber Security and Artificial Intelligence with Applications in Internet of Transportation and Infrastructures, Clemson University Center for Connected Multimodal Mobility, Annual Conference, October 2019.
[5] B. M. Thuraisingham, P Pallabi, M. Masud, L. Khan, Big Data Analytics with Applications in Insider Threat Detection, CRC Press, 2017.
[6] K. W. Hamlen, V. Mohan, M. M. Masud, L. Khan, B. M. Thuraisingham: Exploiting an antivirus interface. Comput. Stand. Interfaces 31(6): 1182- 1189 (2009)
[7] L. Liu, M. Kantarcioglu, B. M. Thuraisingham: The applicability of the perturbation based privacy preserving data mining for real-world data. Data Knowl. Eng. 65(1): 5-21 (2008)
[8] B. M. Thuraisingham, M. Kantarcioglu, E. Bertino, J. Z. Bakdash, M. Fernández, Towards a Privacy-Aware Quantified Self Data Management Framework. SACMAT, pp 173-184, 2018
[9] K. W. Hamlen, M. Kantarcioglu, L. Khan, B. M. Thuraisingham, Security Issues for Cloud Computing. IJISP 4(2): 36-48 (2010)
[10] Y. Li, Y. Gao, G. Ayoade, H. Tao, L. Khan, B. M. Thuraisingham, Multistream Classification for Cyber Threat Data with Heterogeneous Feature Space. WWW, pp 2992-2998, 2019
[11] H. Qiu, Q. Zheng, G. Memmi, J. Lu, M. Qiu, B. M. Thuraisingham, "Deep Residual Learning based Enhanced JPEG Compression in the Internet of Things", accepted by IEEE Transactions on Industrial Informatics, 2020
[12] G. Ayoade, V. Karande, L. Khan, K. W. Hamlen, Decentralized IoT Data Management Using BlockChain and Trusted Execution Environment. IRI, pp 15-22, 2018 10

