AI-ENABLED SECURED TRANSPORTATION SYSTEM

Dr.J.Krishna[1], P.ReddiSri[2], P.Poorna[2], S.Furqhan[2], M.Sai Mohan Reddy[2]

[1]Associate Professor in Department of AI&ML, Annamacharya Institute of Technology and Sciences (Autonomous), Rajampet, Andhra Pradesh, India-516126.

[2]Department of Computer Science and Engineering, Annamacharya Institute of Technology and Sciences (Autonomous), Rajampet, Andhra Pradesh, India-516126.

Article History: Received: 13.10.2022 Revised: 28.11.2022 Accepted: 21.12.2022

ABSTRACT: The impact of the Internet of Things on transportation will be significant. Automated vehicles (AVs) are designed to make regular activities easier, such as shipping, vehicle traffic, and freight transit. A broad variety of applications are served by AVs, which can even be airborne or underwater in addition to being transport vehicles. An assortment of AVs makeup the Internet of Transportation, a subset of IoT systems. In addition to managing a lot of sensor data, these IoT devices send a lot of sensor data to the cloud for processing. Although AVs have great promise and can dramatically enhance transportation, worries about safety and confidentiality there will be new issues that need to be resolved. In order for these IoT systems to effectively control AVs, AI-based approaches are becoming increasingly important. For virtualized Network of Things devices, this article tackles access control and AI.

Keywords: Artificial intelligence, cloud computing, and the internet of transportation.

I. INTRODUCTION

The quantity of AVs has grown recently. Organizations are investing a lot of money in AVs. AVs employ a variety of sensors to examine their environment. Regardless of the capabilities of AVs and the advantages that could offer the industrial issues with privacy, security, and the industry bring new problems that require to be solved. It is possible to intentionally manipulate the sensors. Devices should verify frequency response validity while acting on it [1].

The methods of IoT comprised with group of AVs are referred to as the Network of Transport systems. The Network of Transport Systems might be attacked (like any cyber-physical system). These technologies, like driverless cars in the future, as well as autonomous vehicles, are gathering streaming data. The switch to electric transportation systems necessitates energy saving. Assaults on energy management might seriously affect security of these systems, resulting, among other things, in collisions, fatalities, and being stopped on deserted highways. The objective seems to be to employ data science/ML tools to analyse AV data in addition to utilizing broadcast data analysis and learning approaches on transportation information.

So, for example ML algorithms can be used to analyse the enormous volumes of telemetry information that AVs are producing? [2]. The Network of Transport Systems will likewise largely focus on big analytics like Autonomous driving is useful for a variety of tasks, including giving the best routes, artificial intelligence and deep learning (ML) approaches. Our machine-learning models will be familiarised with the opponent, who will then try to sabotage them [3]. Despite the massive quantities of data that the Internet of Transportation Systems may collect, each person's privacy must be protected. We believe that the Internet of Transportation System and cloud-based services will be used for a significant amount of data sharing and analytics [4].

In order to build effective network devices, this research explores how cloud computing, security, and artificial intelligence may be coupled. In the part that follows, we first go through how artificial intelligence and cyber security are related. Section III discusses the usage of a secure cloud for evaluation of data for Internet-based public transportation. The safe and protection of the transport system network are covered in Subsequent Sections. Following Section explains how to integrate several components, to build an intelligent and safe network of transportation networks, use technologies like AI and information protection.

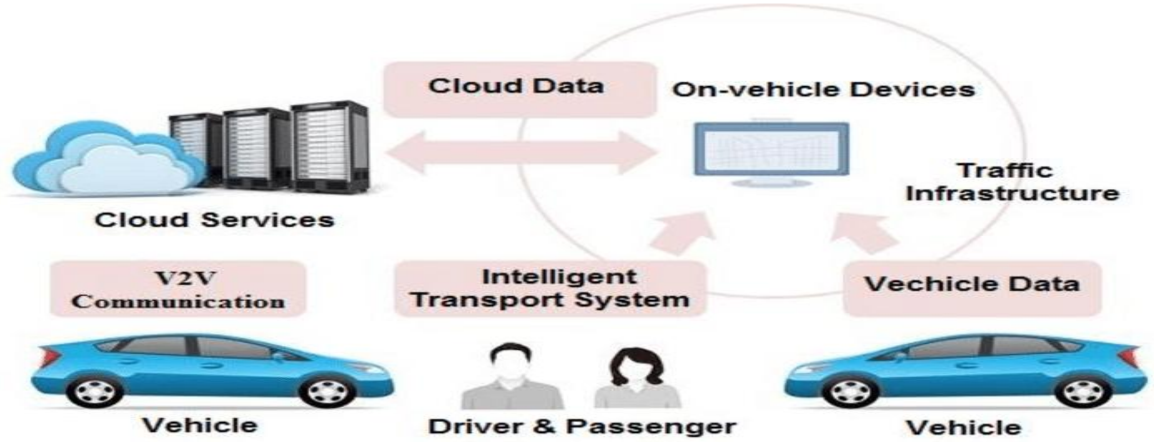


Figure 1: Architecure for AI Enabled Scured Transportation System

II. AI AND CYBER SECURITY INTEGRATION

The fusion of artificial intelligence with cyber security entails three steps. The first two express worries about employing Artificial Intelligence for cyber threats, while the third expresses concern about privacy risks brought on by AI. The middle of the 1990s saw the start of research into using AI for cyber security. Using machine learning (ML) techniques, the goal is to identify unauthorised breaches.

In the 2000s, this study was expanded to encompass malware analysis and the detection of insider threats [5]. The amount of attack data being gathered is enormous. In order to identify malicious assaults, this data must be evaluated. In order to stop the attacks, we also need to foresee how the malware can evolve [6]. Additionally, streaming data are being examined to look for insider threats.

Securing AI techniques is the second area. Over the past ten years, this field—now often referred to as adversarial machine learning—has gained considerable attention. Every element of our life, from healthcare to AVs, depends more and more on ML approaches. Attacking these machine-learning algorithms could have disastrous consequences. As a result, wemust analyse thevarious attack types and alter the ML processes. To identify different risks, for instance, we adjusted support vector machine (SVM) methodologies in our research. The adversary will adapt its strategies in response to our models. Our stochastic support vector machine technique can analyse the data and find a wide range of human attributes by identifying the opponent's behaviours and enormous volumes of data. The individual's right to privacy might be at risk as a result. Numerous supervised learning strategies for secrecy have been developed [7]. Although it is challenging, enforcing the proper regulations is essential for agenda information gathering, preservation, interconnection, evaluation, and distribution [8].

III. PROTECTED DATA CENTER

As mentioned previously, we believe that a sizable amount of the AVs' data collection will be sent to the web for further analysis, such as metrics. To analyse vast volumes of data, including malware data, several ML algorithms may be utilised on the cloud. Thus, the cloud must be safe in and of itself, specifically if this is required to carry out security-sensitive tasks.

For a secure cloud, we have created and built a layered architecture [9]. The VNM is located at the base layer (Virtual Network Monitor). The Virtual Machine Monitor layer, which performs virtual machine introspection, is the next layer. The cloud storage layer, which is built on tools like Hadoop/Map Reduce, is placed above that. There will need to be analytics and querying on the encrypted data because the data may be encrypted. This layer is positioned above the query layer, which is used to query cloud data. The final layer is the application layer, which in our case consists of software tools that enhance the Network of Transport Systems.

IV. NETWORKED TRANSPORTATION SYSTEMS: SECURE AND PRIVATE

Making the Anomaly Detection Based on Physics reference monitor for both earth and aerial AVs (PBAD) algorithm is one of the Facilities to improve the secure and private of the Networked Transportation Systems [1]. The process entails these three steps: Three steps are taken: (1) Asynchronous modelling of the AV's natural integrals; (2) Virtual monitoring of predicted and actual behaviour to spot anomalies; and (3) issuing of an alert in the event of an important accumulated difference between assassinations. The techniques have been used for both Ariella AVs and land vehicles. Below, we go into further detail on the stages.

(i).Asynchronous pre-processing: A well-known semi model for ground and aircraft is used to find the AV's primitives. The aerial vehicle uses sensor data from a speedometer, joystick, and tachometer on the i, j, and k axes. Positioning and angular velocities are utilised by the landscape transportation.

(ii). Virtual platform: Making use of the Extended Kalman Filter (EKF), which extrapolates unidentified properties from noisy sensor data, the physical behaviour of an AV is anticipated. Before the estimation is compared to the sensor data, the procedure is split into two sections that anticipate and correct it.

(iii).The shipping industry might gain a lot from a supporting infrastructure that enables data exchange and remote control on lights, above and beyond the safety of individual automobiles. It modifies itself in response to the assaults. We begin to play games with the opponent as time goes on. The thirsty aspect of employing ML algorithms is the potential privacy issues. For instance, it is presently possible to include Indicating traffic congestion, rerouting cars, and improving vehicle safety are all possible thanks to signs, cameras, and other devices (to mention a few).From the user's point of view, privacy problems are raised by all the data required for such a system and may result in the revelation of personal data, including dashboard, driving patterns, and identity. Government officials, technicians, and researchers need to be cognizant of protection issues along with IoT an innovation in daily life is increasing. This will reduce scepticism from customers, enhance public perception, and hasten the implementation of contemporary techniques [4].

V. CLOUD-BASED INTERNET OF TRANSPORTATION SYSTEMS AI AND SECURITY INTEGRATION.

The goal is to use data science and machine learning to analyse and interpret transportation data utilising stream analytics and learning technologies. To apply broadcast analytics methodologies and use them on the vast volumes of varied sensor data now being received, it is crucial to understand the essence of the complicated type of data. These data are frequently provided in the form of data streams. It is necessary to do extensive study on a variety of broadcast hardware approaches [10]. We still need to understand more about deep learning-based approaches created for Internet of Things systems [11].

In order to provide the best directions, drive autonomously, and use machine learning, artificial intelligence, and data science techniques, the network of Transport Systems will heavily rely on artificial intelligence (AI).

The information utilised to train the models and by the vehicles will become familiar to the adversary. The enemy will make an effort to prevent the vehicle from learning. The learning algorithms must therefore modify in order to counteract the adversary's actions. Eventually, the machine learning techniques in the automobile and the attacker start to compete with one another [3].

Despite the massive quantities of data that the Network of Transport systems may collect, each person's privacy must be secured. The data volume of the AVs won't be enough to hold all of the sensor data as it is gathered. Older information and/or data that isn't used very often will be sent to an encrypted cloud storage component. Some of the gathered data will be made accessible to local apps operating on the AVs based on the access control restrictions. Through a straightforward query interface, the capability of these AVs to retrieve a portion of the encoded information kept in the internet as needed. According to our predictions, cloud-based services will be used often for data exchange and analytics [8].

Reliable analytics [12] is another way to improve security while maintaining high performance computing. Massive computational resources may be needed for computations on bigdata, therefore businesses (like automakers) may outsource some of their work to a third-party service calculations to be economical. Data is unintentionally made public in untrusted contexts when computation is done on a third-party server, such as when data transmission is being observed by a individual watching or when executive threats are coming from enemies at the penultimate site. In these circumstances, it may be necessary for data owners in order to safeguard their data and want encryption guarantees from these third-party services on the security of their data and the reliability of their computations. We are looking at Protected Cryptographic Real-time data Processing and Trustworthy Analytics, which makes use of improvements in the field of embedded hardware like Intel SGX, enable dependable implementation environments (TEE). We must investigate how TEEs can be applied to infrastructures and the Internet of Transportation.

VI. IMPLEMENTATION AND RESULTS

Modules: Implementation of this system used three modules are used 1. Autonomous Vehicle 2. Cloud Server and 3. User (Sender/Receiver).

Autonomous Vehicle: The antivirus software will inspect the incoming files and provide information to the recipient through email, along with a secret key to access the file contents.

1. **Cloud Server:**
   - **1.1 Views data sent by user:** In this, the data sender (user) will submit a certain file to the cloud.
   - **1.2 Files being sent to AV:** In this, the file will be transferred from the sender to the AV by the cloud.

1.3 Tracking the status: In this, the file status may be tracked as either sent or pending.

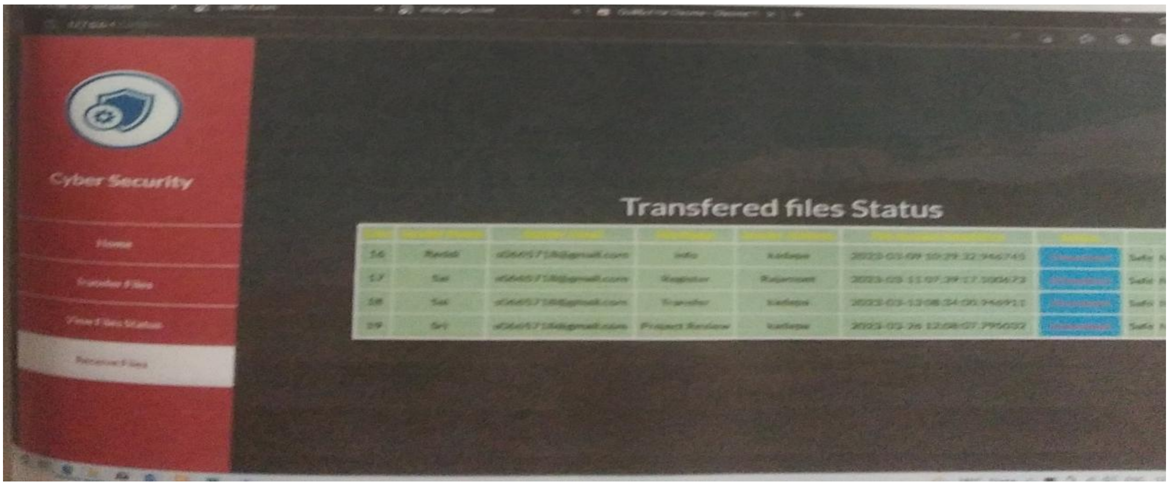
2. **User (Sender/Receiver):**

2.1 Register & Login: The user must register and login with proper information in order to submit a file to the cloud.

2.2 Transfer files via upload: Having logged in, the sender will upload the files to the cloud.

2.3 Checking the Status: The file status will be verified after the transmission.

2.4 Obtaining the file: To access the received file, the private key sent by AV is utilized.



Transfered files Status

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
16	Reddi	[illegible]@gmail.com	info	kadapa	2023-03-09 10:29:32.946745	[illegible]	Safe
17	Sai	[illegible]@gmail.com	Register	Rajampet	2023-03-11 07:39:17.100673	[illegible]	Safe
18	Sai	[illegible]@gmail.com	Transfer	kadapa	2023-03-13 08:34:00.946911	[illegible]	Safe
19	Sri	[illegible]@gmail.com	Project Review	kadapa	2023-03-26 12:08:07.795032	[illegible]	Safe

Figure 2: Received File Information: We download the file in the icon of receive files.

VII. CONCLUSION

In this study examined the features of AVs in relation to Network of Transport Systems as well as the safety and confidentiality issues that may arise with these systems. The combination of AI and security will then be covered. Additionally considered were internet-based network of Transport Systems. Finally, we noted that despite integrating security, artificial intelligence, and cloud computing into your transportation system. As far as protecting the network of Transport Systems is concerned, we have only just begun to explore the issues. To identify and prevent the assaults, we must create ML algorithms and get awareness of the many tracks. Additionally, we must consider ways to thwart attempts to weaken the machine learning (ML) methodologies required to create intelligent internet transportation systems. Eventually, we must decide which data types to send for analytics to the secure cloud.

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] Hamlen, V. Mohan, M. M. Masud, L. Khan, B. M. Thuraisingham: Exploiting an antivirus interface. Comput. Stand. Interfaces 31(6): 1182-1189 (2009)

[7] 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] Hamlen, M. Kantarcioglu, L. Khan, B. M. Thuraisingham, Security Issues for Cloud Computing. IJISP 4(2): 36-48 (2010)

[10] 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

[13] J.Krishna, M.Rupesh Kumar Reddy, Dr.M.Rudra Kumar, "Efficient High Utility Top-K Frequent Pattern Mining from High Dimensional Datasets", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN:2456-3307, Volume2, Issue 4, pp.625-631, July-August-2017.