RESEARCH ARTICLE OPEN ACCESS

# Cyber Security and Artificial Intelligence for Cloud-based Internet of Transportation Systems

**Mrs J Sarada MCA,M.Tech,M.Phil,(Ph.D) [1] , Kadiyam Venkata Rao [2]**

[1] Associate Professor, Department of Computer Application
[2] Student, Department of Computer Application
[1], [2] ChadalawadaRamanamma Engineering College (Autonomous)

**ABSTRACT**
The Internet of Things (IoT) has major implications in the transportation industry. Autonomous Vehicles (AVs) aim at improving day-to-day activities such as delivering packages, improving traffic, and the transportations of goods. AVs are not limited to ground vehicles but also include aerial and sea vehicles with a wide range of applications. To overcome this problem we are implementing Cyber Security (CS) based data transfer to Autonomous vehicle. Here a cloud is the mediator that which transfers sender files to autonomous vehicle with more security we are using CS based algorithm (Advanced Encryption Standard) which is used to hide the transferred data into cipher text. The cipher text can be decrypted by the private key generated by sender to the particular AV.

**Keywords: -** Cyber Security, Cipher text, AES, Private key, AV.

## I. INTRODUCTION

Data Science/ML techniques are being applied to analyze the data of AVs and a challenge is to apply the stream analytics/learning techniques for transportation data. For example, how can the ML techniques be applied to the massive amounts of sensor data emanating from the AVs?. The Internet of Transportation Systems will also depend heavily on Data Science/AI/ML (Machine Learning) techniques for various applications including optimum directions, driving without a human in the loop and many more. The Adversary will learn the machine learning models that we use and try and thwart our models. Finally, while massive amounts of data are collected by the Internet of Transportation Systems, the privacy of the individuals has to be protected. We envision that much of the data sharing and analytics will be carried out using the services running in the cloud integrated with the Internet of Transportation System.This paper explores how Artificial Intelligence, Security and the Cloud can be integrated to develop Intelligent Internet of Transportation Systems. We first discuss the integration of cyber security. Next, we discuss how a secure cloud may be utilized to carried out data analytics for the Transportation Systems. We discusses security and privacy for the data Transportation Systems. We discusses how the various components (e.g., AI, Security for Cloud) can be integrated to provide Intelligent and Secure Transportation System. Autonomous Vehicles (AVs), including aerial, sea, and ground vehicles, assess their environment with a variety of sensors and actuators that allow them to perform specific tasks such as navigating a route, hovering, or avoiding collisions. So far, AVs tend to trust the information provided by their sensors to make navigation decisions without data validation or verification, and therefore, attackers can exploit these limitations by feeding erroneous sensor data with the intention of disrupting or taking control of the system. In this paper we introduce SAVIOR: an architecture for securing autonomous vehicles with robust physical invariants. We implement and validate our proposal on two popular open-source controllers for aerial and ground vehicles, and demonstrate its effectiveness.

The Internet of Transportation Systems are subject to attacks (like any cyber physical system). Streaming data is being collected from such systems including autonomous and in the future driverless vehicles. As transportation systems go electric, they need energy conservation. Threats to the security of such systems could cause massive damage including accidents, loss of lives as well as being stranded on lonely highways due to attacks on energy management.

## II. LITERATURE REVIEW

**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.**

Autonomous Vehicles (AVs), including aerial, sea, and ground vehicles, assess their environment with a variety of sensors and actuators that allow them to perform specific tasks such as navigating a route, hovering, or avoiding collisions. So far, AVs tend to trust the information provided by their sensors to make navigation decisions without data validation or verification, and therefore, attackers can exploit these limitations by feeding erroneous sensor data with the intention of disrupting or taking control of the system. In this paper we introduce SAVIOR: an architecture for securing autonomous vehicles with robust physical invariants. We implement and validate our proposal on two popular open-source controllers for aerial and ground vehicles, and demonstrate its effectiveness.

**Cyber Security Based on Artificial Intelligence for Cyber-Physical Systems**

The ten papers in this special issue focus on cybersecurity for cyber-physical systems (CPSs). The systems have become very complex, more sophisticated, intelligent and autonomous. They offer very complex interaction between heterogeneous cyber and physical components; additionally to this complexity, they are exposed to important disturbances due to unintentional and intentional events which make the prediction of their behaviors a very difficult task. Meanwhile, cyber security for CPS is attracting the attention of research scientists in both industry and academia since the number of cyber-attacks have increased and their behaviors have become more sophisticated, commonly known as zero-day threats. The papers in this issue aim to bring together researchers from academic and industry to share their vision of AI application in the cyber security context, and present challenges and recent works and advances related to AI-based cyber security applied to CPSs.

**M. Masood, L. Khan, and B. Thuraisingham, Data Mining Applications in Malware Detection, CRC Press 2011.**

Data mining is the process of posing queries to large quantities of data and extracting information, often previously unknown, using mathematical, statistical, and machine learning techniques. Data mining has many applications in a number of areas, including marketing and sales, web and e-commerce, medicine, law, manufacturing, and, more recently, national and cyber security. For example, using data mining, one can uncover hidden dependencies between terrorist groups, as well as possibly predict terrorist events based on past experience. Furthermore, one can apply data mining techniques for targeted markets to improve e-commerce. Data mining can be applied to multimedia, including video analysis and image classification. Finally, data mining can be used in security applications, such as suspicious event detection and malicious software detection. Our previous book focused on data mining tools for applications in intrusion detection, image classification, and web surfing. In this book, we focus entirely on the data mining tools we have developed for cyber security applications.

**Bayesian network based analysis of cyber security impact on safety**

Cyber security gains further importance regarding life cycle risk analysis of technical systems, e.g. Cyber Physical Systems (CPS) or Systems of Systems (SoS) in the context of increasing dependency on networked systems and processes in domains like industry 4.0 or smart home. At the same time, the operation of networked systems in environments critical to safety poses the challenge of analyzing a growing number of potential interactions between safety and security aspects. In industrial environments, the assessment of functional safety is a standard procedure, e.g. using IEC 61508 and domain-specific derivatives, while cyber security in safety relevant domains has only been introduced in the last few years. The assessment of cyber security is a rapidly developing discipline, but until now there have been only few approaches to merge the standardized procedures in safety and security. This

paper presents an approach based on Bayesian Networks (BN) that enables to consider the impact of cyber security threats on functional safety considerations. By means of a simplified x-by-wire system, safety and security relations as well as structures are derived and an integrated safety and security BN is established. It is shown that parameter learning in BN can be used to adapt chosen target parameters to a required integrated safety and security level. Thus, it is possible to enhance the system configuration considering new cyber security threats.

## III. SYSTEM ANALYSIS

**Existing Method:**

In the previous development IOT is been used to store the data which will be transferred to autonomous vehicle. But this system have some drawbacks regarding security during data transfer.

**Disadvantages:**

- Less security
- Improper data transfer
- More cyber attacks

**Proposed System:**

In proposed system we are implementing Cyber Security (CS) based data transfer to Autonomous vehicle to overcome the existing problems. Here a cloud is the mediator that which transfers sender files to autonomous vehicle with more security we are using CS based algorithm (Advanced Encryption Standard) which is used to hide the transferred data into cipher text. The cipher text can be decrypted by the private key generated by sender to the particular AV.

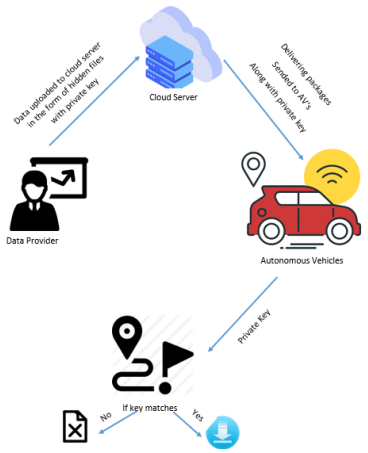


**Fig 1. Block diagram of proposed method**

**Advantages**:

- More Security
- Accurate data transfer
- Less cyber attacks

## IV. SECURITY AND PRIVACY

One of the approaches to the security and privacy of the Internet of Transportation Systems is to build a reference monitor using a Physics-Based Anomaly

Detection (PBAD) algorithm for ground and aerial AVs [1]. The algorithm will consist of three parts: (i) Building a model offline of the AV's physical invariants, (ii) Implementing an online tool to monitor expected and observed behavior to detect anomalies, and (iii) Raising an alarm if significant residual difference exists between executions. The techniques have been applied both for ground and Ariella AVs. Below we provide more details of the steps. (i) Offline pre-processing: The AV's invariants are calculated using a well-known non-linear model for aerial and ground vehicles. Accelerometer, gyroscope and magnetometer sensor data on the x, y, and z axis is used for the aerial vehicle. Vehicle position and steering angle is used for the ground vehicle. (ii) Online stage: An Extended Kalman Filter (EKF) is used to predict AV's physical behavior by estimating unknown parameters from noisy sensor input. The algorithm is divided into two sections that predicts and corrects the estimation before it is compared against the sensor data. (iii) Anomaly detection: A CUSUM algorithm is then used to detect persistent attacks. An alarm is raised if the residual difference is larger than a predefined threshold. Beyond the security of individual vehicles, the transportation sector could greatly benefit from a supporting infrastructure that allows communication between vehicles, motion sensors on lamp posts, and surveillance cameras (to name a few) to help identify traffic jams, re-route vehicles and increase vehicle safety. From the user's perspective, privacy concerns arise from all the information needed by such system that could lead to private information being exposed such as vehicle identification and driving patterns. Legislators, engineers and scientists should keep privacy concerns in mind as advances in IoT become more prominent in day-to-day activities. This will aid in improving the public perception, reduce hesitation from consumers and increase the adoption rate of new technologies [4].

## V. INTEGRATING AI AND SECURITY

Data Science/ML techniques are being applied to analyze the data and a challenge is to apply the stream analytics/learning techniques for transportation data. The main question is to understand the nature of the complex transportation data and adapt the stream analytics techniques and apply them on the massive amounts of heterogeneous sensor data being collected. Such data will often emanate as data streams. Therefore, many of the techniques for stream-based machine learning need to be examined [10]. In addition, deep-learning based techniques developed for IoT systems need to be examined [11]. The Internet of Transportation Systems will depend heavily on Data Science/AI/ML techniques for various applications including optimum directions, driving without a human in the loop and many more. The adversary will be learning the models used by the vehicles as well as learn about the data used in the training of the models. The adversary will attempt to thwart the vehicle's learning process. Therefore, the learning algorithms have to adapt to thwart the adversary's actions. Eventually it becomes game playing between the adversary and the vehicle's machine learning algorithms [3]. While massive amounts of data are collected by the Internet of Transportation systems, the privacy of the individuals have to be protected. As more and more sensor data are collected, the storage on the AVs will not be sufficient to store all of the data. We envision an encrypted cloud storage component where older data and/or less frequently accessed data are pushed to the cloud. Based on the access control policies, local applications running on the AVs will be given access to some of the collected data. When needed, these AVs will be allowed to access some of the encrypted data stored in the cloud via a simple query interface. We envision that much of the data sharing and analytics will be carried out using the services running in the cloud [8]

## VI. CONCLUSION

Herewe implemented Cyber Security (CS) based data transfer to Autonomous vehicle system. Cloud is used has mediator to transfers files from sender to autonomous vehicle with more security using CS based algorithm (Advanced Encryption Standard) for converting data into cipher text. The cipher text is decrypted by the private key generated by sender to the particular AV.

## REFERENCES

[1] IBM, "Smarter Cities," 2017. [Online]. Available: https://www. ibm.com/smarterplanet/us/en/smarter cities/overview/

[2] B. Telecom, "BT CityVerve Portal," 2017. [Online]. Available: https://portal.bt-hypercat.com/

[3] S. de Luca, R. D. Pace, A. D. Febbraro, and N. Sacco, "Transportation Systems With Connected and Non-Connected Vehicles: Optimal Traffic Control," in 2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS). Naples, Italy: IEEE, June 2017, pp. 13–18.

[4] H. Qin and C. Yu, "A Road Network Connectivity Aware Routing Protocol for Vehicular Ad Hoc Networks," in 2017 IEEE International Conference on Vehicular Electronics and Safety (ICVES). Vienna, Austria: IEEE, June 2017, pp. 57–62.

[5] M. Alam, J. Ferreira, and J. Fonseca, "Introduction to Intelligent Transportation Systems," in Intelligent Transportation Systems. Springer, 2016, pp. 1–17.

[6] A. Munir, "Safety Assessment and Design of Dependable Cybercars: For today and the future," IEEE Consumer Electronics Magazine, vol. 6, no. 2, pp. 69–77, April 2017.

[7] K. B. Kelarestaghi, K. Heaslip, and R. Gerdes, "Vehicle Security: Risk Assessment in Transportation," arXiv preprint arXiv:1804.07381, 2018.

[8] L. Figueiredo, I. Jesus, J. A. T. Machado, J. R. Ferreira, and J. L. M. de Carvalho, "Towards the development of intelligent transportation systems," in ITSC 2001 IEEE Intelligent Transportation Systems., Aug 2001, pp. 1206–1211.

[9] J. B. Kenney, "Dedicated Short-Range Communications (DSRC) Standards in the United States," Proceedings of the IEEE, vol. 99, no. 7, pp. 1162–1182, July 2011.

[10] SAE, "Dedicated Short Range Communications (DSRC) Message Set Dictionary," 2016. [Online]. Available: https://www.sae.org/ standards/content/j2735 201603/

[11] K. M. Bayarou, "E-Safety Vehicle Intrusion Protected Applications," 2008. [Online]. Available: https://www. evita-project.org/index.html

[12] T. Wollinger, "OVERSEE - Open Vehicular Secure Platform," 2010. [Online]. Available: https://www.oversee-project.com/ index.html

[13] J. M. d. Fuentes, A. I. Gonz ´alez-Tablas, and A. Ribagorda, "Overview of Security Issues in Vehicular Ad-Hoc Networks," 2010.

[14] L. He and W. T. Zhu, "Mitigating DoS Attacks Against SignatureBased Authentication in VANETs," in 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE). Zhangjiajie, China: IEEE, May 2012, pp. 261–265.

[15] B. Poudel and A. Munir, "Design and Evaluation of a Reconfigurable ECU Architecture for Secure and Dependable Automotive CPS," IEEE Transactions on Dependable and Secure Computing, 2018.

[16] Satish, Karuturi S R V, and M Swamy Das. "Quantum Leap in Cluster Efficiency by Analyzing Cost-Benefits in Cloud Computing." In Computer Science and Engineering by Auroras Scientific Technological & Research Academy Hyderabad, vol. 17, no. 2, pp. 58-71. Accessed 2018.