IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

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

1Pasupuleti Sushma Satya, 2Dr.S.Jhansi Rani, 3S.Nandini

1Masters of Technology, 2Professor, 3Research Scholar

1Andhra University,

2Andhra University,

3Andhra University

***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. The IoT systems consisting of a collection of AVs have come to be known as the Internet of Transportation systems. While such IoT systems manage large quantities of sensor data, much of the data is also sent to a cloud for offline analysis. While there is great potential in AVs and the improvements it can make to the transportation industry, security and privacy concerns pose new challenges that need to be addressed as we move forward. In addition, Artificial Intelligence techniques are also becoming crucial for such IoT systems to be able to intelligently manage the AVs. This paper discusses AI and security for cloud-based Internet of Transportation Systems.**

Keywords*— *Cyber Security, Artificial Intelligence, AI, Cloud Internet of Transportation

1 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.

2 LITERATURE REVIEW

Cyber Security Based on Artificial Intelligence for Cyber-Physical Systems

The ten papers in this special issue focus on cyber security 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.

2.1 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 analysing 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.

2.2 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

2.3 PROPOSED METHOD

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.

ADVANTAGES:

- More Security
- Accurate data transfer
- Less cyber attack

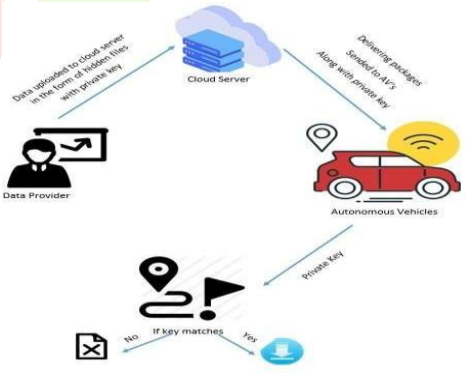

Figure 1

2.4 AES Algorithm

The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data. The data to be encrypted. This array we call the state array. You take the following aes steps of encryption for a 128-bit block: Derive the set of round keys from the cipher key. Initialize the state array with the block data (plaintext). Add the initial round key to the starting state array. Perform nine rounds of state manipulation. Perform the tenth and final round of state manipulation. Copy the final state array out as the encrypted data (cipher text). The reason that the rounds have been listed as "nine followed by a final tenth round" is because the tenth round involves a slightly different manipulation from the others. The block to be encrypted is just a sequence of 128 bits. AES works with byte quantities so we first convert the 128 bits into 16 bytes. We say "convert," but, in reality, it is almost certainly stored this way already. Operations in RSN/AES are performed on a two-dimensional byte array of four rows and four columns. At the start of the encryption, the 16 bytes of data.

2.5 MODULES

1. Cloud Server:

1.1 Views data transferred by user:

Here data sender (user) will send the particular file to cloud.

1.2 Files transferring to AV:

Cloud will transfer the file from the sender side to AV.

1.3 Status tracking:

Once after sending the file status can be tracked as either the file is sent or in pending.

2. Autonomous Vehicle:

AV will view the received files and send information to receiver through mail along with a private key to view the file data.

3. User(Sender/Receiver)

3.1 Register & Login:

User will register and login with the valid data to send a file to cloud

3.1 upload transfer files:

Once after login sender will transfer the files to cloud.

3.2 Status Checking:

After transferring the file status will be checked.

3.3 Receiving the file:

With the use of private key sent by AV is used to view the received file.

3 OUTPUT

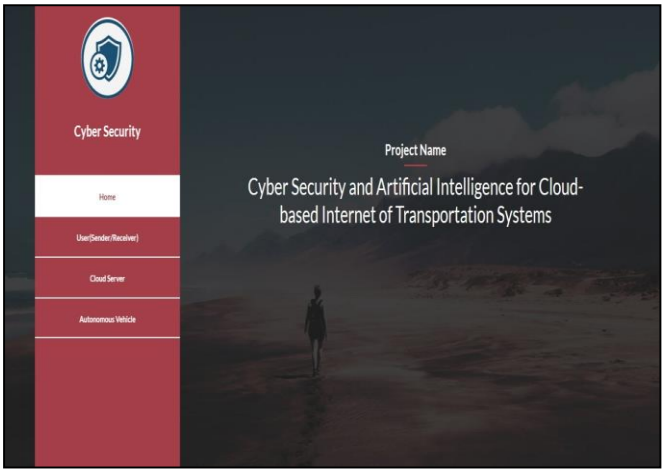

Figure 2

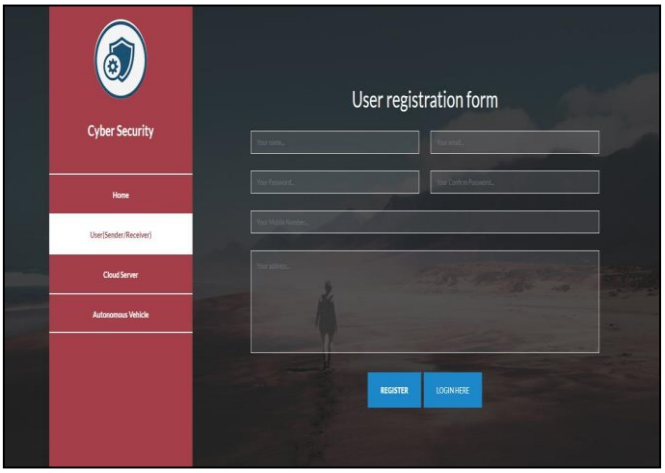

Figure 2.1

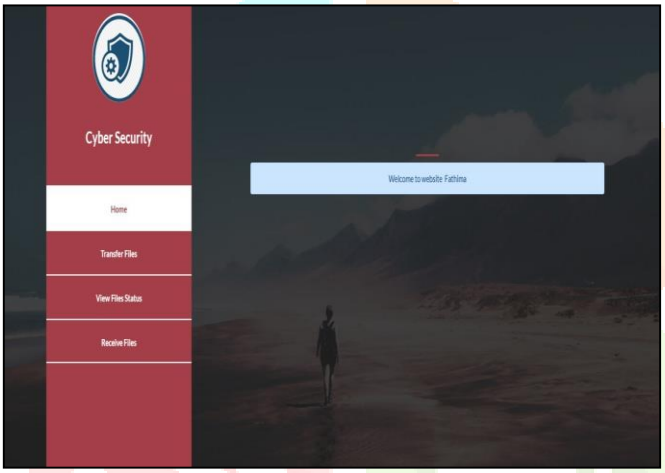

Figure 2.2

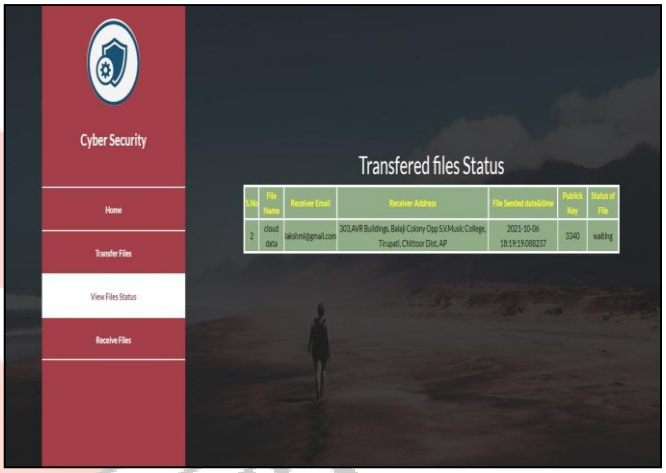

Figure 2.3

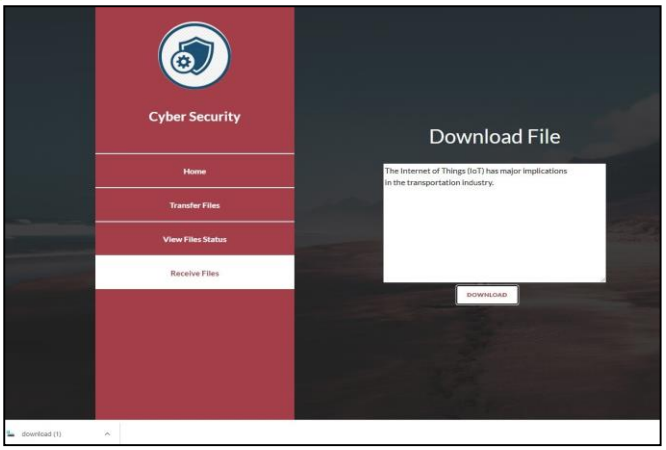

Figure 2.4

4 CONCLUSION

Here we 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.

This paper has discussed the characteristics of the Internet of Transportation Systems with respect to AVs as well as the security and privacy concerns of such systems. Next, we discuss how AI and Security may be integrated. Cloud-based Internet of Transportation Systems were also discussed. Finally, we discussed how AI, Security and the Cloud may be integrated with the Internet of Transportation Systems. We have only scratched the surface with respect to securing the Internet of Transportation Systems. We have to understand the various types of tracks and develop ML techniques to detect and prevent the attacks. We also have to examine how to handle the attacks on the ML techniques that are needed for the development of Intelligent Internet of Transportation Systems. Finally, we need to determine the types of data to send to the secure cloud for carrying out analytics.

4.1 FUTURE SCOPE

In future we can implement the process by transferring different type of data(Audio, Video, Images) with more security.

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

[2] Y. Zhou, M. Kantarcioglu, B. M. Thuraisingham, B. Xi, Adversarial support vector machine learning. ACM KDD 2012: 1059-1067

[3] 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.

[4] B. M. Thuraisingham, P Pallabi, M. Masud, L. Khan, Big Data Analytics with Applications in Insider Threat Detection, CRC Press, 2017.

[5] 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)

[6] 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)

[7] 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