IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CLOUD-BASED AI TRANSPORTATION SYSTEM WITH CYBER SECURITY

D.Leelavathi(M.Tech)
Department of CSE
School of Engineering and Technology
Sri Padmavathi Mahila Visvavidayalayam
(women's University)
Tirupati.

Dr.N.Padmaja
Department of CSE,
School of Engineering and Technology,
Sri Padmavathi Mahila Visvavidayalayam
(women's University)
Tirupati.

B. Uma, M.Tech(Ph.D)
ASSISTANT PROFESSOR,
Department of CSE,
School of Engineering and Technology,
Sri Padmavathi Mahila Visvavidayalayam
(women's University)
Tirupati.

ABSTRACT

The Internet of Things (IoT) has significant ramifications. Autonomous vehicles (AVs) are designed to make daily tasks easier, such as delivering parcels, reducing traffic, and transporting commodities. Aerial and marine vehicles, as well as ground vehicles, are included in Autonomous Vehicles, which have a wide range of uses. We are deploying Cyber Security (CS) based data transmission to autonomous vehicles to solve this challenge. Here, a cloud serves as the intermediary, transferring files from the sender to the autonomous car. For added security, we employ a CS-based algorithm (Advanced Encryption Standard) to encrypt the transmitted data into cipher text. The private key generated by the sender to the specific Autonomous Vehicles can decipher the encryption text .While these IoT systems manage vast amounts the majority of sensor information is also sent to the cloud for delayed processing. While Autonomous Vehicles have a lot of promise in terms of the benefits they may offer Security and privacy are important to the transportation business. Issues represent

additional difficulties that must be addressed as we go. Furthermore, Ai Research approaches are becoming increasingly important for IoT systems to automatically manage AVs. This study examines artificial intelligence (AI) and security in relation The Internet of Transportation Systems is a cloud-based system.

Keywords— Cyber Security, Cipher text, AES(Advanced Encryption Standard), Private key.

1.INTRODUCTION

The Internet of Transportation Systems refers to IoT systems that include a variety of Autonomous vehicles. Internet of Transportation Networks attacks is a common occurrence. Data from technologies such as self-driving automobiles and, in the future, self-driving cars are collected in real-time. Energy-saving is a requirement for electric transportation systems. Assaults on power systems might result in massive devastation, including accidents, deaths, and being stranded on lonely highways.

Integrating cyber security with AI has three components. The first is to use Artificial Intelligence to improve cyber security, the second is to detect AI-related privacy breaches, and the third is to use AI to improve cyber security. In the mid-1990s, artificial intelligence for cyber security was first studied. The goal is to use machine learning techniques to detect illegal intrusions. In the 2000s, this study was expanded to incorporate hazard assessment and threat intelligence detection. A great deal of information on attacks is being gathered. This data must be evaluated to detect malicious attacks. Moreover, we must be able to foresee how ransomware will evolve to avoid assaults. Furthermore, streaming data is being scrutinized for potentially dangerous insiders. The safety of AI technology is the second point of worry. This topic, presently known as adversarial machine learning, has gained prominence during the previous decade.

The second element is the potential for privacy concerns as a result of using machine learning algorithms. For example, vast volumes of data may now be combined, analyzed, and various features of persons extracted. Individuals' privacy may be jeopardized as a result of this. There have been a slew of privacy-conscious machine learning (data mining) algorithms created. The difficulty is to enact proper policies so that we can gather, store, integrate, analyses, and share data in a policy-aware manner.

1.1PROBLEM DEFINITION:

This application aims to call attention to the fact that cyber security is rapidly becoming a major issue for consumers, businesses, and researchers alike. Keeping our data safe in a world when something is on the World Wide Web, from beautiful kitten videos to our vacation journals to our credit card details, is one of the most difficult tasks of Information Technology. Cyber security threats may take various forms, including ransom, phishing assaults, malicious programs, and other more complex issues.

1.2 OBJECTIVE OF THE PROJECT:

There are four basic purposes for AI in cyber security. Reaction in real-time AI allows for the speedy response to attacks to decrease danger, based on an infinite quantity of data and context. Many dangers can be immediately addressed thanks to automation, which lowers the cost of recognising and responding to them.

Massive data management: AI prioritises which situations and attacks demand immediate response and which are bogus threats, allowing the system to free up resources.

Real-time response: Based on an infinite quantity of data and information, AI enables swift action as a result of assaults to decrease danger.

Many dangers may be automatically reacted to, minimising the cost of identification and action.

Prediction: Artificial intelligence (AI) assists in the forensic examination of previous assaults, resulting in improved security.

2.LITERATURE SURVEY

2.1CYBER SECURITY AND ARTIFICIAL INTELLIGENCE:

M.Masood,L.Khan,andB.Thuraisingham(2011)Using mathematical, statistical, and machine learning approaches, The technique of asking questions of massive amounts of data and recovering previously unknown information is known as data mining.Marketing and sales, web and e-commerce, medical, law, manufacturing, and, more recently, national and cyber security are just a few of the fields in which data mining can be applied. Data mining, for example, may be used to reveal hidden ties between terrorist groups and even forecast terrorist activities based on previous occurrences. In addition, data mining techniques may be used to improve e commerce for specific markets.

B. M. Thuraisingham, SecAI (2019)In the transportation industry, the Internet of Things (IoT) has significant ramifications. Autonomous vehicles (AVs) are designed to make daily tasks easier, such as delivering parcels, reducing traffic, and transporting commodities. Aerial and marine vehicles, as well as ground vehicles, are included in AVswhich can be used in a various of ways. The Internet of Transportation systems are a type of IoT system that consists of a collection of AVs. While these IoT devices handle massive volumes of sensor data, the majority of it is also sent to the cloud for offline analysis. While AVs have a lot of promise in terms of the improvements they may bring to the sports business,Concerns about security and privacy face new difficulties that must be addressed as we move forward. For IoT systems to successfully manage Autonomous Vehicles, Artificial Intelligence techniques are becoming increasingly critical.

B.M.Thuraisingham, SecAI (2019)The perturbation technique is an important privacy protecting tool in data mining. With this method, there is always a trade-off between the loss of information and the privacy protection. The question is how far individuals are willing to give up personal privacy. This is a personal choice that differs from one individual to the next. In this study, we provide an individually configurable perturbations model that allows people to choose their own privacy degree. As a result, our methodology delivers varying privacy assurances based on the privacy preferences of the user. We put our novel perturbation model to the test by using several reconstruction approaches on perturbed data sets.

B.M.Thuraisingham,M.Kantarcioglu,E.Bertino,J.Z.Bakdash,M.Fernández(2018)The different commercial and marketing goals, massive volumes of data are collected kept and analysed. While such data analysis is necessary for many purposes, it may also infringe on people's privacy. This paper discusses the issues of creating a privacy-aware data management system for data collection, storage, and analysis. Discuss the features ofa formal system based on rewriting rules that provides a data management architecture that is privacy aware as well as behavioural aspects of data sharing.

R.Quinonez, J.Giraldo, L.Salazar, E.Bauman, A.Cardenas, Z. Lin (2020)

Aerial, maritime, and ground autonomous vehicles (AVs) use a range of sensors and actuators to analyse their surroundings and execute particular tasks like as navigating a route, hovering, or avoiding collisions. As Autonomous vehicles have traditionally relied on sensor data to make navigational choices without data validation or verification, attackers can take advantage of these flaws by supplying erroneous sensor data to interrupt or gain control of the system. We provide SAVIOR, an approach for securing autonomous vehicles with rigorous physical invariants, in this work. We illustrate the efficacy of our idea by implementing and validating it on two prominent open-source controllers for aerial and ground vehicles.

2.2 TABLE FOR GAPS IDENTIFICATION:

SNO	TITLE	DESCRIPTION	KEY FINDINGS
1.	Data Mining Applications in Malware Detection.	Tim Berners-stack Lee's and a functional design for the semantic web, in particular, are discussed in this review of semantic web technologies and the concept of semantic web services. Then there's XML, RDF, ontologies, and semantic webpage rules to consider. Finally, consider how semantic web technologies might help meaningful online applications.	The"branchfunction" obfuscation has little impact on dextor.The primary purpose of this obfuscation is to hide the control flow of an executable so that it cannot be disassembled. There is currently no universal answer to this problem. dextor is likely to yield fragmented "code blocks" in our situation, with some of the original code gone. As long as the "missed" block contains a large number of instructions, this will not affect dextor.
2.	UsingBayesian Networks for Cyber Security Analysis.	In real-time security analysis, our BN modelling technique distinguishes three 6 sources of uncertainty of The success of the attack, the uncertainty of the attacker's judgement, and the uncertainty of defective IDS sensors are all factors to consider. This permits CPT parameters to be used to be calculated using current data sources.	We describe our current attempts to identify the most relevant forms of uncertainty and to capture them using Computational methods for stronger security assessments. We construct an example neural framework based on a cyber-security graph structure, then use attack mantis and an experimental investigation to support our modelling approach.

3.	Integrating Cyber Security and Artificial Intelligence with Applications in Internet of Transportation and Infrastructures.	Have just started to expose what's underneath regarding getting Transportation Networks on the Internet. There need to comprehend the different sorts the number of tracks and foster Machine learning strategies to identify what's more forestall the assaults prevent the attacks.	While these IoT solutions handle the logistics of transportation,vast amounts of wearable sensors, most of it is also transferred to the cloud for evaluation offline. While Autonomous Vehicles have a lot of potential and can enhance the business, security and privacy issues bring additional difficulties that must be solved as we go forward.

3. OVERVIEW OF THE PROPOSED SYSTEM

3.1ARCHITECTURE OF THE PROPOSED SYSTEM:

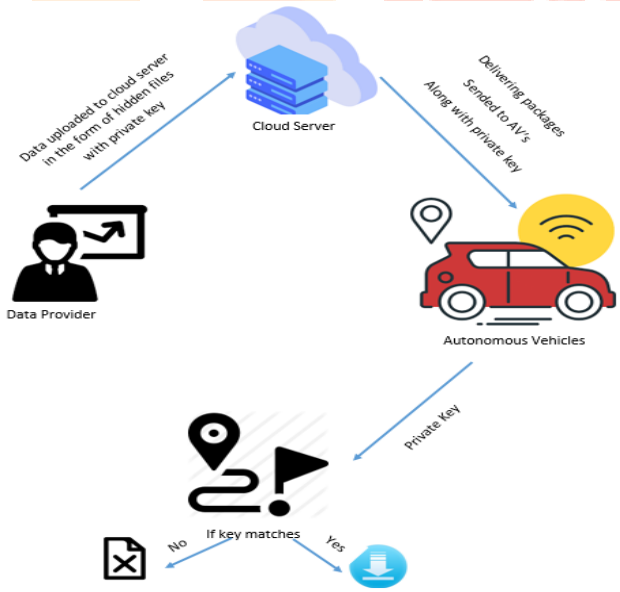

Fig 3.1 Proposed System's Arechitecture

To address current issues, we are adopting Cyber Security (CS) based data transmission to autonomous vehicles in the proposed system. Here, a cloud serves as the intermediary, transferring files from the sender to the autonomous car. For added security, we employ a CS-based algorithm (Advanced Encryption Standard) to encrypt the transmitted data into cipher text. The private key generated by the sender to the specific AV can decipher the encryption text.

3.2 ALGORITHM:

AES Algorithm

A collection of round keys, which are randomly generated keys, are used in the encryption process. These would be applied to data arrays containing exactly one block of data, as well as other processes. The information that will be encoded. This array is referred to as the state array.

For a 128-bit block, you use the following encryption steps: Make a succession of circular keys deriving from the cypher key Fill in the block data in the state array (plaintext). To the starting state array, add the initial round key. There are a total of There are a total of nine rounds of state manipulation required. The eleventh and final phase of state manipulation should be completed. As encrypted data, make a copy of the final output sequence (ciphertext). The matches are listed as "nine presented in the final tenth round" since the tenth round has a slightly different alteration than the rest.

A 128-bit sequence will be used to encrypt the block. We must first divide the 128 bits into the 16 bytes because AES works in byte increments. Although we say "convert," it is almost certainly already saved in this format. For activities, RSN/AES employs a double byte array with four rows and four columns. At the start of the encrypting process, there are 16 bytes of data.

Algorithm Flow:

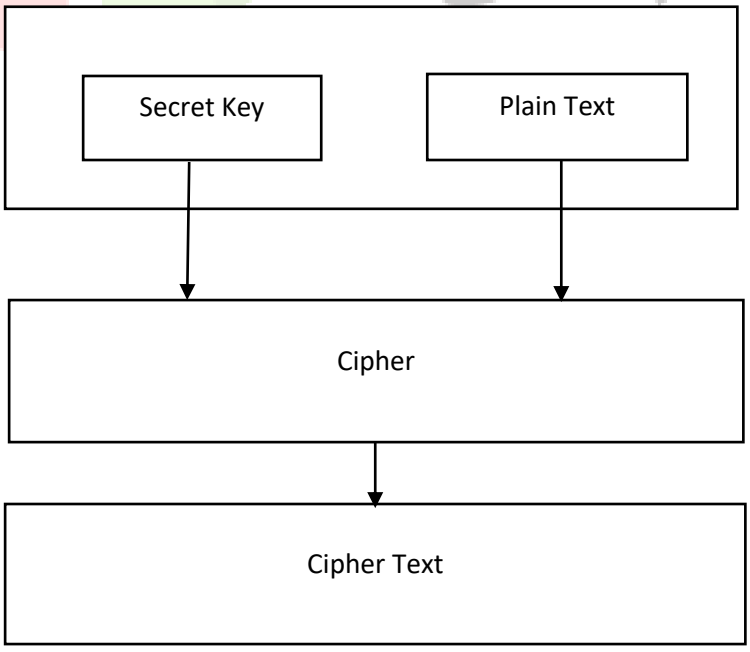

Fig: Flowchart of Algorithm

4.CONCLUSION:

We used Cyber Security (CS) to pass data to an autonomous car system. The cloud is utilised as a mediator to deliver files from a sender to an autonomous vehicle with greater security by transforming data into cypher text using a CS-based algorithm (Advanced Encryption Standard). The private key generated by the sender to the specific AV is used to decipher the encrypted text.

5.REFERENCE:

[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] 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