An MQTT based Improved Authentication Algorithm for Intelligent Transport System

Arockia Jaya J[1], Dr.Shanti M A[2], Vigneshwari K[3], Dr.Jayasundar S[4], Mahesh V[5]

[1,4]Associate Professor, [2,3,5]Assistant Professor
[1,4]Department of Computer Science and Engineering
[2,3]Department of Information Technology
[5]Department of Computer Applications
[1,4]Idhaya Engineering College for Women, Chinnasalem, Tamilnadu, India
[2,3,5]Idhaya College for Women, Kumbakonam, Tamilnadu, India

Abstract:

Internet of things (IoT) is one of the promising technology in the 21st century. It involves a huge number of sensors and connected devices. IoT generated a huge volume of data. IoT contributes to improving the local area development by connecting homes, cities, hospitals, industry, etc. MQTT protocol is used to send the messaging purpose in IoT. The MQTT is a lightweight protocol and easily implemented variant. With the evolving smart cities project across the globe and transmitting to the digital environment, the Intelligent Transport System (ITS) makes city life easy. The ITS aims to achieve traffic minimization and time minimization. The city vehicle is connected by IoT devices. In this work, we propose an improved MQTT protocol for effectively transferring the information from IoT devices to Cloud servers. The Pi 3 was used to transmit the data to the cloud server for analysis. The result shows the improved version of the MQTT protocol is out formed well compared to the previous MQTT Protocol.

Keywords: IoT, ITS, MQTT, sensor

1. Introduction:

Vehicle traffic is a significant issue to be addressed in megacities to a small town. From the research, traffic noise and traffic-related environment creates a lot of health issues [1]. The vehicle is contributing more to air quality problems, which have more harmful to our health. The Intelligent Transport System (ITS) is proposed to reduce traffic congestion and other related traffic. The ITS is used to reduce the traffic and waiting time of the vehicle. The effective process of ITS is as follows: Sense, Analyse, Control, and communication to improve human safety, efficiency and mobility[2]. Automating the vehicle movement in roadways, railways, and airports reshape people's experience. The purpose of ITS:

- Improving the easy mobility of goods and people.
- Reduce the traffic waiting time and congestion.
- Meeting transport policy and goals.
- Improving the safety of the people.
- Improving the quality of the public vehicle.
- Significantly improve the air quality.
- Reduce the impacts of a highway accident.

The Internet of things (IoT) is a tiny computing hardware device used as an umbrella for ITS to connect multiple objects. Connected objects could be roadways, cars, etc. The IoT is an internet-enabled embedded device. It has the sensing and processing capability and transfer the data to the server and also own battery backup. Most of the work is done by sensors without human interventions. People can communicate with the device easily[3]. The IoT connects real-world data to virtual worlds. IoT technology plays a vital role in the global ITS environment [4]. The IoT device easily senses the data, processes the data, and analysis it. The big data methods are used to analyze the data. In the digital world, the Internet of Things optimizes the transport industry (both people and goods).

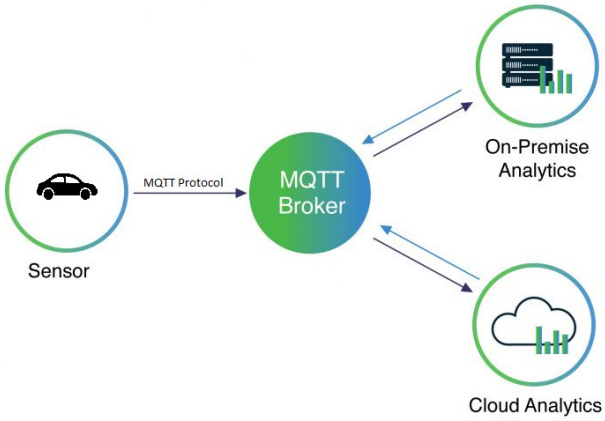

Fig 1: Architecture of ITS using MQTT

The many advantages are listed using ITS Technologies:

- Search the best route based on real-time data.
- Avoid the crash situation alert the driver before occurring.
- Show the empty parking space to the driver.
- Divert the traffic based on the conditions.
- Less fuel consumption.
- Improve the tracking mechanisms.
- More reliable and convenient.

MQTT stands for MQ-Telemetry Transport, also called Message Queuing Telemetry Transport. The MQTT is mainly used for IoT machine-to-machine communication. MQTT was originally introduced in the year 1999. It requires a tiny microcontroller for processing purposes. The message header of MQTT is very small. So, we can optimize the network bandwidth. It allows two-way communication from device to Cloud and Cloud to device [5]. Scalability is very high. MQTT Protocol can connect millions of devices. Reliable message communication between the device to cloud. The main two features of the MQTT protocol is

as follows: easy to implement and lightweight. Lightweight means consuming low power for processing.

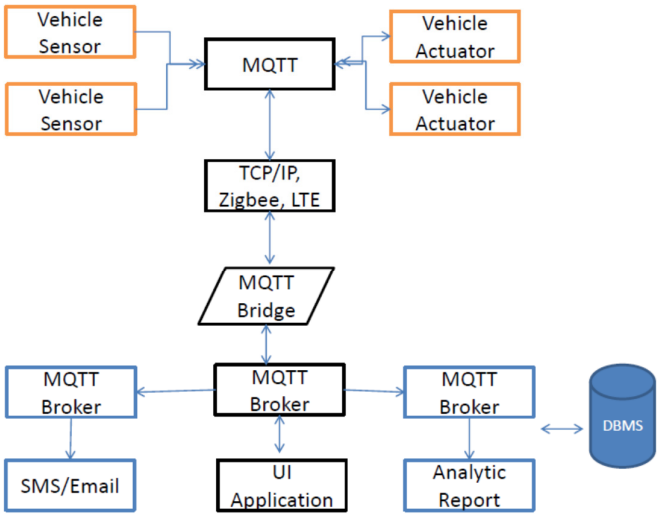

Fig 2: Architecture flow of MQTT Protocol

The organization of the paper follows Section 2 detailed report on existing related works. Section 3 describe the detailed design requirements. Section 4 is about the proposed improved MQTT algorithm. Section 5 for Experiment result and Section 6 for Conclusion.

2. Related Works

Research Paper Name	Author Name	Methodologies	Metrics	Demetris
Smart vehicle monitoring and assistance using cloud computing in vehicular Ad Hoc networks [6]	Agarwal, Y., Jain, K., Karabasoglu, O	Time of arrival (TOA) based localization in VANET.	Traffic Safety, localization, collision avoidance mechanism.	Partially implemented in real-time and hardware-implemented partially.
Smart vehicle automation [7]	Desai, S., Desai. S	Collision warning, Collision avoidance, and driver safety system	Safe system design with collision warning	No real-time implementation
Artificial intelligence-based vehicular traffic flow	Azzedine Boukerche, Yanjie Tao, Peng Sun	ML-based prediction method. Statistics-based	More flexible.	Less adaptability in the Statistics method.

prediction methods for supporting intelligent transportation systems [8]		prediction method.		
Nanogenerator as new energy technology for self-powered intelligent transportation system [9]	Long Jin, Binbin Zhang, Lei Zhang, Weiqing Yang	piezoelectric nanogenerators, triboelectric nanogenerators.	More safety, efficiency, and convenience.	Nanogenerators are Limited performance.
Convolutional neural networks for 5G-enabled Intelligent Transportation System: A systematic review[10]	Deepika Sirohi, Neeraj Kumar, Prashant Singh Rana	Deep learning (DL) is based on object detection and localization.	Security is high	More number of data sets.
Single-message-based cooperative authentication scheme for intelligent transportation systems [11]	Ming Yang, Shuang Wei, Rongwang Jiang, Faizan Ali, Boxiong Yang	Single message cooperative authentication	High security and avoid the malicious attack	Authentication delay
Vehicle communication network in intelligent transportation system based on Internet of Things [12]	Hong Zhang, Xinxin Lu	OPNET modeler Software. Layered network method.	More throughput, Reduce the network delay, Less packet loss.	The simulation result is done by low-speed motion.
Performance of DSRC and WIFI for Intelligent Transport Systems in VANET [13]	A.Fitah, A.Badri, M.Moughit, A.Sahel	VANET, IEEE802.11	Packet Delivery Ratio, End-to-End Communication	Suitable for low traffic Scenario
Optimal charging scheduling for large-scale EV	Yugong Luo, Tao Zhu, Shuang Wan, Shuwei Zhang,	Novel optimal charging schedule	Improve the grid performance.	No real-time implementation

(electric vehicle) deployment based on the interaction of the smart-grid and intelligent-transport systems[14]	Keqiang Li			

3. Design Requirements

Figure 3 shows the bird's view of the proposed architecture. The component of the proposed architecture follows:

Sensor

The sensors are fitted in the vehicle. All the sensors are connected together and transforming the information using smart technologies. IoT technology is used for gathering information from vehicles or the environment and transfer to the Cloud using MQTT.

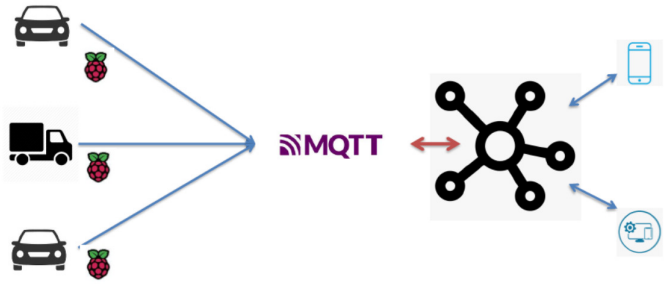

Fig 3: Proposed Architecture

Raspberry pi

The Rasp Pi is a tiny and cheap computing device that runs on a Linux platform. It has a future of GPIO (General Purpose Input/output). The GPIO is used to control the sensor and Electronic Components. Figure 4 shows the GPIO pins module.

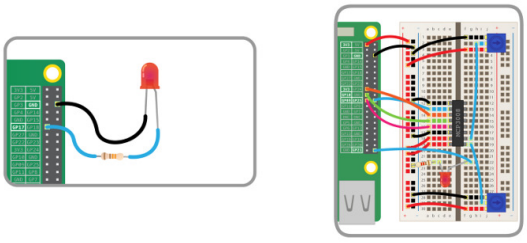

Fig 4: GPIO Pins Module

MQTT

MQTT protocol supporting the IoT technologies based on publishing subscribe model. Most of the IoT technology uses the MQTT protocol for transferring the message. MQTT is a very tiny size; that enable secure and stable transmission over a low bandwidth network. MQTT has a special future of decoupling between subscribers and publishers.

Cloud/Big Data

The MQTT transfer the data to Cloud for backup. The big data methodology is used to analyze the data. Cloud is an on-demand available device based on our requirements.

4. Proposed Improved MQTT Algorithm

The MQTT protocol has a "Publish-Subscribe" model for transferring the message. It consists of two important components.

1. End-point-Device: used to control the communication traffic.
2. Gateway: Transferring input/output message.

The message received by the Gateway is transferred to any device. The MQTT Algorithm is supported for multicasting. The MQTT publisher device is the one output for n subscribers with individual topics for the entire subscriber. The two methodologies provide the complete security mechanism for the MQTT protocol. The first one is Authentication using a username and password. The second security is Access Control (both database and file). The CONNECT message transfers the Username and Password message [15]. If Authentication is identified, the Gateway responds with a CONNACK message.

User Registration Process

The proposed algorithm is based on Schnorr Algorithm [17] for Zero-Knowledge Protocol. The objective of the algorithm is Gateway is to make a certain decision that the client device knows the password without directly transmitting it[18].

Symbol	Abbreviations
Login	Identifying of User
H(.)	Hash function
||	Concatenation
Password	User Password
dl_ID	Device Identity
X	XOR Operation
R	Random Numbers
t_i	Time Stamp
T	Token
PSK	Public Security Key
g,p	Any Large Numbers

Table 2: Abbreviations

Table 2 shows the abbreviations used by the proposed algorithm. The User registration process steps are followed:

Step 1: Calculate TOKEN Value

The token values can be calculated by following equations:

$T = H(H(login|| t_i.dl\_ID)X\ PSK$ (1)

Step 2:

The Devices are receiving Token F from Gateway. The value of X and Y can be calculated by the following equations:

$X = H(Password)$ (2)

$Y=g^x \bmod p$ (3)

Step 3:

Transferring Y value into Gateway.

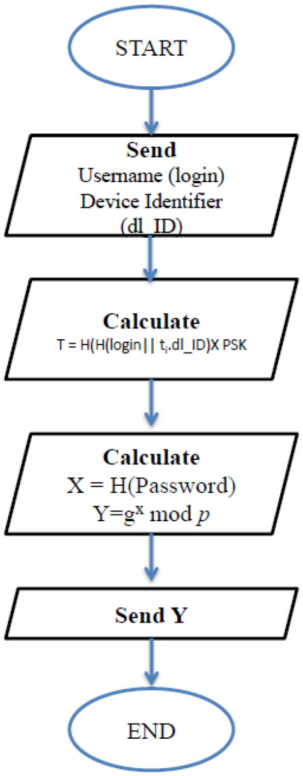

Fig 5: Flowchart of Registration Process

Authentication Process

The Authentication process usually involves all the values (X, Y, F). The random number R_{rand} is largely generated by devices.

Step 1: Generating Session Key (S)

The Token value (F) and the Hash value of a variable (r) are used to calculate the Session key.

The Session key can be calculated using the following formula

$S = F * H(r)$ (4)

Where $r = g^r \bmod p$ (5)

Timestamp

The timestamp variable is used to avoid the re-authentication. The device checks the timestamp. If the timestamp exceeds the limited time, the authentication process is denied. The devices send CONNECT messages along with M, *timestamp*, and password. The MQTT protocol receives the CONNECT message with the variable field.

5. Experiments

The proposed MQTT protocol was tested using Eclipse Mosquito [17]. Mosquitto is an open-source MQTT broker protocol. The Mosquitto platform is a low-power single-board computer to a high-end server. Figure 6 shows the MQTT explorer connection. The username is MQTT, and the password is Tommy. Figure 7 shows the encrypted password of Tommy.

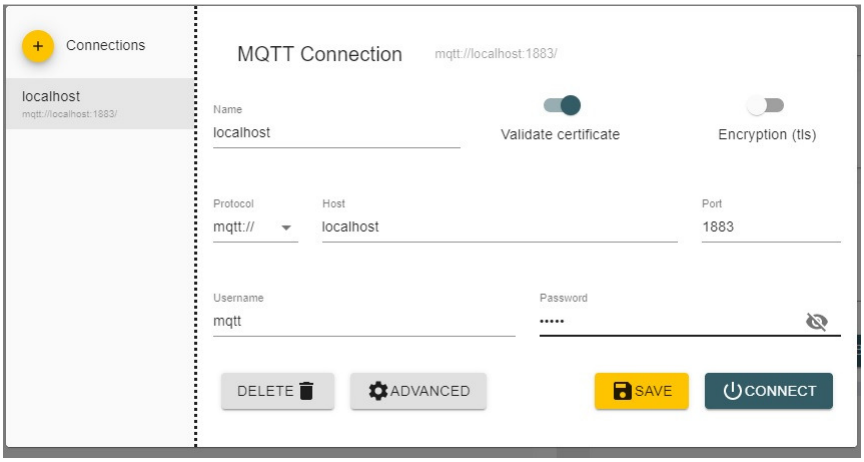

Fig 6: MQTT explorer Connection

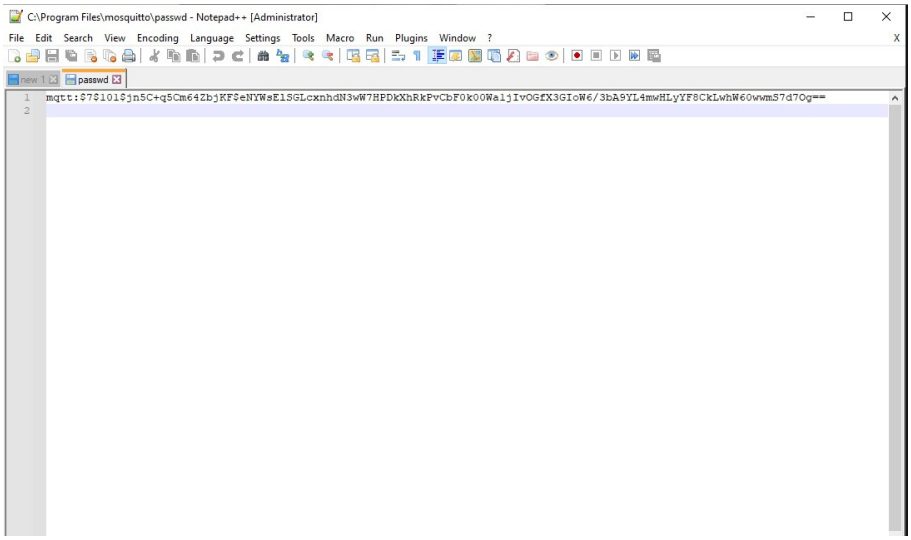

Fig 7: Encrypted password

Statistical Analysis:

Authentication Type	Insecure Channel	TLS Protocol	Proposed Algorithm
Time of Connection(min)	17	415	14
Time of Connection (Max)	2850	3438	1826
Mean	31.2	460	41.2
MSD	102	121	69.7

Table 3: Comparison of Improved MQTT algorithm

Table 3 shows the comparative analysis of the proposed MQTT algorithm with TLS protocol. From table 3, the Authentication is very fast using the insecure channel. TLS protocol was significantly slow compared with MQTT protocol and also clearly shows the proposed MQTT protocol give the effective results Intelligent Transport System.

6. Conclusion

The emerging technologies IoT and Big data bring a systematic approach to ITS. The number of vehicles is increasing drastically. Due to urbanization, maintaining the traffic in big cities are challenging. To handle the situation, we need a formidable algorithm. In this work, we propose an improved version MQTT protocol for IoT. IoT plays a very important role in proposing any digital applications. The main objective of this paper is the minimization of traffic waiting time and less pollution. The comparison result shows the proposed improved version of the MQTT protocol is outperformed well. The generation of the session key and timestamp secure the data from the sensor to the cloud environment. From the analysis, the proposed algorithm works securely in the insecure channel.

References

[1].https://pharmeasy.in/blog/stress-anxiety-pollution-effects-of-traffic-jam-on-health/#:~:text=Traffic%20and%20its%20allied%20effects,pressure%2C%20heart%20attacks%2C%20etc.
[2]. https://www.n-ix.com/intelligent-transport-system/.
[3]. https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.
[4]. S. Muthuramalingam, A. Bharathi, S. Rakesh Kumar, N. Gayathri,R. Sathiyaraj and B. Balamurugan" IoT Based Intelligent Transportation System (IoT-ITS) for Global Perspective: A Case Study", Chapter13.
[5]. https://mqtt.org/
[6]. Agarwal, Y., Jain, K., Karabasoglu, O.: Smart vehicle monitoring and assistance using cloud computing in vehicular Ad Hoc networks. Int. J. Transp. Sci. Technol. 7, 60–73 (2018)

[7]. Desai, S., Desai. S.: Smart vehicle automation. Int. J. Comput. Sci. Mobile Comput. 6(9), 46– 50 (2017)

[8]. Azzedine Boukerche, Yanjie Tao, Peng Sun,"Artificial intelligence-based vehicular traffic flow prediction methods for supporting intelligent transportation systems", Computer Networks, Volume 182, 9 December 2020, 107484

[9]. Long Jin, Binbin Zhang, Lei Zhang, Weiqing Yang,"Nanogenerator as new energy technology for self-powered intelligent transportation system", Nano Energy, Volume 66, December 2019, 104086.

[10]. Deepika Sirohi, Neeraj Kumar, Prashant Singh Rana, "Convolutional neural networks for 5G-enabled Intelligent Transportation System: A systematic review", Computer Communications, Volume 153, 1 March 2020, Pages 459-498.

[11]. Ming Yang, Shuang Wei, Rongwang Jiang, Faizan Ali, Boxiong Yang," Single-message-based cooperative authentication scheme for intelligent transportation systems", Computers & Electrical Engineering, Volume 96, Part B, December 2021, 107390.

[12]. Hong Zhang, Xinxin Lu, "Vehicle communication network in intelligent transportation system based on Internet of Things ", Computer Communications, Volume 160, 1 July 2020, Pages 799-806

[13]. A.Fitah, A.Badri, M.Moughit, A.Sahel, "Performance of DSRC and WIFI for Intelligent Transport Systems in VANET", Procedia Computer Science, Volume 127, 2018, Pages 360-368.

[14]. Yugong Luo, Tao Zhu, Shuang Wan, Shuwei Zhang, Keqiang Li, "Optimal charging scheduling for large-scale EV (electric vehicle) deployment based on the interaction of the smart-grid and intelligent-transport systems", Energy, Volume 97, 15 February 2016, Pages 359-368.

[15]..R J. Cohn, R. J. Coppen: OASIS Standard Incorporating Approved Errata 01, MQTT Version 3.1.1, OASIS, 2014.

[16]. V. V. Yashchenko: Introduction to Cryptography, 4th Edition, Publishing house of MCNMO, Moscow, 2012. (In Russian).

[17]. https://mosquitto.org/