# Automotive Industry Standard (AIS) 140 Encrypted Device Communication to Increase Privacy, Integrity and Confidentiality of Data

Barkha Airan[1], Mohit Agrawal[2]

[1]*Department of Computer Science and Engineering, Pacific Institute of Technology Udaipur, Rajasthan, India*
[2]*Department of Computer Science and Engineering, University College of Engineering, Kota, Rajasthan, India*

***Abstract*-In world of software development security of data flow is very important. Authentication of IOT devices is very important. Mutual Authentication is so necessary between IoT devices and IoT server to make communication more reliable and secure. By using encryption and decryption at the end of device and server we can increase the authenticity of system. In this research paper we will use single password key mechanism for the authentication of AIS devices.**

***Keywords:*-AIS 140 device Authentication, AIS 140 Security, Internet of things, Intelligent Transport System, Vehicle tracking system, Encrypted communication, Secure Manufacturing Unit.**

## I. INTRODUCTION

Automotive Industry Standard 140 (AIS 140) is a set of standards published by Automotive Research Association of India (ARAI). It is used for **vehicle tracking system**, **camera surveillance system**, and **emergency request button**. The government has directed every state's public transport department to make sure that all **passenger carrying buses** conform to the **AIS 140 guidelines by 1st April 2018**.

Every bus will need to have a GPS tracking system, camera surveillance and an emergency button. By using this department can track the bus and send the help in case of accident. It also enable the passengers to apprise the control room of any kind of emergencies.

Both the existing vehicles as well as the future ones will be required to be fitted with GPS and emergency button. This implies that the automotive OEMs along with aftermarket companies and Tier-1 suppliers need to have these systems ready.

The AIS devices communication protocol data frame format use 15 digit standard unique IMEI number along with every packet for identification of data packet.

Device must transmit the Login message whenever it establishes (re-establishes after disconnection) its connectivity with Server with the specified fields. Login Message will carry following information:

$DeviceName –Vehicle number on which the device is installed

$IMEI –15 Digit IMEI number

$Firmware – Version of the firmware used in the hardware

$Protocol -Version of the frame format protocol.

$LastValidLocation – Last location info saved at the device.

The data value can be either in American Standard Code for Information Interchange (ASCII) or in HEX format [1].

In either mentioned format of data frame IMEI number (device identification) can easily identified. So IMEI number can be easily imitate by the third party or attacker. Which can lead to ambiguity of data and can also create disastrous scenario in emergency situations. So the communication need to be more secure, encrypted so that device authentication and data reliability could be increases.

To authenticate, the data along with IMEI number is encrypted using single key password mechanism. But if the all devices and cloud will use the same single key for encryption and decryption then also there is a chances that attacker can find that single key.

So for making the system more authenticated and secure, we will use shared encryption key between device and server, which is unique to each device. In this research paper include how these unique keys will be exchanged between both the parties.

## II. LITERATURE REVIEW

The Government of India felt the need for a permanent agency to expedite the publication of standards and development of test facilities in parallel when the work on the preparation of the standards is going on, as the development of improved safety critical parts can be undertaken only after the publication of the standard and commissioning of test facilities. To this end, the erstwhile Ministry of Surface Transport (MoST) has constituted a permanent Automotive Industry Standards Committee (AISC) vide order No. RT-11028/11/97-MVL dated September 15, 1997. The standards prepared by AISC will be approved by the permanent CMVR Technical Standing Committee (CTSC). After approval, the Automotive Research Association of India, (ARAI), Pune,

being the secretariat of the AIS Committee, will publish this standard [2].

AIS 140 is a Government approved device.The Government of India, has directed all the state governments to enforce the standards, equip AIS 140 compliant GPS tracking devices with the supporting software for all passenger-carrying buses and other public transport vehicles effective January 1, 2019 [3].

Automotive Industry Standard 140 (AIS 140) is a set of standards published by ARAI (Automotive) for vehicle tracking system, camera surveillance system, and emergency request button. This mandate is in line with the Ministry of Road Transport and Highways notification dated 28th November 2016 [4].

According to Dr. Ajay Kumar, IAS, Addl. Secretary, Ministry of Electronics and Information Technology (MeitY), there is a need to create test infrastructure and the government is in the process of developing testing capabilities for IoT based devices in its Standardization Testing and Quality Certification (STQC) labs [5].

KPIT (BSE: 532400, NSE: KPIT), today confirmed the availability of **India's first ARAI (Automotive Research Association of India)-certified AIS-(Automotive Industry Standard)-140 compliant vehicle telematics and emergency button solution** in line with the Ministry of Road Transport and Highways (MoRTH), Government of India's notification dated November 28th 2016. The AIS-140 regulation, applicable from April 1st, 2018, mandates a vehicle tracking device and one or more emergency button(s) in all existing and new public service vehicles [6].

## III. PRESENT WORK

In above literature review, we found details about AIS 140 devices and its protocol, which states about, how the device should send the data to the server. But it did not describe anything about how data authenticity will maintained. In this paper, we will present a way by which we can securely transfer the data, ensuring authenticity and preventing data manipulation by any traffic listener.

First, we will transfer device id (IMEI number) to the server via a symmetric key encryption using a shared encryption key during device manufacturing process in SUM (Secure unit manufacturing).

Secondly, in exchange of the device id, server will generate a unique random token and encryption key, which should be used for any further communication along with the token for device identification.

## IV. MECHANISM

To make system authenticate, device should share its device id securely to server.

The steps are as follows:

1. While manufacturing process, whenever firmware is flashes into device. A flasher will flash encryption key (Key-X) provided by server. Which should be change iteratively every hour.


Fig.1. Server providing key-X to device, flash using flasher.

**2.** Within this timespan of one hour, the devices which have been flashes with encryption key-X would send a registration request packet containing device-id (IMEI No.) which is encrypted by any symmetric key algorithm (e.g. AES-256, DES, Blowfish etc.) using this key-X.


Fig.2. Device registration request encrypted with Key-X

3. Then the server will decrypt registration data by using same encryption key-X and get IMEI number and other details of device. In exchange server will provide a unique token-T and a new encryption key-Y against a device-id, which should be send to device encrypted with Key-X.

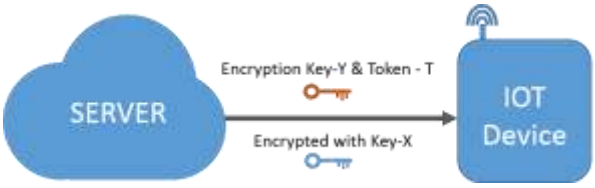


Fig.3 Server providing token and new encryption key

4. Further, device will decrypt the registration response from the server using Key-X. And get new Key-Y and token-T. Which will be used for any further communication.
5. Now, whenever need of communication, device will use encryption key-Y to encrypt the data and then send encrypted data along with token-T. So that by using token-T server will easily find out that from which device this data packet is coming and will decrypt the data via stored key-Y.


Fig.4.Devicewill send encrypted data and token for further communication

## V. ARCHITECTURE

The client server architecture is:

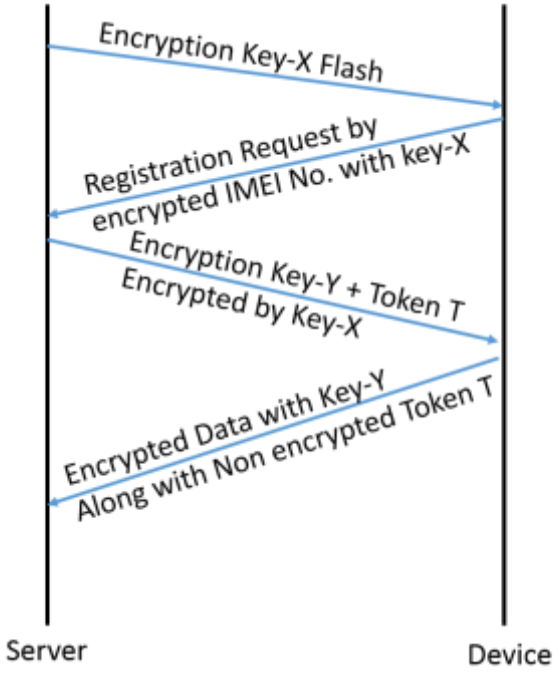


Fig.5.Client Server Architecture

## VI. CONCLUSION

By exchanging the key in secure manufacturing environment we can authenticate the devices so the chances of attack will be less and system willbecome more secure. This is one time process.

## REFERENCES

[1]. Finalized Draft- Automotive Industry Standard(AIS) Intelligent Transportation Systems (ITS) - Requirements for Public Transport Vehicle Operation https://araiindia.com/hmr/Control/AIS/68201793238AMFinal_Draft_AIS_140.pdf

[2]. Intelligent Transportation Systems (ITS) - Requirements for Public Transport Vehicle Operation https://araiindia.com/hmr/Control/AIS/82201693742AMDraftAIS140_DraftD1_26July2016.pdf

[3]. AIS-140 Automotive Industry Standard Compliant location Tracking System for Public Transport Vehicles Launched by Unlimitedhttp://www.businessworld.in/article/AIS-140-Compliant-Location-Tracking-System-For-Public-Transport-Vehicles-Launched-By-Unlimit/07-01-2019-165869/

[4]. India's AIS-140 Automotive Industry Standard: Intelligent Transportation Systems (ITS) https://zenodo.org/record/1182955#.XNQfLhQzbIU

[5]. 7th Telematics India 2017 Conference, August 17-18, 2017, Pune.

[6]. KPIT expands mobility solution portfolio - Adds AIS-140(Automotive Industry Standard) compliant telematics system https://www.kpit.com/company/news/2018/kpit-expands-mobility-solution-portfolio-adds-ais-140-compliant-telematics-system