# IMPLEMENTATION OF LIGHTWEIGHT SECURITY PROTOCOL ON COMMUNICATING HARDWARE OF INTELLIGENT TRANSPORTATION SYSTEM

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 solutions. 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). [3] Apart from IOT, there is a description of how ITS operate. As the implementation 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. [8, 15] 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. [1,21] 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 VII 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.”[11, 15].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.[14,19] 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 other things. 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. [3, 6, 8, 20]

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). [18] Benefits of IOT will go as far as our imagination and that is limitless, millions of devices and sensors will be connected and lots 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.

## 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. [7,12,13] 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. [4,17,21]

### A. 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.[5,9,16]

## IV. 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"[10]

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.[2]

## V. RELATED WORK

Vijay Sharma, Amogh Vithalkar, Mohammad Hashmi in [23] proposed that, the RFID based communication between objects within the framework of IoT is potentially very efficient in terms of power requirements and system complexity. The new design incorporating the emerging Chipless RFID tags has the potential to make the system more efficient and simple. However, these systems are prone to privacy and security risks and these challenges associated with such systems have not been addressed

appropriately in the broader IoT framework. In this context, a lightweight collision free algorithm based on n-bit pseudo random number generator, X-OR hash function, and rotations for Chipless RFID system is presented. The algorithm has been implemented on an 8-bit open-loop resonator based Chipless RFID tag based system and is validated using BASYS 2 FPGA board based platform. Sahilkumar Chakraborty, Astha Nachrani, Aronee Dasgupta, Pritam Gajkumar Shah proposed different method in [24] there is a paramount need for developing a robust encryption which does not required heavy cryptography processes but still provides sufficient security for the required application. Wireless Sensor Networks have emerged as one of the leading technologies. These networks are designed to monitor crucial environmental parameters of humidity, temperature, wind speed, soil moisture content, UV index, sound, etc. However, security remains the key challenge of such networks as critical data is being transferred. Implementing a robust yet lightweight algorithm is needed not just in the central base station but also the sensor nodes. Hereby a protocol which is lightweight and is secure for wireless sensor applications is proposed. Xin-Wen Wu, En-Hui Yang, Junhu Wang In [25] this paper, a suite of lightweight security protocols for the Internet of Things (IoT) is presented. It comprises protocols for lightweight encryption, authentication as well as key management. The key management protocol is the application of our early work on information theoretically secure key management to IoT; it is computationally efficient and information-theoretically secure, and enables that every data item (file) is encrypted with its own random key. The security and computational efficiency of the proposed protocols are compared with those of IPsec. The proposed security protocols can be employed in IoT and CPS applications, replacing the IPsec core algorithms or the whole IPsec suite, to achieve a higher level of security with a very low resource consumption that helps to maintain the system sustainability. Kamanashis Biswas in [26] proposed that Wireless Sensor Network (WSN) consists of a large number of small sensor nodes (SNs) that are usually deployed in hostile environments. These nodes are vulnerable to a number of security attacks and it is difficult to implement complex cryptographic schemes in SNs due to their resource constrained nature. In this work, They propose a secure and lightweight encryption scheme based on chaotic map and genetic operations. We also present some initial results of security strength and performance evaluation experiments. Gaurav Bansod, Nishchal Raval, and Narayan Pisharoty in [27] this paper Lightweight cryptography is an interesting field that strikes the perfect balance in providing security, higher throughput, low-power consumption, and compactness. In this paper, They present the design of a new lightweight compact encryption system based on bit permutation instruction group operation (GRP), which is widely studied and extensively researched. Using the S-box of PRESENT, we have added the confusion property for GRP, because all the existing algorithms using bit permutation instructions do not have this confusion property.

## VI. PROPOSED WORK

All the Security methods such as AES, 3DES, Twofish, RSA 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 system, so we need algorithm which are light in overhead and over all resource consumption. Hence the name lightweight protocol is used more in IOT field.

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.

**Table – 1 Comparison With other Algorithm**

| Lightweight Algorithm | Block size(Bit) | Key length(Bit) | GEs(Gateway Equivalent) |
|---|---|---|---|
| HIGHT[5] | 64 | 128 | 3048 |
| mCrypton[5] | 64 | 64 | 2420 |
| SEA[5] | 96 | 96 | 3758 |
| TEA[5] | 64 | 128 | 2355 |
| ICEBERG[5] | 64 | 128 | 7732 |
| CLEFIA[5] | 128 | 128 | 2488 |
| PRESENT[5] | 64 | 128 | 1884 |
| PROPOSED ALGORITHM | 16 | 16 | 1000 |

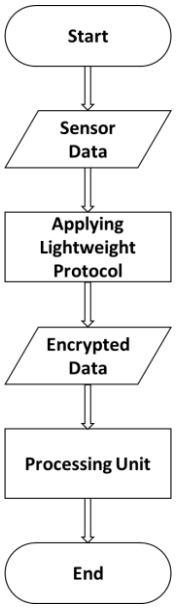


**Figure - 1 Flow chart**

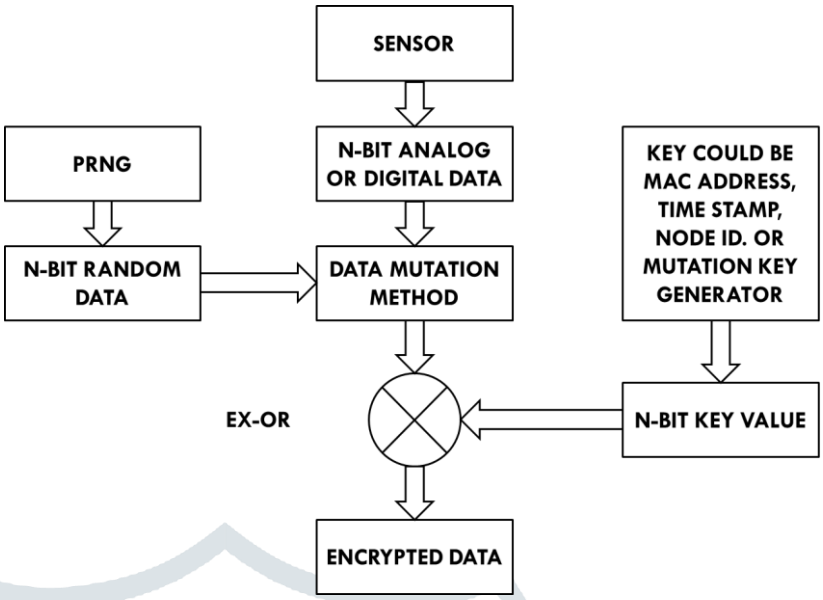


**Figure – 2 Block Diagram for Encryption.**

**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.

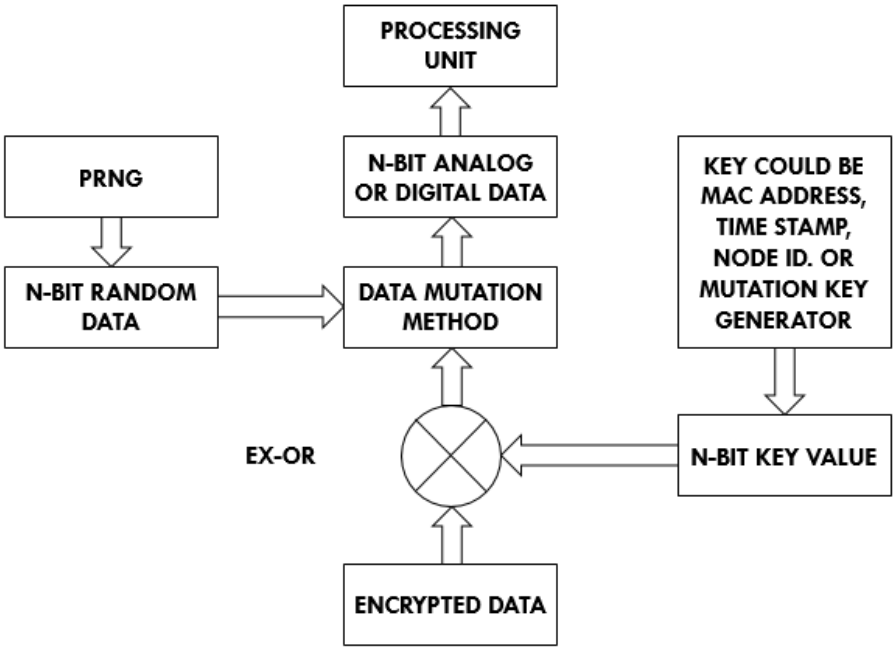


**Figure – 3 Block Diagram for Decryption.**

**Steps of Decryption block diagram**

Step 1: 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 Decrypted data which is sent to Processing unit.

## Proposed Pseudocode

**//encrypt**

```
String XOREncryption(String str, int key)
{
   String enc()
for (unsigned int i(0); i < str.length(); i++)
      enc += str ^ key;
   return enc;
```

**//decrypt**

```
String XORDecryption(String str, int key)
{
  String dec()
for (unsigned int i(0); i < str.length(); i++)
dec += str ^ key;
 return dec;
}
```

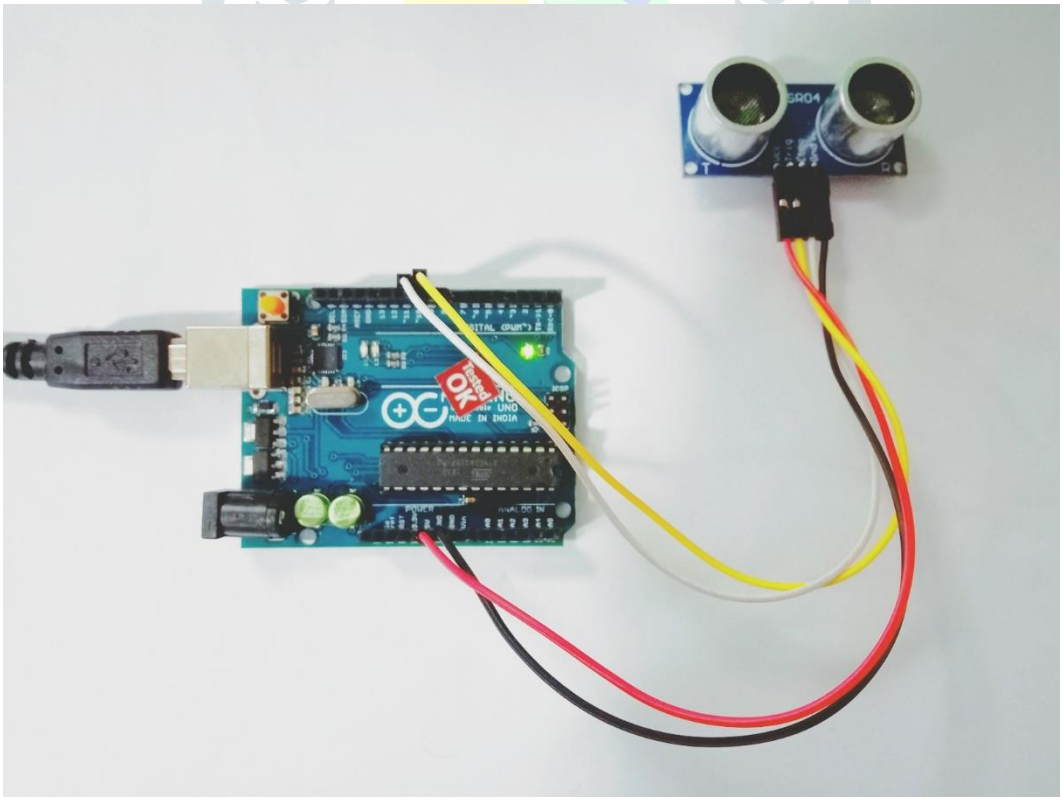

**Figure – 4 Hardware Setup**

```
Encryption key: 9LKSUR&#5A
CRIPTED:  §§§jø§§§ Computation time: 280 microseconds
ORIGINAL: 101110101   Real IV: 76 Computation time: 180 microseconds

Encryption key: 9LKSUR&#5A
CRIPTED:  ohluuz□fN Computation time: 280 microseconds
ORIGINAL: 101110101   Real IV: 76 Computation time: 184 microseconds

Encryption key: 9LKSUR&#5A
CRIPTED:  §§§§§§§§§ Computation time: 276 microseconds
ORIGINAL: 101110101   Real IV: 76 Computation time: 188 microseconds

Encryption key: 9LKSUR&#5A
CRIPTED:  §ø§§Uf§ Computation time: 280 microseconds
ORIGINAL: 101110101   Real IV: 76 Computation time: 180 microseconds

Encryption key: 9LKSUR&#5A
CRIPTED:  □□lhyw□fS Computation time: 276 microseconds
ORIGINAL: 101110101   Real IV: 76 Computation time: 180 microseconds
```

**Figure – 5 Program Output**

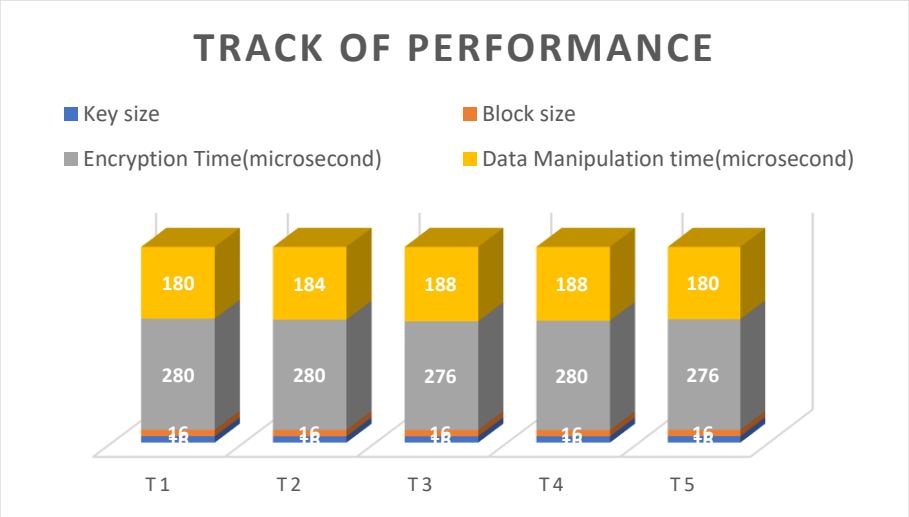


**Figure – 5 Bar chart Output**

## VII. 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.

## VIII. REFERENCES

[1] Anik Khokhar, Gayatri Pandi (2018). A survey on intelligent transportation system with the security perspective. Journal of Emerging Technologies and Innovative Research(JETIR), 759-93.

[2] 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.

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

[4] 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.

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

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

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

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

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

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

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

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

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

[14] 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.

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

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

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

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

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

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

[21] 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.

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

[23] Vijay Sharma, Amogh Vithalkar, Mohammad Hashmi "Lightweight Security Protocol for Chipless RFID in Internet of Things (IoT) Applications" 2018 10th International Conference on Communication Systems & Networks (COMSNETS).

[24] Sahilkumar Chakraborty, Astha Nachrani, Aronee Dasgupta, Pritam Gajkumar Shah "Lightweight Security Protocol for WiSense based Wireless Sensor Network " International Journal of Computer Applications (0975 – 8887) Volume 145 – No.3, July 2016.

[25] Xin-Wen Wu, En-Hui Yang, Junhu Wang "Lightweight Security Protocols for the Internet of Things" IEEE 2017.

[26] Kamanashis Biswas "Lightweight Security Protocol for Wireless Sensor Networks" IEEE 2014.

[27] Gaurav Bansod, Nishchal Raval, and Narayan Pisharoty "Implementation of a New Lightweight Encryption Design for Embedded Security" IEEE Transactions On Information Forensics And Security, Vol. 10, No. 1, January 2015