International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST

Advanced Machine Learning Techniques for Predicting a Student's Performance in A University

Cheepurupalli Durga Pradeep[1], Barma Bharath[2], R.Yogitha[3]
(UG Student)[1&2] (Professor)[3]
Department of Computer Science, Sathyabama Institute of Science & Technology, India

Article Info
Volume 9, Issue 5
Page Number : 212-218

Publication Issue
September-October-2022

Article History
Accepted : 05 Sep 2022
Published : 23 Sep 2022

ABSTRACT

The Internet of Things has a big influence on the transportation industry (IoT). Autonomous vehicles (AVs) are designed to improve a variety of daily activities, such as package delivery, traffic flow, and freight transportation. Aside from being on the ground, AVs may also be in the air or underwater, and they have a wide range of applications. To address this problem, we are employing data transfer to autonomous cars based on cyber security (CS). In this instance, a cloud serves as an intermediary to transmit files to an autonomous vehicle. We use the CS-based Advanced Encryption Standard algorithm to further secure the communication by converting the supplied data into cipher text. The encrypted content may be decrypted using the sender's private key created for that particular AV.

Keywords : Cyber Security, Cipher text, AES, Private Key, AV.

I. INTRODUCTION

The number of AVs has increased dramatically in recent years. Businesses are spending a lot of money on AVs.

Despite the promise of AVs and the advantages they might bring to the transportation sector, security and privacy issues present additional difficulties that must be resolved. The sensors are vulnerable to intentional manipulation (e.g., IMUs are susceptible to sound waves and GPS receptors are susceptible to spoofing signals). Before acting on sensor signals, vehicles should make sure they're accurate.

Attacks are possible on the Internet of Transportation Systems (like any cyber-physical system). Such technologies, such as autonomous and in the future, driverless automobiles, are collecting streaming data. Energy conservation is necessary when transportation systems transition to electricity. Due to assaults on energy management, threats to the security of such systems might result in accidents, loss of life, and being trapped on isolated roadways, among other grave consequences.

The objective is to apply stream analytics/learning approaches to transportation data while using data science/ML to examine AV data. How, for instance, might the ML approaches be used to process the vast volumes of sensor data coming from the AVs? For a variety of applications, such as providing the best

instructions, driving without a person in the loop, and many more, the Internet of Transportation Systems will also largely rely on Data Science/AI/ML (Machine Learning) approaches. The adversary will become familiar with our machine learning models and attempt to undermine them. The privacy of the person must be maintained even if the Internet of Transportation Systems captures enormous quantities of data. We anticipate that the cloud-based services coupled with the Internet of Transportation System will be used for a large portion of data exchange and analytics.

This study investigates the integration of artificial intelligence, security, and the cloud to create intelligent internet transportation systems. The integration of cyber security is the first topic we cover. Next, we go into how data analytics for transportation systems may be done via a secure cloud. We talk about privacy and security for data transportation systems. We go over how the various elements (such as AI and cloud security) may be combined to create intelligent and secure transportation systems.

II. RELATED WORKS

Securing Autonomous Vehicles with a Robust Physics-Based Anomaly Detector: Autonomous vehicles (AVs), which include air, sea, and land vehicles, use a range of sensors and actuators to analyze their surroundings in order to carry out particular tasks like navigating a route, hovering, or avoiding collisions. As long as AVs continue to rely on sensor data without data validation or verification, attackers can take advantage of these weaknesses by providing false sensor data to the system with the goal of causing disruption or taking over control. Using solid physical invariants, SAVIOR is an architecture for securing autonomous cars that we describe in this work. On two well-known open-source controllers for aerial and ground vehicles, we put our suggestion into practice, confirm it, and show how well it works.

Cyber Security Based on Artificial Intelligence for Cyber-Physical Systems: Ten pieces are included in this special issue, all of which discuss cyber security for cyber-physical systems (CPSs). Systems nowadays are far more sophisticated, intricate, autonomous, and intelligent. They include very intricate interactions between various cyber and physical components; in addition to this complexity, they are subject to significant disruptions as a result of purposeful and inadvertent occurrences, making it exceedingly challenging to forecast their behavior. As a result of the rise in cyber-attacks and the sophistication of their activities, sometimes known as zero-day threats, research scientists in business and university are becoming more interested in cyber security for CPS. The articles in this issue seek to bring together academic and industrial researchers to discuss their vision of AI application in the context of cyber security, and showcase problems and current efforts and advancements related to AI-based cyber security applied to CPSs.

Data Mining Applications in Malware Detection: The practice of asking questions about vast amounts of data and extracting information—often previously undiscovered—using mathematical, statistical, and machine learning approaches is known as data mining. Numerous industries, including marketing and sales, online and e-commerce, medical, law, manufacturing, and, more lately, national and cyber security, can benefit from data mining. Data mining, for instance, may be used to identify unrecognized connections between terrorist organizations and even forecast terrorist activities based on prior incidents. To enhance e-commerce, one may also use data mining techniques for specific markets. Multimedia applications such as video analysis and picture classification can benefit from data mining. Data mining may also be employed in security applications including the identification of dangerous software and suspicious events. In our last book, we concentrated on data mining technologies for applications in online

browsing, picture categorization, and intrusion detection. We only highlight the data mining technologies we have created for cyber security applications in this book.

Bayesian network-based analysis of cyber security impact on safety: With the consideration of life cycle risk analysis of technical systems, such as Systems of Systems (SoS) or Cyber-Physical Systems (CPS) are terms used to describe the growing reliance on networked systems and processes in fields like industry 4.0 or smart homes. The problem of examining an increasing number of possible linkages between safety and security elements arises when networked systems are used in contexts where safety is crucial. The assessment of functional safety is a regular technique in industrial settings, e.g. using IEC 61508 and domain-specific derivatives, but cyber security in safety-relevant domains has just recently been introduced. Although cyber security assessment is a fast-evolving field, there have only been a few attempts to combine standardized security and safety standards. In this study, a method based on Bayesian Networks (BN) is presented for taking into account how functional safety concerns are impacted by cyber security risks. Integrated safety and security BN is created using a reduced x-by-wire approach to infer safety and security relations as well as structures. The ability to modify selected target parameters to a necessary integrated safety and security level using BN's parameter learning has been shown. As a result, the system configuration may be improved while taking new cyber security risks into account.

SecAI: Integrating Cyber Security and Artificial Intelligence with Applications in the Internet of Transportation and Infrastructures: The topic of intelligent transportation systems (ITS), which is still in its infancy, is distinguished by sophisticated data models, dynamics, and stringent time constraints. The efficiency and safety of transportation depend on the complicated challenge of ensuring cyber security in ITS. One of the crucial phases in the development of ITS is the imposition of standards for a complete architecture as well as specialized security requirements. The paper looks at ITS architecture's broad contours and security concerns. The setup and initialization of the devices during manufacture at the perception layer, as well as anonymous authentication of nodes in VANET at the network layer, are the key objectives of security techniques; Fog-based structural defense at the support layer, definition and standardization of the intricate data and metadata model, and AI-based system defense at the application layer. The article discusses certain traditional techniques that should be modified and used in ITS cyber security, such as network segmentation and cryptography. The emphasis is on cutting-edge solutions that have recently been attempting to find a place in ITS security plans. Blockchain, bloom filters, fog computing, artificial intelligence, game theory, and ontologies are a few of these methods. In conclusion, a connection is drawn between the approaches that are discussed, the issues they address, and the architectural levels where they are used.

III. Methodology

Proposed system:

We are implementing CS-based data transfer to autonomous cars in the suggested solution to overcome the problems. In this instance, a cloud serves as an intermediary to transmit files to an autonomous vehicle. We use the CS-based Advanced Encryption Standard algorithm to further secure the communication by converting the supplied data into cipher text. The encrypted content may be decrypted using the sender's private key created for that particular AV.

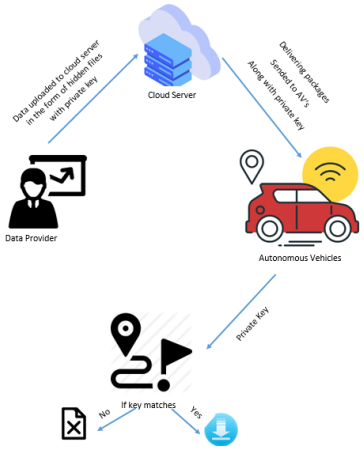


Figure 1: Block diagram

IV. IMPLEMENTATION

The project has been implemented by using the below-listed algorithm.

1. AES Algorithm

Round keys are a specific collection of specially generated keys used in the encryption process. These are used on a data array that contains exactly one data block, along with additional operations. The encrypted data. We refer to this array as the state array.

You do the AES encryption methods below for a 128-bit block:

- From the cipher key, get the set of round keys.
- Use the block data to initialize the state array (plaintext).
- Include the starting state array with the initial round key.
- Manage the state for nine iterations.
- Complete the eleventh and last state manipulation.
- Export the encrypted data as a copy of the final state array (ciphertext).

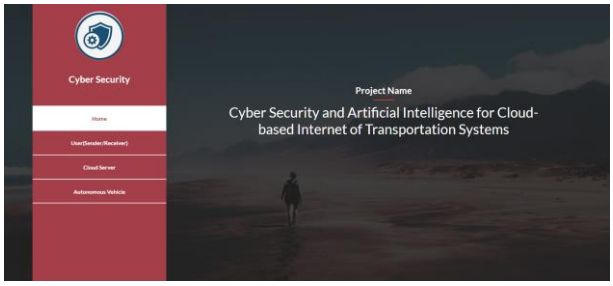
The tenth round includes a slightly different manipulation from the other nine rounds, which is why the rounds are labeled as "nine followed by a final tenth round."

There are only 128 bits in the block that has to be encrypted. We first divide the 128 bits into 16 bytes because AES only works with byte amounts. Although we say "convert," data is probably definitely already saved in this manner. A two-dimensional, four-row, four-column byte array is used for operations in RSN/AES. The 16 bytes of data were encrypted at the beginning.

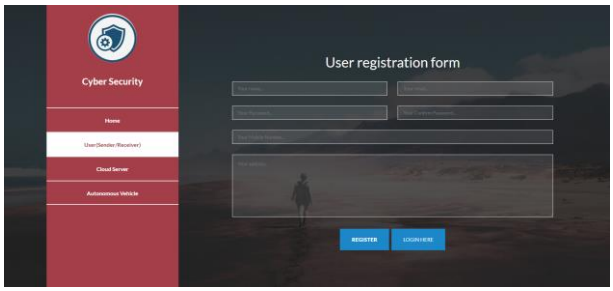
V. Results and Discussion

The following screenshots have depicted the flow and working process of the project.

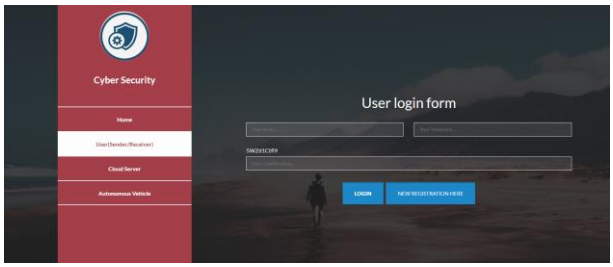
Home Page: This is the home page of cyber security and artificial intelligence for cloud-based internet of transportation systems.



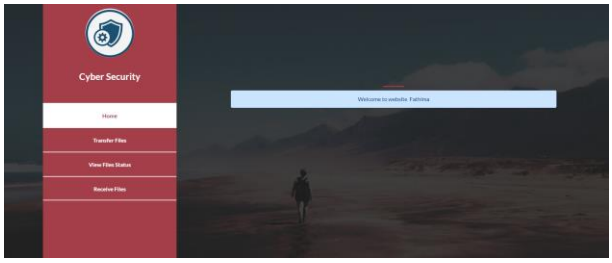
User registration page: The user can get registered into the application.



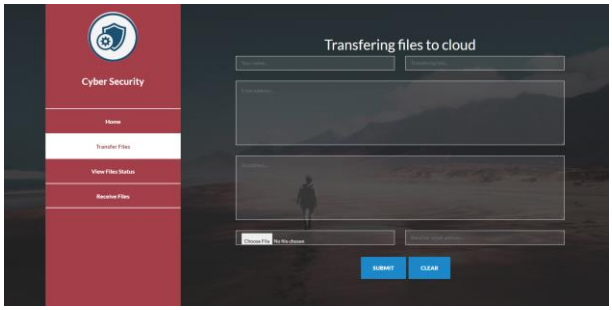
User registration form: The user needs to fill up this registration form for registration.



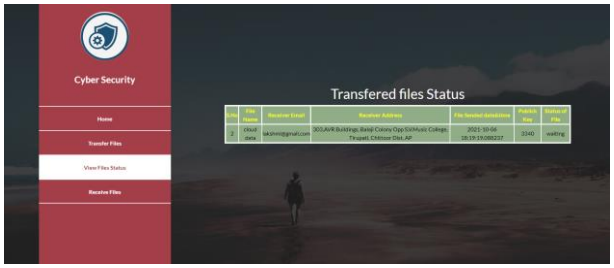
User home page: After successful login user can view this home page.



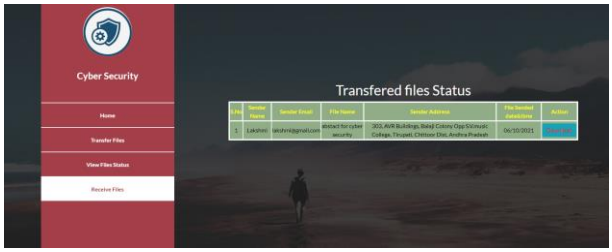
Upload transferring files: Files get uploaded from this page.



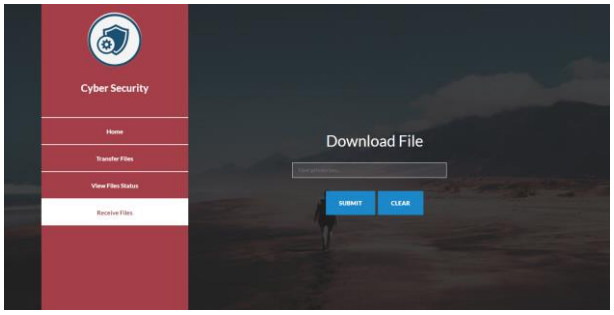
Transferring files status tracking: This page shows the status of transferring files.

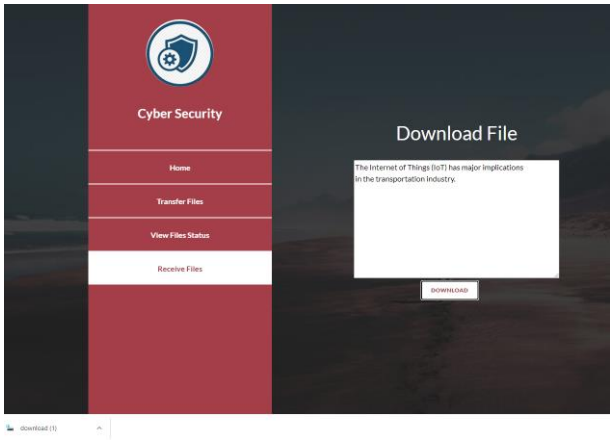


Received files information: Here we can see the received files information.

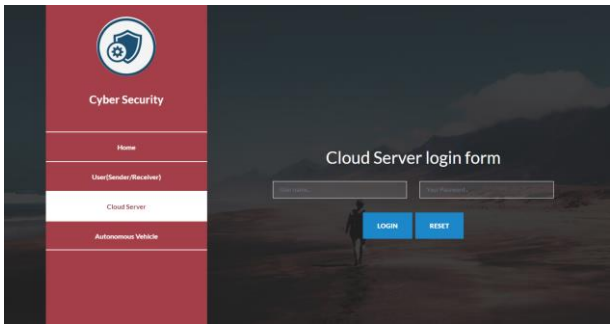


Downloading file: Files can download from this page.

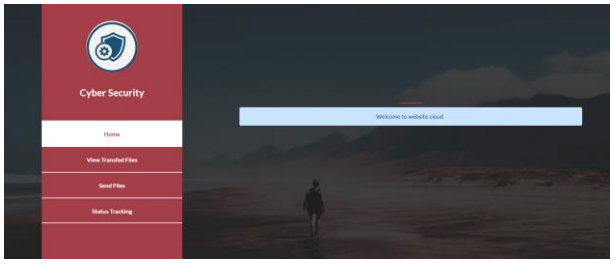




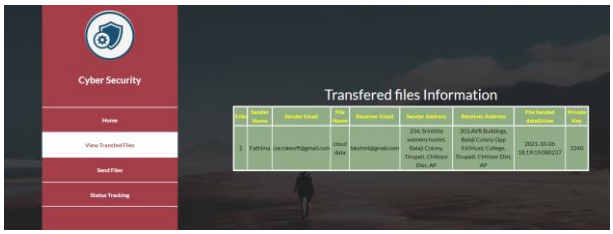
Cloud server login page: Here cloud server can log in with valid credentials.



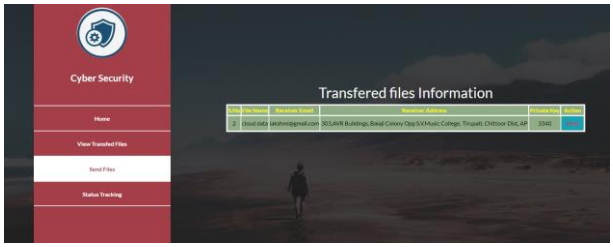
Cloud server home page: After login cloud server can view this home page.



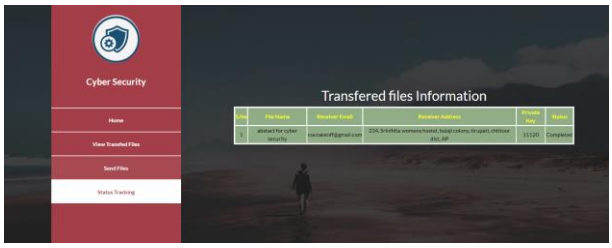
View transferring files: The cloud server can view the transferring files.



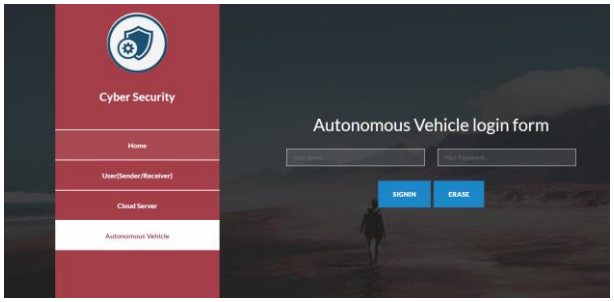
Send files: Files will be sent from this page.



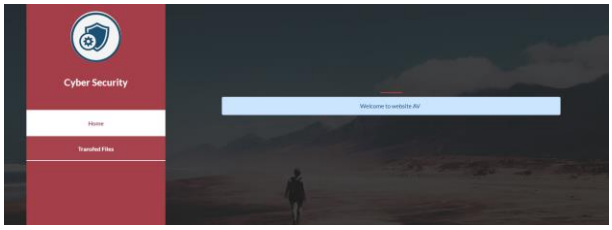
Status tracking: This page displays the status tracking of sending files.



Autonomous vehicle login page: Autonomous vehicle can log in with valid credentials.



Av home page: After login Autonomous vehicle can view the home page.



Sent transferring the file to the user: Here AV can transfer files to the user.

VI. CONCLUSION

Here, we implemented Cyber Security (CS) based data transfer to an Autonomous vehicle system. AES-based CS-based algorithm (Advanced Encryption Standard) is employed as a mediator in the cloud to more securely transfer files from the sender to the autonomous car. The private key created by the sender and given to the specific AV is used to decrypt the encrypted text.

VII. REFERENCES

[1]. R. Using a Powerful Physics-Based Anomaly Detector to Secure Autonomous Vehicles, Quinonez, J. Giraldo, L. Salazar, E. Bauman, A. Cardenas, and Z. Lin. USENIX Security Symposium's 29th annual (USENIX Security 20). Boston, MA, August 2020.

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

[3]. Y. Adversarial support vector machine learning by Zhou, M. Kantarcioglu, B. M. Thuraisingham, and B. Xi. 2012 ACM KDD: 1059–1067.

[4]. B. SecAI: Integrating Cyber Security and Artificial Intelligence with Applications in Internet of Transportation and Infrastructures, M. Thuraisingham, Annual Conference, Clemson University Center for Connected Multimodal Mobility, October 2019.

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

[6]. K. Exploiting an antiviral interface by W. Hamlen, V. Mohan, M. M. Masud, L. Khan, and B. M. Thuraisingham. Comput. Stand. 31(6):1182–1189 Interfaces (2009).

[7]. L. The usefulness of perturbation-based privacy-preserving data mining for real-world data is discussed by Liu, M. Kantarcioglu, and B. M. Thuraisingham. Info Knowl Eng. 65(1): 5-21 (2008).

[8]. B. Towards a Privacy-Aware Quantified Self Data Management Framework by M. Thuraisingham, M. Kantarcioglu, E. Bertino, J. Z. Bakdash, and M. Fernández. 2018 SACMAT, pp. 173–184

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

[10]. Y. Multistream Classification for Cyber Threat Data with Heterogeneous Feature Space by Li, Y. Gao, G. Ayoade, H. Tao, L. Khan, and B. M. Thuraisingham. WWW, pp 2992-2998, 2019.

[11]. H. "Deep Residual Learning based Enhanced JPEG Compression in the Internet of Things," by Qiu, Q. Zheng, G. Memmi, J. Lu, M. Qiu, and B. M. Thuraisingham, accepted by IEEE Transactions on Industrial Informatics, 2020.

[12]. G. Decentralized IoT Data Management Using BlockChain and Trusted Execution Environment by Ayoade, V. Karande, L. Khan, and K. W. Hamlen. IRI, pages 15-22, 2018.

Cite this article as :

Cheepurupalli Durga Pradeep, Barma Bharath, R.Yogitha, "Advanced Machine Learning Techniques for Predicting a Student's Performance in A University", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 9 Issue 5, pp. 212-218, September-October 2022.
Journal URL : https://ijsrst.com/IJSRST229543