Researchers develop AI tool to safeguard vehicles from cyber threats

Scientists have developed an artificial intelligence scheme able to consolidate privacy of autonomous vehicles and their drivers from cyberattacks and hackers.

SHARJAH, EMIRATE OF SHARJAH, UNITED ARAB EMIRATES, November 11, 2024 /EINPresswire.com/ -- By Saad Lotfy

Scientists claim to have developed an artificial intelligence tool to consolidate the privacy of vehicles and their drivers.

How to preserve the privacy of the so-called Internet of Vehicles (IoV) has emerged as a major challenge due to geographical mobility of vehicles and insufficient resources, the scientists say.

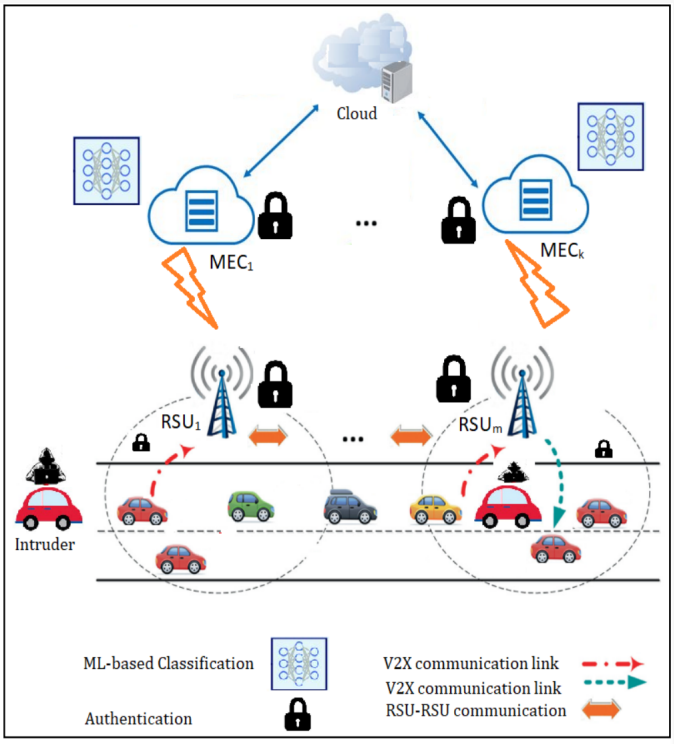

Fig. 1. Architecture of a secured distributed edge intelligence for IoV

Architecture of a secured distributed edge intelligence for IoV.

The problem has aggravated, according to the scientists, due to the "limited resources of onboard units (OBUs)" and the shortcomings of embedded sensors installed in vehicles, which "lure the adversaries to launch various types of attacks."

"Thus, lightweight but reliable authentication schemes need to be designed to combat these attacks," they write in the IEEE Internet of Things Journal. The research is co-authored by scientists from the University of Sharjah in the United Arab Emirates, the University of Maryland in the US, and Abdul Wali Khan University Mardan, Pakistan. (Original source URL: https://ieeexplore.ieee.org/abstract/document/10722874?casa_token=0iHAjeDsIeUAAAAA:3jeREtde_2B46YI6JpE_WMAzWZ0hPkgNB1OQWLgCyGHAzpvakrIokVtP6V1mmyKA7VIMl_0ypeY)

The Internet of Vehicles (IoV) refers to a network in which vehicles can communicate with each other, as well as with intelligent communication devices in parking lots, pedestrians, and road

infrastructure. This technology “has transformed cities around the globe by providing real-time communication,” the authors note.

Vehicles connected via IoV are also equipped with embedded sensors and units that collect useful data and communicate it to the closest roadside units (RSUs) or server modules. “The operational capabilities of these vehicles are further augmented by artificial intelligence, particularly machine learning and deep learning, which analyze and interpret data in real-time,” the researchers write.

The security of vehicles in the IoV age has been found to be vulnerable to cyberattacks that may cause regrettable events via interception or even alteration of vehicle-infrastructure communication. Machine Learning has been suggested as a solution, and the authors’ AI tool is promoted as such.

The autonomous vehicles today are supplied with an onboard Unit device or OBU as part of their Intelligence Transportation System or ITS.

However, the authors maintain that the communication system installed in the vehicles still encounters challenges, particularly those related bandwidth scarcity, and delays in the responses from cloud-located services within a stipulated time.

Currently available cloud servers, the authors emphasize, are yet not reliable even if supplemented with machine learning (ML) and deep learning (DL) algorithms because they are still “unable to provide swift responses to the vehicles that can lead to catastrophic circumstances at the roads.”

So are the embedded sensors on-board units (OBUs) and RSUs, which “are resource-constrained and are unable to support computationally complex security and privacy preservation schemes. It would require ample of resources for these devices to securely communicate with the cloud servers,” the authors highlight.

To addresses these challenges, the authors propose “an ML-based authentication scheme that trains and classifies the vehicles at the edge servers in a distributed manner, preserves the privacy of communicating entities and minimizes the bandwidth consumption and delay experienced by the vehicles.”

For this purpose, the authors design a new machine learning-based authentication mechanism to solve privacy and security issues which the emerging Internet of Vehicle (IoV) ecosystem is currently grappling with.

The research team conducted its experiments in a simulated environment using comparative analysis of the proposed scheme with “the existing state of-the-art schemes in terms of communication, processing, and storage overheads.

“Simulation results have concluded that the proposed scheme is not only pruned against well-known intruder attacks, but it is equally lightweight and effective concerning various performance evaluation metrics such as computation, communication, and storage overheads”.

The authors emphasize the scheme they have developed solves the issue of bandwidth scarcity and excessive delays vehicles currently experience when communicating via cloud servers.

“The ML-based approach extends the decision power of vehicles and edge servers to identify adversaries. Our scheme requires that each vehicle participates in an offline phase, where a trusted authority shares a list of MaskIDs and secret keys of legitimate vehicles and edge servers,” they stress.

The proposed scheme requires each vehicle to participate in an offline phase, where a trusted authority shares a list of masked identities or MaskIDs and secret keys of legitimate vehicles and edge servers.

Once vehicles and servers have their unique list of masked identities, they can authenticate each other without needing to rely on cloud servers, ensuring faster and more efficient communication.

When a vehicle starts to communicate, the nearest edge server verifies its identity using the MaskIDs and secret keys, reducing the computational load on the vehicle.

The scientists explain, “In our scheme, each vehicle and edge server (via RSU) is equipped with an ML algorithm to classify adversaries from legitimate ones.”

The machine learning algorithm analyze and verify communication patterns in real-time, strengthening security against common cyber-attacks including man-in-the-middle or impersonation attacks.

What makes the approach stand out in comparison with currently available tools is the embedding of a timespan “in the payload of each encrypted message to prune the proposed scheme against well-known adversarial attacks.

“The simulation results verify the exceptional performance of our scheme in terms of computational overhead, communication overhead, and storage overhead,” according to the research.

LEON BARKHO
University Of Sharjah
+971 50 165 4376

email us here