INTELLIGENT TRANSPORTATION SYSTEM WITH THE SECURITY PERSPECTIVE

Anik Khokhar, Gayatri Pandi
Student, Head of Department (CE)
ME(CE)LJIET
Ahmedabad, Gujarat

Abstract: IOT (Internet of Things) is an incredibly vast area, future holds 50 billion devices connected to each other by the end of 2025. ITS (Intelligent Transportation System) is a part of enormous IOT project. ITS concern with smart transportation, safety and in reducing energy consumption. However, entering into a new environment always brings new challenges. In this paper, various implementation area of IOT is included and then an explanation of ITS with its pros and cons are described. Security issues in ITS leads to a specific problem of Data security, Methods by which it can be solved is given in brief, With Detailed Explanation of Lightweight protocol, which is one of the feasible solution. Ending up with three distinct and unique example, which was implemented with a lightweight protocol in a different scenario. In addition, we have provided a proposed model of an algorithm, which will help in increasing security and reducing footprint.

Keyword: Internet of Things, Intelligent Transportation System, Lightweight protocol, Sensors

I. INTRODUCTION

Smart devices and the speedy Internet have an opportunity for rapid growth of the IOT. The network of IOT contains sensors and actuators, this network could be private or public. Standard protocols are applied to give better communication in the IOT network and some places there is a combination of standard protocols and protocols that are supported by the Internet of things such as lightweight protocol named CoAP (Constrained Application Protocol) or MQTT (MQ Telemetry Transport). [12] Apart from IOT, there is a description of how ITS operates. As the impleme ntation scenario expands, more and more possibility comes up for better traffic management, applying safety to road traveling and Achieving optimal travel time. Some of the implementation scenarios are briefly discussed in this paper, which contains the futuristic solution to our current transportation problems. Not all the working of ITS is so smooth there are security loopholes. Therefore, security issues and its countermeasures are given, from which data security is a main concern of security. In addition, to solve that problem one of the best solutions is Encryption. [42, 55] As we know, traditional encryption have a key size of 128 bits and above, so we need lightweight security. Lightweight security works well with IOT because it has a small footprint and lower overhead. [93] This paper is organized as section-II gives a description of IOT, which contains its working, benefits, implementation area, and issues in IOT. Section-III Gives idea about ITS which contains techniques of ITS, implementation and its pros and cons. Section-IV Explains the basics of sensors, which contains classification, types of sensors, sensors used in ITS, security threats with countermeasures and secure encryption methods. Section-V provides information about the lightweight protocol that contains basic idea about the concept with a type of lightweight protocol & implementation examples. With a proposed model that can be solution to security issues. Section VI give conclusion and way towards possible future work.

II. INTERNET OF THINGS

“IOT (Internet of Things) is all about communication and sharing of data between various sensors, actuators and smart-Devices via a communication Network.”[42, 55].In 1999 the term IOT first mentioned by Kevin Ashton, in which data can be accessed by the things without human interaction. Market analysts & Auto-ID Center at MIT these two were the initial spark that popularized the concept of IoT. Since then it is gradually growing its market and in recent times its creating a hype, to communicate with any device connected anywhere anytime in this virtual structure is the main aim of this concept. [93] IOT keeps on creating various smart concepts on which our future is designed. Some of them are Intelligent Transportation Systems (ITS), E-health, logistics, business/process management, assisted living. And the list keeps going on.[50,65] We humans, have senses such as ears to listen, eyes to see, touch to feel, nose to smell and so on. What we are now watching is world moving towards a future were "things" are given power to senses various objects. These devices having such senses can give us detailed data even from most remote places on earth. All we need is some simple hardware, durable battery, constant power source like the sun, and a network. IoT is giving benefit to us in ways like increased revenue or by optimizing various consumptions. We can use it to get information from places where humans are not much suited. It will be used in the betterment of life, and of course, the army of various countries are already using it in every possible way. [12, 30, 35, 76]

How to make efficient and affordable communication between two humans that live far away geographically was a very interesting question, which was later replaced by another question, how we could better use machines by understanding their communication language. Now the next question that we need to answer is how can two machine communicate which in turns gives benefit to humans. So basically the first question is about H2H (Human to Human) communication, the second one is about M2H(Machine to Human) or H2M(Human to machine) communication, And the last one is M2M (Machine to Machine). [64] Benefits of IOT will go as far as our imagination and that is limitless, millions of devices and sensors will be connected and huge amount of data will be extracted, and utilizing all the data for the automated process will be a real task for IOT. Such a vast network of devices and tons of data will help to solve some serious problems and it can be used in serving people. There is also some disadvantage like Privacy & security, Complexity, Lesser jobs, Dependability. Even some other issues like expanding the network and adding hardware to our current working environment are going to be a big challenge.

A. WORKING OF IOT

a. Hardware:

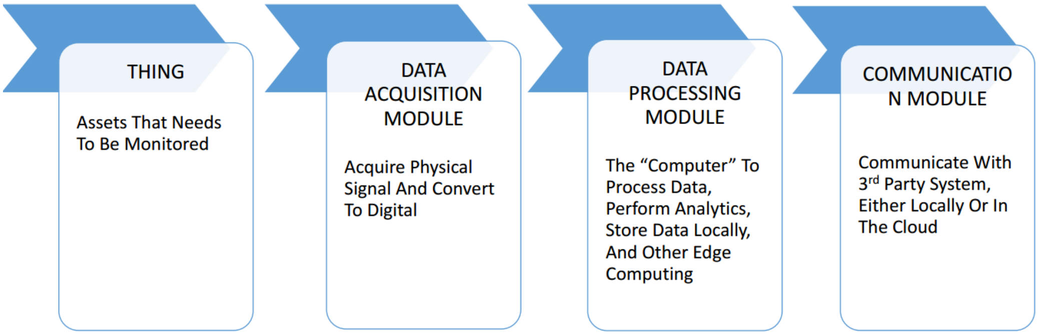
THING
Assets That Needs To Be Monitored
DATA ACQUISITION MODULE
Acquire Physical Signal And Convert To Digital
DATA PROCESSING MODULE
The "Computer" To Process Data, Perform Analytics, Store Data Locally, And Other Edge Computing
COMMUNICATIO N MODULE
Communicate With 3rd Party System, Either Locally Or In The Cloud

Figure – 1 Communication process

The hardware is most important in the entire IOT environment because it is going to give system all the valuable data that will be used in the various process. The data will mostly be in an analog form such as temperature, voltage, acceleration, speed, etc. As shown in Figure-1 the process is divided into four stages first one is having "things" those are hardware such as RFID (Radio-frequency identification), Sensors, and Actuators. The second stage is Data acquisition, which collects all the data from things and converts it into digital format so processing can be done on it. Third stage Data processing model, that is obvious that we need a processer where we can run our algorithm to apply various analytical programs, also storage is needed. It will not be powerful as our desktops or laptops. Various chipsets are available for this purpose like Arduino Yun, Raspberry Pi, BeaglBone Black. [4]

b. Language

After selecting hardware for any project if the language is still undecided then hardware is like a battery-operated toy without any command. Therefore, we can say the language is equally important, with different hardware different combination of language works, for example, Arduino works on 'C++ & C'. Similarly, there are different language as Java, Python, node.js, and JavaScript. [1]

c. Networking technologies

IOT hardware is capable of having the various working capability but the most important one is communication between hardware. In addition, what command will hardware follow will be decided by commands given by the language selected. Nevertheless, communication medium is still needed so which technologies are used is also important. [22] And there are various technologies as shown in Figure-2 and listed below.

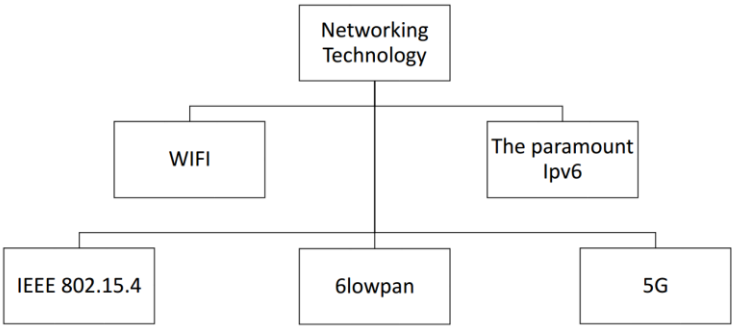

Figure – 2 Networking Technology

WIFI: - It is the most common and most used technology for communication indoors. [74]
IEEE 802.15.4:-Its chart-busting technology in radio standards. [31]
IPv6 over Low Power Personal Area Network (6Lowpan):- For critical task having specific time limit we need 6lowpan.
The paramount - IPv6:- For communication with devices in remote places, we need Ipv6.
5G: - Next generation networks and standards are needed to solve complex challenges. [8, 71]

B. BENEFITS OF IOT

Some advantages of IOT are:

- **Communication: -** IOT works on M2M communication so it increases the efficiency of work and also the transparency.
- **Automation and Control: -** Because of things connected to each other through wireless infrastructure. There is a large amount of automation and control in working. As there is no human, interference in between the output is comparatively fast.
- **Information: -** no matter what filed we talk about more information always means more accurate decisions, IOT does that by providing lots of data from different objects and it can be processed for different scenarios using various mining technologies.
- **Time: -** 24hours a day seems to be short for humans when there is a deadline for such a critical period of time we can utilize systems and infrastructure like IOT to work faster and save time.
- **Money: -** If the money spent after producing IOT devices are less than saving money globally, then we can say we are gaining profit. In addition, it happens because of utilization of IOT system will get cheap, once it is mass-produced and it is automated, it saves lots of money in the various process. Like collecting data from numerous sources in very less time.
- **Better quality of life: -** All the above benefits are targeted for single most important achievement, it is a better quality of life, that is possible because of the utilization of IOT

An IOT vision statement way beyond merely changing software and hardware to set upgrade from the current system the bigger picture is to give benefit to humankind [6, 10, 47]

C. IMPLEMENTATION AREA

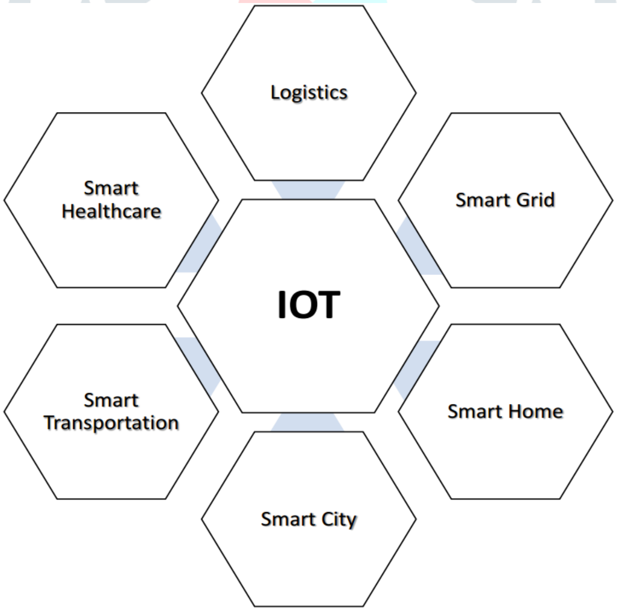

Figure – 3 IOT Application Area

IOT technology has been applied to many application domain, some of the important ones are shown in Figure-3. Which are expected to grow exponentially in upcoming decade. [63, 72, 81, 85]

(a) **Smart logistics: -** Traditional logistics is not able to provide consistent result in a dynamically changing environment. Recently aspect like flexibility and adaptability gained importance and that can only be achieved by technological integration with logistics. “Smart logistics” is term given to such integration of technologies and logistics. [80]

(b) **Smart grid: -** Power electronics, transmission, bulk generation, distribution is a general domain which is covered in domain span of the smart grid, some of the relatively new domains such as renewables and electric vehicles are also part of the smart grid. Ultimately, smart grid is a system of distributed system. [32]

(c) **Smart home: -** Home objects such as appliances, door lock, surveillance camera, furniture, garage doors and so on are provided with a certain level of intelligence. The ultimate aim is that all appliances and things in home communicate in between them and take the decision which usually is done manually. Thus saving time on decision-making and giving the command to things. [54]

(d) Smart city: - It is all about leveraging technology to serve people it starts with information network, which is also designed to optimize resources, Thereby promote sound sustainable development. Connected streets are the core of smart cities for e.g. each street light can gather and send information such smart connected streetlight can open up many possibilities. Smart dustbin, which gives real-time feedback for how much it is filled, and when to pick it up. Many other sensors such as weather sensor, pollution sensor can help us make decisions critical to smart city people's health. [19]

(e) Smart transportation: - It is not just about getting from point A to point B, but getting there safer, greener and more convenient way by connecting and distributing intelligent processor inside a vehicle and throughout the transportation infrastructure, we can transform infrastructure in profound and unimaginable ways. Intelligent travel will be multi-model enhancing all the forms whether by car, rail or by air. In addition, travelers will be seamlessly connected across every means of travel. Future vehicle will be connected with the intelligent processor, delivering the processing headroom to many tasks simultaneously, such as improving navigation, communication and passenger entertainment, all while enabling safer more efficient travel. Car will be able to connect over a variety of wireless standard to the Internet, to intelligent traffic signals and even to over vehicles. Essentially, Car becomes another extension of our digital lifestyle

Example, when fuel level or battery power starts to get low vehicle will be automatically searching for recharging stations. Providing directions to those with the lowest prices. Sensors inside and outside our vehicle will also improve safety. Inside cameras can recognize driver and passengers and adopt seating, entertainment preferences and navigation to match. Outside sensors will detect lane departures sense and response to potential danger, such as not slowing down for upcoming slope, sign, and continually identify the object on the side, front or behind car to avoid the collision. Assistant parking, or allow driver cruising control to adapt speed to maintain a safe distance from the car in front. Connected intelligence will be extended beyond vehicles, existing and emerging wireless standards enables vehicles and devices across transportation infrastructure to communicate with each other, enabling an automatic intelligent real-time decision to optimize travel. Distributed intelligence that is secure and reliable is the key, transforming the entire traffic infrastructure from being passive and unaware to proactive intelligent sense and response system that improves traveling in every way. [48]

(f) Smart health: - Explained by current city example of the developed country. Here in the smartest city we have the same problem our healthcare system every city has. Rising cost inconsistent quality limited access to timely core, we also recognize that the population demographic where changing, creating new demands for services from aging citizens. What we came to realize as many of our problems were in fact problems of the healthcare system. So smarter city took a holistic approach to healthcare. We built a smarter health system starting by tearing down silos and connecting doctors, patients, and insurgents so they can share needed information seamlessly and more securely. In addition, the good things healthcare system in the smarter city used to be overly complicated. Patients had to provide the same health history each time they went to a new doctor, coordinating doctors, caregivers, and the pharmacist was left to the individuals. Caregivers never seem to know previous health conditions over prescriptions they might be taking, their emergency contact, there allergies or tests had already been performed. Critical information was often inaccessible. Electronic health record can get the right information to physician caregiver and the insurgents at the right time.

Allowing them to deliver personalized care and increase the value to everyone by improving quality and efficiency. A connected healthcare system allows doctors to collaborate on diagnosis and treatment plans. No matter where they are and reference patient information such as imaging in real time and infrastructure interconnected intelligence. The system makes our entire communities healthier. In the smarter city, we can walk into any interconnected healthcare facility just as they do in Spain. Now we would have up to date information means we get higher quality for care. Moreover, data that we now collect and analyze in real time help us shift from treating one patient at a time to proactively focusing on prevention and wellness. Disease outbreaks are a real threat to health and safety of any community, city officials use advanced software models and supercomputers to monitor public health, identify outbreaks, determine most infectious mutation of the virus and simulate the spread of disease. These tools allow health officials to track and forecast health event. Educate the public more effectively mobilize the resources and most importantly take preventive measures. Information is also playing role fostering the smarter cities a life science. Researchers are playing and advance analysis to a vast amount of data to help discover new drugs and therapies and using fast reliable supercomputers to test different drug characteristics to see what work and what does not. The healthcare system in the smarter cities puts the focus of the entire system purely where it belongs on the individual. [23]

D. ISSUES IN IOT

Security: As the security regulation is still not fully developed, there are numerous serious issues present in IOT environment. One of the biggest threat is the internet to IOT because the idea of anyone can access from anywhere is very horrifying If security is not tight enough. The annual economic cost of cybercrime is estimated to be around 1 trillion dollars. Serious security threats are expected to be caused by a recent rise in ransomware. In which cloud vendors and service providers will be the prime targets. Objects using A.I are also under threat of such attack because A.I is still in development phase and cannot deal with recent malware, which is capable of avoiding detection in A.I environment having IOT system working with it. [18,20,49,77,82]

Privacy: User privacy is one another pressing issue not only in violation of consumer privacy but also it is a security breach. The university of Glasgow recently did a study and showed how most of the users of IOT where not satisfied by lack of privacy in IOT. As users are getting more and more aware of cyber surveillance, the user is taking this privacy issues seriously and demands ultimate control over data. In addition, increased transparency is needed to ensure the safety of user's data. [14,37,89]

III. INTELLIGENT TRANSPORTATION SYSTEM

"An intelligent transportation system (ITS) is a technology, application or platform that improves the quality of transportation, or achieves other outcomes based on applications that monitor, manage or enhance transportation systems." ITS is an emerging transportation system which is comprised of an advanced information and telecommunication network for users, roads, and vehicles. [33,45,46] ITS is the integrated application of advanced technology using electronics, computers, communication and advanced sensors. This application provides travelers with important information while improving the safety and efficiency of the transportation system. [16,57,79]

A. TECHNIQUES USED- WORKING

(a) Wireless communication
(b) Computational technologies
(c) Floating car data/ Floating cellular data
(d) Sensing technologies

- Inductive loop detection
- Video vehicle detection
- Bluetooth detection
- Audio detection
- Information fusion from multiple traffic sensing modalities

a. Wireless communication: Dedicated Short Range Communication (DSRC) and continuous air interface long and medium range (CALM)[25]

b. Computational technologies: New technologies in a vehicle electronics have been lead towards lesser, more capable computing processors on vehicles. Earlier this decade a vehicle would have 20 to 100 individual programmable logic controller modules with no real time O.S. [41] But the trend is towards fewer, more costly microprocessor modules with hardware memory management and real-time O.S. Embedded system platform gives chance for implementation of more complex software application that includes ubiquitous computing, artificial intelligence and, model-based process control. Most important technologies from mentioned above is artificial intelligence for ITS. [1]

c. Floating car data:

There are a total of four widely used methods for obtaining raw data

1) **Triangulation method:** In most of the counties, a high proportion of four wheelers contains one or more mobile phones. Mobile phones periodically send their presence information to a network provider. Even when there is no calling or texting. A concept of using phones as anonymous traffic problem was experimentally carried out in the mid-2000. As the vehicle moves so does the signal of the mobile phone. Traffic flow information will be gathered with pattern matching or cell sector statistics and by measuring and analyzing network data using triangulation method. Where there is more traffic there are more car and phones and so more data is obtained. In cities, the distance between antennas is shorter so result in accuracy increases. Advantage of this method is it don't need any additional hardware implementation near the roadside. In practice, the triangulation method was very hard to implement, especially when there were parallel lanes of different vehicles or overlapping of transportations like a road under the metro rail. By early 2010 the popularity of this method was declining.[78]
2) **Vehicle re-identification:** Sets of detectors mounted along the roadside are required for this method a unique serial number of a vehicles device is identified of each point where detectors are mounted. Travel time and speed are calculated per the arrival from one pair of a detector to another. These unique number can be of MAC number of Bluetooth or it can be the RFID Tag number used for toll tax collection. [44]
3) **GPS based method:** The number of vehicles equipped with in-vehicle satellite navigation is increasing now a day. This system has 2-way communication with the traffic data provider. Vehicles position readings are used for calculation speed. The modern method may use mobile instead of inbuilt hardware.[17]
4) **Smart phone based rich monitoring:** Traffic speed and its density can be traced by the sensor of the smartphone. The accelerometer data can be used to find out traffic speed and road quality. Audio data and GPS(Global Positioning System) tagging is also a source of data which can be used for identification of possible traffic jam.[67]
   Benefits of these technologies:
   - Less expensive than sensors or cameras.
   - More coverage.
   - Faster to set up less maintains.
   - Works in all weather conditions including heavy rainfall.

d. Sensing technologies:

Pavement loops are used to sense the presence of vehicle demand at intersections and parking lot entries pressure pads are used to sense the presence of pedestrian waiting to cross a roadway. Radar and an acoustic sensor is used for detecting vehicles in the roadway. How it works: - transmits radar pulses a portion of the energy is reflected or scattered from the vehicle and roadway back towards the sensor. This energy is received and interpreted.

Benefits:

- Low power
- Most accurate technology for detecting speed
- Traffic count accuracy
- Easy installation

1) **Inductive loop detection:** One or more loops of wire are embedded under the road and connected to a control box. When a vehicle passes over or rests on the loop, inductance is reduced showing a vehicle is present.[43]
2) **Video vehicle detection:** Vehicle detection can be done by video camera also it can be used for traffic flow and incident detection. The video camera does not include any extra equipment embedded on the roadside so this type of system is known as “non-intrusive” method of traffic detection. The processor analyzes the changing an image of the video. Mostly camera is mounted on traffic poles. Initial information needs to be feed to the system such as the height of the camera from the road, distance between two lanes. Also, how and what bases speed is calculated. Video detection processor can capture traffic from eight similar branded camera simultaneously. Vehicle speed, counts, lane occupancy are some of its output that is provided by the video processor. Also, additional outputs like including a gap, headway, stopped vehicle detection and wrong way vehicle alarm. [29]
3) **Bluetooth detection:** An inexpensive and accurate way to measure travel time from origin to destination can be done by Bluetooth. It is a wireless standard used for communication between two electronic devices. If these sensors used in a vehicle travel time can be calculated.[54] Bluetooth is different in the following ways

- Quick to set up with minimum or on calibration
- Non intrusive leads to low cost
- Accurate measurement points
- Number of sensor limited per device

More number of the device integrated with Bluetooth used in more vehicles increase the accuracy of data and make it valuable.

4) **Audio detection:** Traffic density can be measured using an audio signal having various inputs such as tire noise, engine noise, honks, engine idling noise, and air turbulence noise. Roadside can be equipped with microphone and input can be processed with various techniques to accurate estimation of the traffic state.[62]
5) **Information fusion from multiple traffic sensing modalities:** All the data of individual methods can be combined to get the most accurate data analysis. This can be done by the data fusion based approach.[92]

B. IMPLETATION OF INTELLIGENT TRANSPORTATION

Emergency vehicle notification system: E-call is the method where vehicle itself calls when service required or occupants of the vehicle want help in emergencies. In such emergency both voice and data sent directly to the nearest emergency point (normally the nearest E1-1-2 public safety answering point, PSAP). While E-call is been received by E-call operator. Meanwhile a minimum set of data which contains information like the position of the vehicle. An id of the vehicle is sent to the operator desk. E-call system depends on manufacturer it can be mobile phone-based (Bluetooth connection to an in-vehicle interface) or integrated telematics device connect to a network, Also a similar example to study is Blackbox Implementation.[69]

Automatic road enforcement: Traffic enforcement system achieved by the camera and also vehicle monitoring system. [2] Speed camera is used to detect a vehicle traveling over illegal speed it can also be done by electromagnetic loops buried in each lane. A signal camera which detect vehicle crossing the line when the signal is red and emailing the bill by verifying number plate Bus lane camera that identifies a vehicle traveling in bus reservation lanes. Railway crossing camera used for illegal crossing of two-wheelers.

Variable speed limits: This method can help improving smooth flow of traffic when there is congestion on road in such conditions variable speed is decreased. In addition, in most of the condition, the variable speed is used only to decrease in poor condition and not to increase in good conditions [87]

Collision avoidance system: This is achieved by installing sensors on the highway which notify others cars on the same road about a stalled car in their way [84]. Even it can be achieved by sensors used in car and one car can communicate with the upcoming car.

C. ADVANTAGES OF ITS

What could business do if the freeways and roads could communicate with their fleet what if the vehicle could communicate with each other? If drivers could predict traffic conditions 15 mins ahead in time? Smart roads vehicles and devices linked in a network. The data, the knowledge to forecast traffic conditions and the ability to rely on the prediction. These are the foundation of the intelligent transportation system. Intelligent transport will create tremendous value for business and society, ITS will transform how traffic is managed and how vehicles operate. Those factors create new possibilities for logistics and supply chain management. And traffic planning and even the design of private and commercial vehicles. At the basic level, ITS should solve traffic condition problem. At more advanced level transportation system should base its decision on the current traffic conditions and the traffic conditions that it expects to see in the next few minutes that is also known as situational awareness. Intelligent transportation system creates situational awareness by gathering real-time data from roadways equipped with sensors, individual vehicles, smartphones, and HPS devices. And other sources such as accident pattern and even city event panel. The system analyzes this data, turning it into knowledge that vehicles and drivers can use to stay one-step ahead of delay and other hazards

The key to intelligent transportation system is that the system is a self-learning and self-improving one. It makes predictions based on what it has learned and what is happening in real time. That intelligence makes the system dynamic and responsive. An intelligent transportation system can reroute traffic and roads when it predicts congestion ahead. A fleet vehicle will interact with an intelligent transportation system to select optimal routes then changes them on the fly or necessary, this can even unable the faster option of driverless vehicles. With these capabilities, the intelligent transportation system can transform how cities and companies will manage transportation in future, the government cites country state will have better information and new tools for planning and operating transformation infrastructure in the future this will make traveling safer and should help reduce cost. As an example, roadway expansion can be directed where it is the most need. While the impact of the construction work is accurately forecast and planned for. Logistics providers will likely be tomorrow's transportation management companies their expertise and experience combine with the intelligent transportation system. Capabilities position them to design manage and operate traffic management solutions for tomorrow's intelligent cities.

Sensor and communication technology vendors will help IFS acquire, process and integrate information so that data can become intelligence that other players in the ecosystem can use. the manufacturer will make vehicles capable of been connected to and collaborating with other vehicles as well as a centralized system. Control and decision support system. These vehicles makers will take full advantage of the ITS to deliver a new and more satisfying driving experience. Many companies are working to build a system that will help their vehicles communicate in real time with the intelligent transportation system and also analyze the data for resource planning. Better data means the company to ship more goods on time of lower cost using fewer vehicle traveling on optimized routes. A project like smarter toll technology is also being developed which traffic flowing streamlines revenue collection and reporting and the toll stop become another data point on the intelligent transportation system. Every sensor deployed, every smartphone traffic app, every connected vehicle, adds to the knowledge of the intelligent transportation system. Intelligent transport will enable more intelligent cities, logistics, and business. Companies must start bringing intelligent transportation system into their design, supply chain, and logistics management models today to be ready for the future.

D. DISADVANTAGES OF ITS

When we use a combination of sensor all the disadvantages are also combined from all sensor. The basic problem of the sensor are the environment, for e.g. camera won't be that efficient at night. So all the work related to the camera such as traffic management with the camera, or number plate scanning. The similar problem arise with a microphone attached to the roadside. Such as when there is heavy rain audio quality decrease because of such heavy rain and wind noise. Apart from that electricity problem, battery problem, wiring problem malfunctioning product, a defect in the sensor are all such reason why it can give a false reading. Also when sensors in car or road are unattended for long time chances of someone misusing it for his/her own benefit increase. As the number of hardware increase, the amount of database increase which mean to be handled and also the cost of maintenance of the database and all hardware used on the grid needs to be taken into account.

IV. BRIEF ABOUT SENSORS

As a human we Perceive the world through our senses we see how we can grab an object like a hammer, we can smell a fire from far away, we can taste fruit is ripe and ready to eat we hear a car coming and feel when it's cold. These are our five senses sight, hearing, touch, smell, and taste. As a human, we use a lot of products like cars, phones, and computers. These products have senses too only we call them sensors. Sensors like temperature sensors, pressure sensors, and light sensors. That's how a product like an automatic door knows when you want to pass through it.[24,65,73]

A. CLASSIFICATION OF SENSORS

There is classification on a different level of complexity. But if we take most simple classification of sensors it will be active and passive sensors. Active sensors need an external power source to work, where on other hands in a passive sensor there is no need for any external power sources. It is more durable and long life than active sensors.[15,40] Means of detection is another type of classification. The means of detection can be electrical, biological, chemical, and radioactive. Input and output conversation can also be considered as another classification type such as photoelectric, thermoelectric, electrochemical, electromagnetic, thermos-optic, etc. Analog and digital is a final classification in this list, Analog output which is continuous in nature on other hand digital sensors give a discrete output that is digital data. It is used for conversion and transmission in digital nature. [9,11,13]

B. DIFFERENT TYPES OF SENSORS

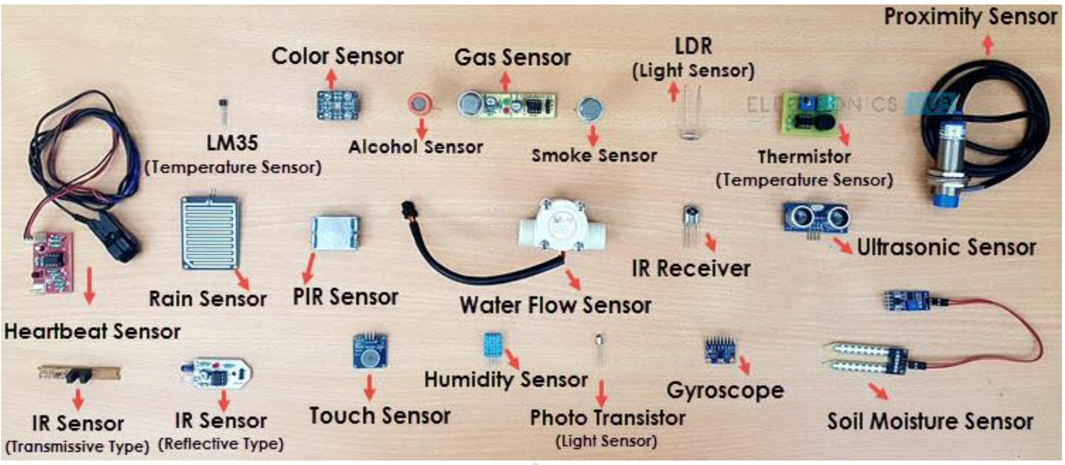

Figure – 3 Type of Sensors

- Temperature sensor
- Proximity sensors
- Accelerometer
- IR sensor(infrared sensor)
- Pressure sensor
- Light sensor
- Ultrasonic sensor
- Smoke , gas , alcohol sensor
- Touch sensor
- Humidity sensor
- Tilt sensor
- Flow and level sensor

C. SENSORS USED IN ITS

Safety is a most important aspect of driving so for securing that expect various sensors are used such as a micromechanical oscillator, speed sensors, camera, ultrasonic sensors, proximity sensors, night vision sensors. Diagnostic through the gathering of data for finding out faults in vehicles sensors used will be a position sensor, chemical sensor, temperature sensor, pressure sensor, airbag sensor. For monitoring traffic conditions some of the sensors like camera, radar, ultrasonic and proximity are usually used. Assistance for various steps in driving can be provided with sensors such as Gas composition sensors, humidity sensors, temperature sensor, position sensor, an image sensor, distance sensors. For environment updates of the vehicle and outside vehicle sensors named pressure sensor, temperature sensor, camera and weather conditions can be accessed from mobile devices. Health conditions of drivers can be known by a camera, thermistor, electrocardiogram ECG sensor, electroencephalography (EEG), heart rate sensors.[26,36,56]

D. SECURITY THREATS AND COUNTERMEASURES

1) DOS (denial of service) this attack is done by giving servers many fake requests so server gets busy in answering those requests and meanwhile original request is denied due to overload on the server.so problem of availability arise. To avoid such fake request countermeasures of a digital signature can be applied.[66]
2) Jamming, flooding is the method where the communication line is flooded with lots of requires mixed with fake and authentic users, such problem creates availability issues it can be solved by digital signature attached to its load or header.[28]
3) Sybil attack acquires a fake identity of a node for transmission of unnecessary messages, which lead to congestion of the network. It creates availability and authentication issues which can be solved by a digital signature.[3]
4) Malware, spamming, black hole, grey hole, sinkhole, and wormhole. Are some of the methods, which can create network availability issues in addition to the authentication problem it can be secured by a digital signature. [58]
5) Falsified entities. This type of attack can be done by the user who got valid network Id of an ITS station. Which leads to issues of authentication and authorization. This problem can be solved by encryption and digital signature.[83]

6) Cryptographic replication as the name suggests it replicates the encrypted message and subsequent key of those messages to create ambiguity during verification process at the receiver side. An issue of authentication and authorization can be overcome by applying a solution of encryption and digital signature.[53]

7) GNSS spoofing and timing attack are both responsible for providing false location and time of reciting end network channel this both types of issues compromise authentication and authorization factor of security and countermeasures are digital signature and encryption.[5]

8) Masquerading is basically a disguised attack in which non-user broadcast message at emergency to create disturbances in the network. Data playback is a very similar attack to that of masquerading only difference is it rebroadcast old message such false interruption create congestion in the network. Similarly, data alteration attack can modify the message to create ambiguity in the network, the best countermeasures for such an attack is a digital signature with the certificate.[75]

9) The two very important type of security attack that concern this paper is related to confidentiality and the issues are eavesdropping and data interception. This is the center of all other security issues if the data is hacked and data is leaked there is no meaning of communication in private it's like broadcasting the message, simple solution to this problem is Encryption.[34]

E. SECURE ENCRYPTION METHODS

Encryption is the basic need for protection of data numerous options are available in the market for a consumer to choose a method which fits their requirement.

Here are some most secure encryption methods:-

(a) AES: - (Advanced Encryption Standards) One of the most secure algorithm and it is the symmetric type. This method uses a block cipher, one block of data of a time, basically there id three type of AES on its key bits size that is AES-128, AES-192, AES-256. In AES-128 there is 10 round for each bit key in AES-192, there are 12 rounds and in AES-256 it's 14 rounds.[61]

(b) 3DES: - Triple data encryption standard, or 3DES it's also a block cipher technique. The previous version of this method was DES which used to have a 56-bit key but now this 3DES uses 168-bits key that is 3 times that of DES.[86]

(c) TWOFISH: - This symmetric block cipher method is a better version of blowfish method. Twofish have block size varying from 128-bits to 256-bits. Like AES method it also has rounds at encryption data bit unlike AES no matter whatever the block size it turns 16 rounds for encryption.[59]

(d) RSA: - This algorithm is named after 3 scientist Ron Rivest, Adi Shamir, Len Adelman. It is public-key cryptography using asymmetric algorithm this is secure because it has 2 large prime numbers in its process. Additionally, the key size is larger its keys are 1024-bits and 2048-bits long so it's secure but very slow in operation.[68]

All these methods are very promising and effective in data security and some of the best encryption algorithm. But unfortunately, the IOT and intelligent transportation system contains billions of sensors with limited processing power and battery life.

It is infeasible to apply such heavy algorithm to such a system, so we need an algorithm which are light in overhead and overall resources consumption. Hence the name lightweight protocol is used more in IOT field.

V. LIGHTWEIGHT PROTOCOL

Definition - “lightweight protocol refers to any protocol that has a lesser and leaner payload when being used and transmitted over a network connection. It is simpler, faster and easier to manage than other communication protocol used on a local or wide area network.” Another definition -“Any protocol which has lesser and leaner payload can be said as the lightweight protocol which can be transmitted over the networked connection. In comparison with other communication protocol used on any network such as WAN or LAN lightweight security protocol is easier, faster and simpler to manage”[39]

A. BRIEF ABOUT LIGHTWEIGHT PROTOCOL

Having lightweight footprint is a benefit of using a lightweight protocol which will also provide similar or in some area even better performance than its heavier counterparts. As this protocol includes only most important data in payload and also in header part, we can say it is optimized to work in limited resources so it performs faster and it's more efficient than traditional protocols. The lightweight protocol can also be compressed to make it even lighter in weight giving us the benefits to use it in numerous fields for communication. For example, the TCP/IP protocol is considered lighter than the OSI protocol stack. LDAP(lightweight directory access protocol), LEAP(lightweight extensible authentication protocol) and SCCP (skinny call control protocol) are some popular examples at lightweight protocol.[7]

B. TYPE OF LIGHTWEIGHT PROTOCOL

Here are some of the protocol which can be used in IOT because of its lightweight nature in different layers.

(a) Some of the Infrastructure layer protocol such as:-

- 6LoWPAN:- It stands for ipv6 over low power wireless personal area network. This protocol operates at 2.4 GHz frequency of 250 kbps transfer rate.
- Another protocol that is very important that is UDP(User Datagram Protocol) This protocol is an alternative to TCP and one of the oldest one from networking protocol. It's simple OSI transport layer protocol for network based on (IP). User Datagram Protocol is usually used in applications tuned for real-time performance.
- DLTS (Datagram Transport Layer):- DTLS is used for privacy on data in communication to avoid eavesdropping, tampering, message forgery on a client-server application where DTLS protocol is used. This protocol is based on TLS(Transport Layer) protocol and provides equivalent security.
- Some of the Data protocol that can be useful in IOT are - MQTT(Message Queuing Telemetry Transport) this protocol is used for enabling publish or subscribe messaging model in an extremely lightweight manner. It's a perfect fit for using in IOT because it requires a very small footprint as the resource are limited and the system could be located in a very remote location. Similarly, there is MQTT-SN(MQTT for sensor network) it is lightweight protocol specifically designed for sensor network and mobile application all the benefits of MQTT are present in this protocol too, Mosquito an open source MQTT blocker.[90]
- One of the most used protocol in IOT world is CoAP (Constrained Application Protocol). It is basically application layer protocol which is specifically designed to use in resources constrained (limited) Internet devices, such as wireless sensors network. HTTP protocol is translated to lighter level by CoAP for simplification of its integration with Web. It satisfies the requirement of IOT by simplicity, very low overhead and multicast support. The features of CoAP are that it minimize complexity while reducing overhead. It support the discovery of resources supported by CoAP services also it supports URI and context-type support. We can subscribe via CoAP and get all notification.[27]

(b) Network protocol used in IOT would be as below

- IEEE 802.15.4: - This is a standard that works on the physical layer and it is low-rate wireless area networks for media access control. It comes under IEEE 802.15 standards and maintained by the same working group. IEEE 802.15.4 is also base for ZigBee, ISA100.11a, wireless HART, and MiWi. All this individual protocol are developed like unique protocol with features that are not in IEEE 802.15.4 so we can say all those are an extension of IEEE 802.15.4. Alternatively, this standard can be used with 6lowPan and other standard Internet protocol.[31]
- Bluetooth: - Bluetooth transfers data through low power radio waves whose frequency ranges from 2.40 GHz to 2.485 GHz. Bluetooth devices come in three classes from which class one is an industrial application that ranges from 90 meters to 100 meters. Devices like mobile and Bluetooth headsets are class two devices that have range of 10 meters, class three devices have a range of about 1 meter and are used rarely. Bluetooth use ISM band for data transfer, smart Bluetooth technologies can use 0.01w to 0.5 watts. So it does not drain the battery and because of that reason, it can be used in a wide variety of IOT applications.[70]
- Cellular:- this mode of a network is also been used with its own technology those cellular networks are GPRS/2G/3G/4G/5G.[52]

C. IMPLEMENTATION EXAMPLES OF LIGHTWEIGHT PROTOCOL

Lightweight protocol are used where there is shortage of resources. Resources in terms of processing power, Ram, storage, battery life. In IOT normal communication, data, network protocols cannot be used as it off huge processing power plus it eats up lots of battery and there system could be placed in remote places it can't be maintained so frequently.

Let's consider some of the examples below.

a. Lightweight protocol for industry

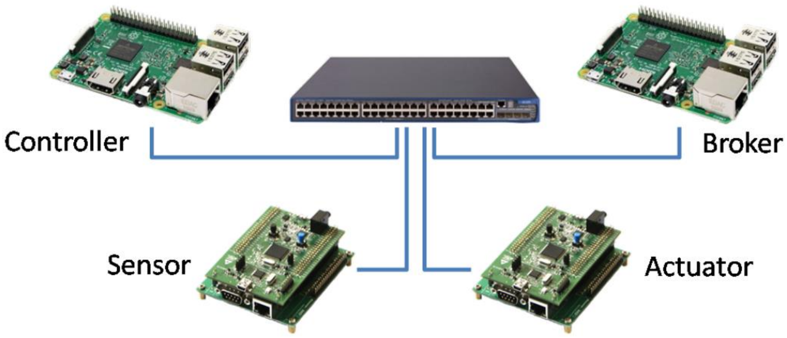

Figure – 4 Platform scheme [51]

There is a rapid transformation in design, operation, and service of a manufacturing system, where machines, sensors, and actuators are interconnected in the factories in order to enable spontaneous coloration, monitoring and control, CPS(cyber-physical system) are still using SOAP and HTTP as their protocols. For communication. These are not efficient in communication in IOT world as it contains large footprint plus memory and energy consumption. To change protocol given above new protocol with smaller footprint protocol are developed such as CoAP(Constrained Application Protocol) and MQTT(MQ Telemetry Transport). These protocols have different features and quality of service, which helps them to become more suitable for IoT world. [51]

b. M2M protocol for IoT

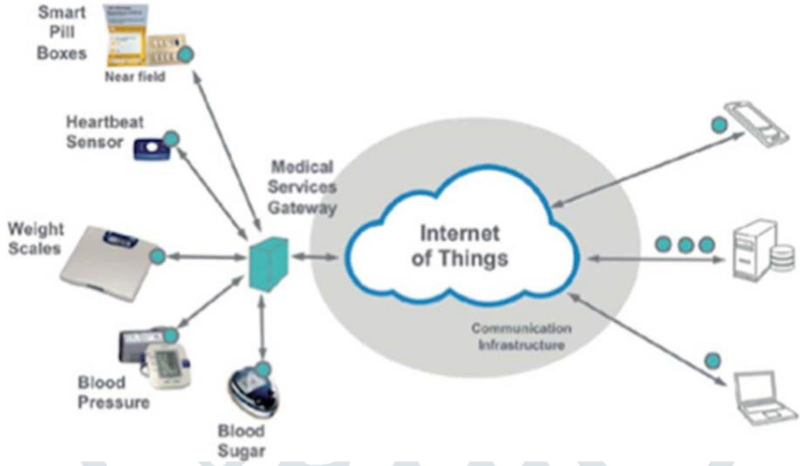

Figure – 5 M2M Architecture[60]

IoT has thousands of devices connected and seamlessly communicating with each other which needs a lightweight data transfer process. The different environment needs different IoT protocol with different capabilities. Due to this protocol needs to be very specific according to the nodes used; power requirement and communication range. According to the requirement of the majority of IoT devices, MQTT and CoAP protocol are used. These protocols are lightweight in terms of operation and data transfer.[60]

c. Identity based authentication protocol.

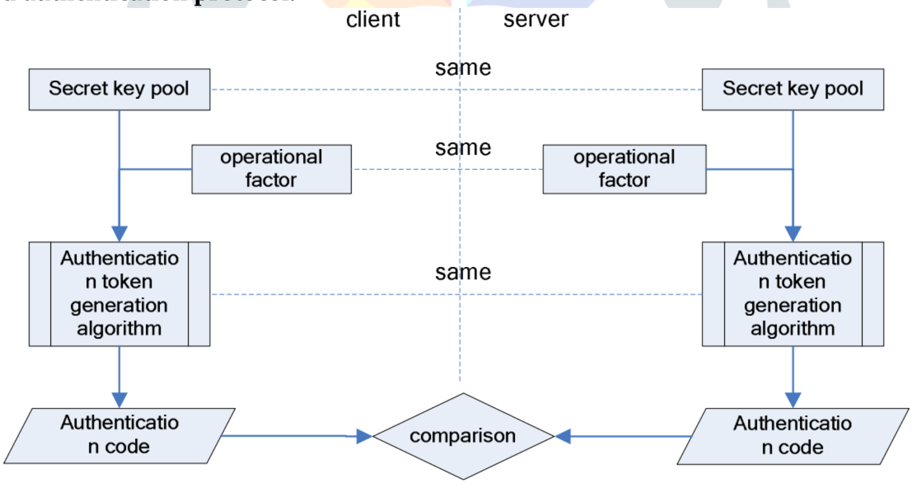

Figure – 6 Authentication protocol principle[88]

To ensure that only authorized user can access nodes of WSNs, we need lightweight authentication protocol which should be based on identity. A basic strategy for this function is to store id on both sides and then compare it to confirm the identification. This work can be simplified by using a token generation algorithm and keypad. OTP can also be used to confirm the identity of an authenticated node. The process of identification is very advanced in the computer system but it contains large overhead and so it cannot be used in IoT environment. Here as the resources are limited the mechanism need to compressed or re-invent in such a way that it leads to smaller footprint and overhead which can be only done by making algorithm lightweight.[88]

D. PROPOSED MODEL FOR LIGHTWEIGHT SECURITY PROTOCOL.

After observing various algorithms under the lightweight protocol. Here we have designed a data encryption algorithm that is a basic variation of how encryption and decryption could work. This algorithm is having a vast area for implementation but for now, experiments would be conducted on sensors related to ITS.

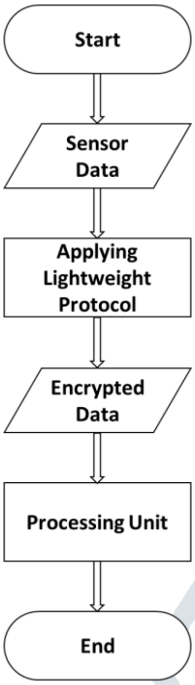

Figure - 7 Flow chart

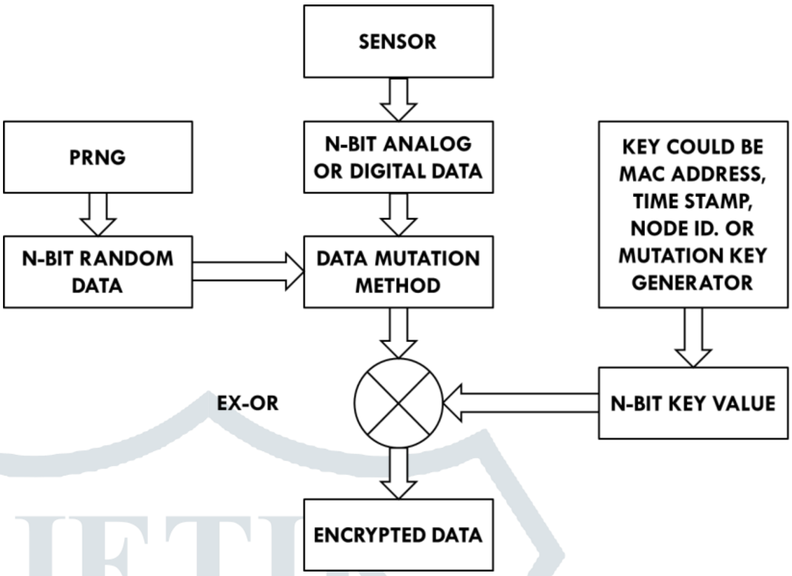
SENSOR
PRNG
N-BIT ANALOG OR DIGITAL DATA
KEY COULD BE MAC ADDRESS, TIME STAMP, NODE ID. OR MUTATION KEY GENERATOR
N-BIT RANDOM DATA
DATA MUTATION METHOD
EX-OR
N-BIT KEY VALUE
ENCRYPTED DATA

Figure – 8 Block Diagram for Encryption.

Steps of Flow chart

Step 1: Data is received from sensor.
Step 2: Lightweight security protocol is applied on Data in transit.
Step 3: Encrypted data is delivered to processing unit.

Steps of Encryption Block Diagram

Step 1: Sensor gives n-bit of analog or digital data depends on the type of sensor used.
Step 2: N-bit of data is the mutated with sensor data and n-bit of random data which is generated by PRNG algorithm.
Step 3: Data from Mutation process is EX-ORed with the data provided by the n-bit key provider, which is generated by combination of MAC address, node id, and time stamp or key generation algorithm.
Step 4: After performing all the above steps we would get an encrypted data which is sent to Processing unit.

VI. CONCLUSION

As we know IOT is in developing phase and various experiment are conducted to get benefits from this technology. Parallel as we find out advantages of IOT we also see its drawback. This paper reviews IOT working in detail and an example of an implementation area with its benefits and drawbacks. The intelligent transportation system is one of the important branches of IOT which is reviewed in detail in this paper. With given insight into software and hardware used. Sensors in general and sensors used in ITS are described with the classification which gives a clear picture of how different protocols can be applied. Such lightweight protocols are reviewed having benefits in IOT environment and various examples are described to give a better understanding of survey leading a roadmap from IOT to security issues in ITS and giving various possible solutions. In addition, an attempt to implement the proposed model on a suitable hardware will be conducted.

VII. REFERENCES

[1] Abdulhafis Abdulazeez Osuwa, E. B. (2017). Application of Artificial Intelligence in Internet of Things. 9th International Conference on Computational Intelligence and Communication Networks, 169-173.
[2] Alwyn J. Hoffman, A. J. (2015). SmartRoad: A new approach to law enforcement in dense traffic environments. 2015 IEEE 18th International Conference on Intelligent Transportation Systems, 598-605.
[3] Amol Vasudeva, M. S. (2018). Survey on sybil attack defense mechanisms in wireless ad hoc networks. Journal of Network and Computer Applications, 1-47.

[4] Andrii Polianytsia, O. S. (2016). Survey of Hardware IoT platforms. 152-153.

[5] Apurva S. Kittur, A. R. (2017). Batch verification of Digital Signatures: Approaches and challenges. Journal of Information Security and Applications, 15-27.

[6] Basim K. J. Al-Shammari, N. A.-A.-R. (2018). IoT Traffic Management and Integration in the QoS Supported Network. IEEE INTERNET OF THINGS JOURNAL, 352-370.

[7] Bassam J. Mohd, T. H. (2015). A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues. Journal of Network and Computer Applications, 73-93.

[8] Breandán Ó hAnnaidh, P. F. (2018). Devices and Sensors Applicable to 5G System Implementations. IEEE.

[9] Bruno Andò, F. B. (2018). Sensors. Springer International Publishing AG .

[10] Catalin Gosmana, T. C. (2018). Controlling and filtering users data in Intelligent Transportation System. Future Generation Computer Systems, 807-816.

[11] Corrado Di Natale, V. F. (2014). Sensors and Microsystems.

[12] Daniel Giusto, A. I. (2010). The Internet of Things 20th Tyrrhenian Workshop on Digital Communications. Springer Science+Business Media, LLC 2010.

[13] Dario Compagnone, F. B. (2014). Sensors.

[14] Djamel Eddine Kouicem, ,. A. (2018). Internet of things security: A top-down survey. Computer Networks, 1-24.

[15] Dr. Enrico Pigorsch, R. B. (n.d.). SENSORS. METRA MARTECH Limited.

[16] Dr.sc.ing. Irina Yatskiv, D. M. (2017). Review of intelligent transport solutions in Latvia. Transport and Telecommunication Institute, Lomonosova 1, Riga, LV-1019, Latvia, 33-40.

[17] Eleonora D'Andrea, F. M. (2016). Detection of Traffic Congestion and Incidents from GPS Trace Analysis. Expert Systems With Applications, 1-33.

[18] ELISA BERTINO, K.-K. R. (2016). Internet of Things (IoT): Smart and Secure Service Delivery. 1-7.

[19] Emile Mardacany. (n.d.). Smart cities characteristics: Importance of built Enviroment component. 1-6.

[20] Fadele Ayotunde Alaba, M. O. (2017). Internet of things Security: A Survey. Journal of Network and Computer Applications, 1-36.

[21] Fantoni, D. M. (2015). Changing the Programming Paradigm for the Embedded in the loT domain. IEEE.

[22] Farhana Javed, M. K.-S. (2018). Internet of Things (IoTs) Operating Systems Support, Networking Technologies, Applications, and Challenges: A Comparative Review. IEEE, 1-39 .

[23] Fran Casino, E. B. (2015). Context-Aware Recommender for Smart Health.

[24] Francesco Baldini, A. D. (2012). Sensors .

[25] Frieder Ganz, P. B. (2014). Multi-resolution Data Communication in Wireless Sensor Networks. IEEE World Forum on Internet of Things (WF-IoT), 571-574.

[26] Gründler, P. (2007). Chemical Sensors An Introduction for Scientists and Engineers. Springer-Verlag Berlin Heidelberg 2007.

[27] Herrero, R. (2018). Analytical model of IoT CoAP traffic. Digital Communications and Networks, 1-7.

[28] Huang, S. M. (2008). Advancements in Modeling, Design Issues, Fabrication and Practical Applications.

[29] Huasheng Zhu, J. W. (2018). Detection of Vehicle Flow in Video Surveillance. 3rd IEEE International Conference on Image, Vision and Computing, 528-532.

[30] Hussain, F. (2017). Internet of Things Building Blocks and Business Models. Springer.

[31] IEEE Standard for Low-Rate Wireless Networks. (2018). 1-12.

[32] IEEE Vision for Smart Grid Controls: 2030 and Beyond Reference Model. (2013). 1-5.

[33] INTELLIGENT TRANSPORTATION SYSTEMS. (n.d.).

[34] Iván S. Razo-Zapataa, C. M.-P. (2012). Masquerade attacks based on user's profile. The Journal of Systems and Software, 2640-2651.

[35] Jeffrey Voas, B. A. (2018). A Closer Look at the IoT's "Things". 11-14.

[36] Jha, C. M. (2015). Thermal Sensors.

[37] Jie Lin, W. Y. (2016). A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. 1-17.

[38] Juan José Vinagre Díaz, A. B. (2016). Bluetooth Traffic Monitoring Systems for Travel Time Estimation on Freeways. IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, 123-132.

[39] K€onig, H. (2012). Protocol Engineering. Springer-Verlag Berlin Heidelberg.

[40] Kalantar-zadeh, K. (2013). Sensors An Introductory Course. Springer Science+Business Media New York .

[41] Kanchana P. Nai, R. J. (2017). Performance Analysis of Constrained Application Protocol Using Cooja Simulator in Contiki OS. International Conference on Intelligent Computing,Instrumentation and Control Technologies (ICICICT), 547-550.

[42] Kewei Sha, W. W. (2018). On security challenges and open issues in Internet of Things. Future Generation Computer Systems, 1-33.

[43] Lala bhaskar, A. s. (2015). Intelligent Traffic Light Controller Using Inductive Loops for Vehicle Detection. 518-522.

[44] Li, C. h. (2010). Automatic Vehicle Identification(AVI)System Based on RFID. IEEE, 281-284.

[45] Ling SUN, Y. L. (2016). Architecture and Application Research of Cooperative Intelligent Transport Systems. 747-753.

[46] Lucia Janušová, S. Č. (2015). Improving Safety of Transportation by Using Improving Safety of Transportation by Using. 9th International Scientific Conference Transbaltica , 14-22.

[47] Luigi Atzori, A. I. (2010). The Internet of Things: A survey. Computer Networks, 2787-2805.

[48] M. Bhaskar Naik, P. K. (2019). Smart public transportation network expansion and its interaction with the grid. Electrical Power and Energy Systems, 365-380.

[49] M. Chernyshev, Z. B. (2017). Internet of Things (IoT): Research, Simulators, and Testbeds. 1-11.

[50] Mahdi H. Miraz, M. A. (n.d.). A Review on Internet of Things (loT), Internet of Everything (IoE) and Internet ofNano Things (IoNT). 219-224.

[51] Markel Iglesias-Urkia, A. O. (n.d.). Towards a lightweight protocol for Industry 4.0: An implementation based benchmark.

[52] Mashael M. Alsulami, N. A. (2018). The Role of 5G Wireless Networks in the Internet-of-Things (IoT). 1-8.

[53] Michelle S Henriques, P. N. (n.d.). USING SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHY TO SECURE COMMUNICATION BETWEEN DEVICES IN IoT.

[54] Min Li, M. L. (2018). Smart Home:Architecture, Technologies and Systems. 8th International Congress of Information and Communication Technology (ICICT-2018), 393-400.

[55] Minhaj Ahmad Khan , & Khaled Salah . (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 395-411.

[56] Octavian Adrian Postolache, S. C. (n.d.). Sensors for Everyday Life.

[57] Pamuła, A. S. (2016). Intelligent Transportation Systems – Problems and Perspectives. Springer International Publishing Switzerland .

[58] Pedram Hayati, V. P. (2010). Definition of Spam 2.0: New Spamming Boom. IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2010).

[59] Pil-Joong Kang, S.-K. L.-Y. (2006). Study on the Design of MDS-M2 TwofIsh Cryptographic Algorithm adapted to Wireless Communication. 692-695.

[60] Priyanka Thota, Y. K. (2016). Implementation and Comparison of M2M Protocols for Internet of Things. 4th Intl Conf on Applied Computing and Information Technology/3rd Intl Conf on Computational Science/Intelligence, 43-48.

[61] Pu wang, Y. z. (2018). Research and Design of AES Security Processor Model Based on FPGA. 8th International Congress of Information and Communication Technology (ICICT-2018), 249-254.

[62] Rama Chellappa, G. Q. (2014). VEHICLE DETECTION AND TRACKING USING ACOUSTIC AND VIDEO SENSORS. 793-796.

[63] Rishika Mehta, j. s. (2018). Intrenet-of-Things: Vision, Application and challenges. 1263-1269.

[64] Rolf H. Weber, R. W. (2010). Internet of Things Legal Perspectives. Springer-Verlag Berlin Heidelberg .

[65] S. C. Mukhopadhyay. (2014). Internet of Things Challenges and Opportunities. Springer International Publishing Switzerland .

[66] Sabrina Sicari, A. R.-P. (2018). REATO: REActing TO denial of service attacks in the Internet of Things. Computer Networks, 1-15.

[67] Sang-Woo Lee, J.-S. P.-S.-S. (n.d.). A Study on Smart-phone Traffic Analysis.

[68] Sattar J Aboud, M. A.-F.-F. (2008). An Efficient RSA Public Key Encryption Scheme. Fifth International Conference on Information Technology: New Generations, 127-130.

[69] Sayem Chaklader, J. A. (2014). Black Box: An Emergency Rescue Dispatch System for Road Vehicles for Instant Notification of Road Accidents and Post Crash Analysis.

[70] Shahid Razaa, P. M. (2016). Building the Internet of Things with bluetooth smart. Ad Hoc Networks, 1-13.

[71] Shancang Li, L. D. (2018). 5G Internet of Things: A Survey. 1-28.

[72] Shanzhi Chen, H. X. (2014). A Vision of IoT: Applications, Challenges, and Opportunities With China Perspective. IEEE INTERNET OF THINGS JOURNAL, 349-359.

[73] Shibin Li, J. W. (2013\). Nanoscale Sensors.

[74] Shubham Saloni, A. H. (2016). WiFi-Aware as a Connectivity Solution for IoT. International Conference on Internet of Things and Applications (IOTA), 137-142.

[75] Sohail Abbas, M. F. (2015). Masquerading Attacks Detection in Mobile Ad Hoc Networks.

[76] Stankovic, J. A. (2014). Research Directions for the Internet of Things. IEEE INTERNET OF THINGS JOURNAL, 3-9.

[77] Sye Loong Keoh, S. S. (2014). Securing the Internet of Things: A Standardization Perspective. IEEE INTERNET OF THINGS JOURNAL, 265-275.

[78] Tatsuki Otsubol, T. Y. (2012). Accuracy of Triangulation Method Sensor with Optical Skid Effect of Reconstruction Method. IEEE.

[79] Tibor Petrova, M. D. (2017). Computer Modelling of Cooperative Intelligent Transportation Systems. TRANSCOM 2017: International scientific conference on sustainable, modern and safe transport, 683-688.

[80] Tomáš Gregora, M. K. (2017). Smart Connected Logistics. TRANSCOM 2017: International scientific conference on sustainable, modern and safe transport, 265-270.

[81] Treffyn Lynch Koreshoff, T. R. (2013). Internet of Things: a review of literature and products. 335-344.

[82] Ulrich lang, R. (2015). Managing Security in Intelligent Transport System. 2015 IEEE 18th International Conference on Intelligent Transportation Systems, 48-53.

[83] V Arun, D. L. (2017). Encryption Standards for security system in Energy Harvesting for IoT requirements - Review. 1224-1227.

[84] Vikas Nyamati, T. C. (2017). Intelligent Collision Avoidance and Safety Warning system For Car driving. 791-796.

[85] Vishu Tyagi, A. K. (2017). Internet of Things and Social Networks: A survey. International Conference on Computing, Communication and Automation, 1268-1270.

[86] Yang Jun, L. N. (2009). A design and implementation of high-speed 3DES algorithm system. Second International Conference on Future Information Technology and Management Engineering, 175-178.

[87] Yihang Zhanga, P. A. (2018). Stability analysis and variable speed limit control of a traffic flow model. Transportation Research Part B, 31-65.

[88] Ying Li, L. D. (2013). A Lightweight Identity-Based Authentication Protocol.

[89] Yuchen Yang, L. W. (2016). A Survey on Security and Privacy Issues in Internet-of-Things. IEEE INTERNET OF THINGS JOURNAL, 1-10.

[90] Yuvraj Upadhyay, M. B. (2016). MQTT Based Secured Home Automation System. Symposium on Colossal Data Analysis and Networking (CDAN).

[91] Zeng, H. (2018). Demo Abstract: An Anti-Jamming Wireless Communication System. IEEE Conference on Computer Communications Poster and Demo (INFOCOM'18 Poster/Demo).

[92] Zhang Ye, C. G. (2008). Modeling and Application of Urban Dynamic Region Traffic Model based on information fusion. Fourth International Conference on Networked Computing and Advanced Information Management, 535-539.

[93] Zhang, Y. W. (2012). Internet of Things. © Springer-Verlag Berlin Heidelberg.