A Totalitarian Technique For Wormhole Detection Using Big Data Analytics In Lot Network

Ms. Gauri Mathur, Dr Wiquas Ghai

Abstract: Internet of Things is one of the most important paradigm in current world which allows connectivity and communication between heterogeneous devices so as to achieve better synchronization and automation with control. These days Internet of Things have gained immense popularity as they function without major requirements of infrastructure and they can function without any central controlling authority. In order to implement communication between devices many sensors are used to collect data, process it, encrypt (e.g. using AES-128, RSA, DSA) and upload it to the cloud. There is huge presence of IoT devices which generates voluminous data called as big data in medical, military, banking and marketing fields but poor security features make it easy for attackers to perform both active attacks and passive attacks. Hence one of the primary objectives is to make this network secure by identifying presence of malicious wormhole which can mitigate in a mobile ad-hoc network. In this proposed paper we will compare various existing wormhole detection techniques in IoT Network and will propose an efficient algorithm which will evaluate the routing tables of nodes connected to IoT Network on the basis of path used, frequency of presence of nodes in table along with threshold value generated by nodes using big data analytics.

Index Terms: Internet of Things, Big Data, Wormhole Attack, threshold value, routing table, Detection techniques, synchronization

1. INTRODUCTION

Internet of Things is a computing conceptualization where in everyday physical objects connect to the Internet and make their presence known to other devices so as to achieve better synchronization and automation with control. To enable communication between two devices anywhere at any time using any network is goal of Internet of Things. The IoT technology works on a three tier architecture namely network layer, application layer and perception layer as depicted in Figure 1. A significant number of data sensors inclusive of Barcodes, RFID and any other smart devices on sensor network form the perception layer. Its major use is to collect and distribute information from the sensors and pass it on to the network layer. The network layer passes on the collected information obtained from the perception layer to any information processor using the network of mobile devices, internet or any other trustworthy network. The main aim of IoT in developing a smart environment is realized at the application layer in the end. The aim of establishing a secure network of IoT devices is a major issue due to heterogeneity, complexity and a wide number of inter-connected components. The intruder may tamper or damage a few nodes in the network of IoT devices or may decide to take advantage of the faults in routing protocols or other network related protocols. A malicious program may also be used to perform the encryption attack. These vulnerabilities results in classification of the attacks in various categories namely network attack, encryption attack, software and physical attack.

- *Ms.GauriMathur, PhDScholar, RIMT University, India, Assistant professor, Lovely Professional University, India Email: gauri.mathur@lpu.co.in Phone number: +91 8146543737*
- *Dr. Wiqas Ghai, Associate Professor, School of Computer Science and Engineering, RIMT University, India Email: ghaialpha@gmail.com Phone Number:+91 9988428677.*

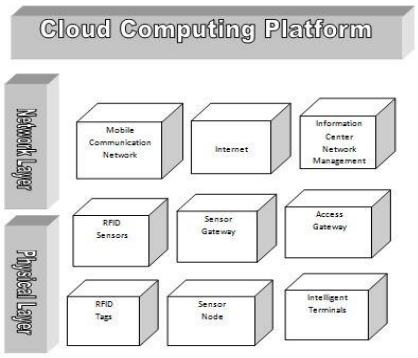

Figure 1: *Architecture of Internet of Things*

1.1 Wormhole Attack

In wormhole attack, a malicious user can connect two distant nodes in the network via direct communication link in the IoT also known as wormhole link. Once a wormhole attack is initiated, the nodes performs wireless transmission on one end and send it through the wormhole link and replay them to the other destination. A wormhole can be identified in a pre setup network and malicious nodes try to infiltrate at further stage and other situation when the malicious nodes are already existing while network setup. A wormhole attack involves the creation of two colluder nodes namely X and Y as depicted in the adjoining figure 1. Both the nodes X and Y are joined together by a wormhole path and the target of attack is the node S1. The path detection and discovery process entails the broadcast of a special message RREQ (i.e. request packet) to a destination node H1. The nodes A1 and C1 who are neighbors of node S1, receive the RREQ packet and forward the same to their neighbors. This RREQ packet which is forwarded by node A1 is received by the colluding node X. This RREQ packet information is recorded and tunnelled by the high-speed wormhole link to its partner node Y. The colluding node Y forwards the RREQ packet to its neighboring node B1.In the end, the node B1 forwards this packet to the destination node H1. Hence the RREQ packet information is passed on via the path node S1-A1-X-Y-B1-H1. The same RREQ packet is also passed through the path S1-C1-D1-E1-F1-G1-H1. As the colluding nodes X and Y are joined with a high speed link, RREQ from the S1-A1-X-Y-B1-H1 reaches H1 first. This prompts the destination node H1 to

ignore the RREQ which reaches late and choose the path H1-B1-A1-S1 to perform a unicast of RREP packet to the source node S1. This result in the node S1 choosing S1-A1-B1-H1 path to send data which actually passes through colluder nodes X and Y which are placed better in comparison to some other nodes in the IOT. Hence we can observe that a wormhole attack is not hard to set up, however it can seriously hamper the network.

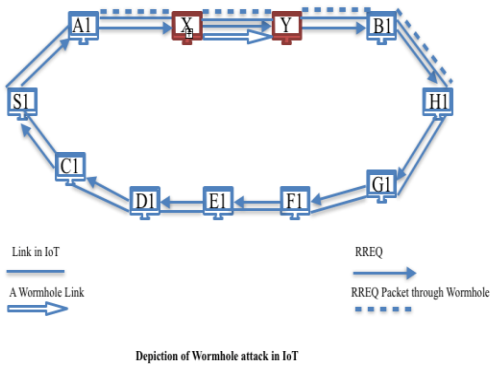

Fig 2 *Detection of Wormhole Attack in IoT*

1.2 Big Data in IoT

Recent studies claim that the number of devices connected to the Internet has surpassed the number of human beings in the world. All of this coupled by IoT network gives rise to insurmountable amounts of information. The overlap between the growth of data consumption by IoT devices and the number of devices connected to the IoT network signals the exponential rise of Big Data. Furthermore, the data generated by the mesh of IoT devices bearing temporal and spatial characteristics by its sheer volume is classified as Big Data and it is at a serious threat of being maligned and misused. The enormous amount of data classified as Big Data is generated and over time it is often seen as the core competitive factor driving organizational growth and development. Big data is of prime significance and needs to be secured as often it bears confidential information which is paramount to the organization's survival. An organization should strive to provide security and establish trust as sensitive data could very well turn out to be a potential goldmine to the prospective attackers. The utilization of Internet of Things in enterprises comprising of but not limited to banking, manufacturing, marketing, banking leads to a flood of unstructured, semi – structured and structured data and this is the root cause of a profusion of security breaches. The gamut of precious information presents a potential gold mine to the attackers of an IoT network and hence presents a big security threat. This aggresive growth has led to new challenges in data collection efficiency, security and data analysis. A secure solution for sensitive information comprising of big data is of utmost importance as its proper implementation can fuel any big data initiative. One of the grave threats to the security and integrity of Big Data is a Distributed Denial of Service (DDoS) attack which works by disrupting the services of a network machine or host by making the network resource inaccessible to the intended users. A wormhole attack can seriously undermine and suspend the trusted operation of any IOT network and seriously jeopardize and put at risk big data. The use of Big data processing and analytics can help us in thwarting the DDoS attacks as this information could be put to good use. In this proposal, we try to create a new approach which is different from the existing approaches for detection of wormhole Attack. This newly adopted approach has benefit of memory management and processing as compared to already existing techniques of wormhole detection. It also utilizes modified routing table where the routing table are modified further to have information of all the paths of each node and the next hop. Further, the information provided by the big data analytics lays down the foundation of our approach for thwarting the DDoS attacks in the IoT networks. This paper highlights the various techniques which are generally used in the detection of wormhole in the IoT network and the need for yet another approach to detect and to mitigate the effect of wormhole attacks.

2. SECURITY CHALLENGES:

Security is a major concern and indeed the most challenging issue in the field of IoT. Increase in the number of connected smart devices also increases the opportunities to exploit security vulnerabilities, as sometimes poorly designed smart devices, can be exposed to theft by leaving data inadequately protected and in few cases can cause harm to people's health and safety. Some of the prime security challenges include:

2.1 Privacy

The Internet of Things imparts different challenges to privacy. Many of it can stem from integrated devices into our environment without us consciously allowing them to invade. Smart devices like tracking devices for cars and phones as well as smart televisions have become highly prone to privacy attacks. Attackers can invade the conversations or watch for activity and selectively transmit that data to a cloud service for processing, which sometimes includes a third party. A case in point in the privacy challenges include the smart TV manufacturers collecting information about their users and analysing the usage patterns. In some instances insurance firms have installed smart devices to collect driver information which has been used to settle insurance claims.

2.2 Data Security

Data Security also poses a huge challenge among communicating devices which interchange data during communication and many times this data has inadequate protection which compounds the problem of Data Security.

2.3 Standards

Some efficient standards and guidelines should be implemented for implementation of IoT devices. Due to the vast gamut of standards and guidelines present and absence of any common standards, there is no consistency among the devices connected to the IoT network.

2.4 Regulations

There are wide range of regulatory and legal issues surrounding the IoT, which needs to be seriously considered. There are non clarity in legal issues and law enforcement surveillance and civil rights. Still be have not developed clear legal policies for data destruction or data retention policies. There should be strict policies to protect unintended users,

security breaches and unauthorized access. Further, technology is advancing rapidly in comparison to legal policies and regulatory laws.

2.5 Technical Issues:

The wide range and amount of devices connected to the internet result in an increase in traffic and hence network capacity as well as storage should be increased to handle the uptick in traffic and the amount of devices connected to the internet.

3. RELATED WORK:

The history of Internet of Things [1] research challenges, introduced the concept of Internet of Things database and proposed different architectures of Internet of Things, open problems related to the Internet of Things and discuss about the future vision of Internet of Things. Internet of Things is connection of equipment, machine, software and everything around us to make these as smart things which have unique IP address to distinguish from other things. Smart home, wearable, health care, smart environment are some examples of IoT applications. In Internet of Things everyday objects can be given capabilities of identifying, sensing, networking and processing capabilities so they can communicate with each other. The popularity of IoT devices brings with it a plethora of problems with some noteworthy malware targeting IoT devices only. Especially, IoT facilitates the creation of an assortment of privacy risks to the consumer associated with the collection of personal and sensitive information. Wormhole attack is a type of external attack initiated by a pair of colluding attackers which are connected on both sides by wormhole links. In[2] authors have proposed a magnificent approach called ADWA (Acknowledgement based technique for detection of the wormhole attack) in Routing Protocol for Low power and lossy networks based Internet of Things networks . This technique works on the acknowledgments send via the nodes in DODAG to the gateway node (root node of the DODAG). The acknowledgement consists of the neighbours nodes of each node in a DODAG of the RPL protocol. Based on the neighbours of each node the malicious node of the wormhole attack can be detected. In [3] authors proposed another RPL-based wormhole detection mechanism. Using this technique the rank of a node-defined RPL is adopted to calculate accurate the distance. The proposed detection method discovers malicious wormhole nodes if unreasonable rank values are identified. The experimental results show that the proposed detection method can identify wormholes effectively under various wireless sensor networks. Another approach proposed by authors in [4] utilizes location information of each node along with the information of its adjoining nodes to identify the Wormhole attack and signal power to identify offensive nodes. Designing of this kind of system will help use to secure IoT network and possibly thwart malicious attacks. The method is highly efficient in terms of energy requirements and takes quantified number of User Datagram packets for the presence of attack, hence it is very useful for resource strapped environment. Yet another is termed as DELPHI [5], which is Delay Per Hop Indication. In this approach, the metric used to determine the existence of wormhole is the delay per hop observed from different paths from source to destination. In paper [6] Directional antennas can also be used to handle and thwart the wormhole attacks. In order to achieve this aim, directional antennas are installed which give incorrect information from nodes which can be avoided. Another scheme which uses the location information gathered with the help of GPS is E2SIW which stands for Energy Efficient Scheme Immune to Wormhole attacks and this information is used for the prevention of wormhole attacks. This approach is more of a preventive approach and does not contain features and facilities to detect a wormhole node and their treatment. In [7] advocated the use of Average One hop RTT in order to calculate average time of larger paths which could be used to avoid wormhole links. The average RTT times hops of the link are noted and in case a link has taken more time than this then this is most likely a suspicious and will be debarred from further communications. The cases where the stated approach may run into trouble are when a high speed link or a congested network are encountered. In [8] proposed a technique based on distance verification for applications on mobile ad hoc network(MANETs). The received signal strength (RSS) of received packets are used to estimate the distance to a sender node and the same is used to verify against the distance computed from the information extracted from the packets. The details about attacks on RPL and 6LoWPAN and their measures on it are well discussed in [9]. In [10] authors proposed a new mechanism known as packet leashes, for detecting and defending against wormhole attacks, and presents a specific protocol called TIK, that implements leashes. In [11] authors discussed the protocols that require an authentication mechanism which is also known as True Link. True Link is virtually independent of the routing protocol that used. The performance evaluation shows that true link provides effective protection against potentially devastating wormhole attack. The [12] authors proposed SAM to detect attacks and to identify malicious nodes, Comparing to the previous approaches; no special requirements are needed in these scheme. Whenever, SAM may act as a module in local detection agents in an intrusion system for wireless ad hoc networks. In [13] author discussed particular severe security attack that affects the ad hoc networks routing protocol is called the wormhole attack. The wormhole attack is two phase process launched by one or several malicious nodes. In [14] author presents a secure routing mechanism against wormhole attack in IPv6 based WSN. The design of this routing mechanism can be classified in to two phases" wormhole defence and detection, which is based on the average distance per hop in the network and the TTL of IP header. In [15] author discussed subtlest security attack in RPL WSANs is the wormhole attack. In which a malicious actor establishes and controls an out of band channel between two distant nodes of the network. Due to its convenience RPL is induced to use such a channel to forward the traffic. In [16] authors proposed a new scheme that monitors the signal strength of nodes, if distance found greater than default distance then the attack is detected. Both techniques act as backup of each other such that if one method fails other will detect the attack. This scheme doesn't require excessive power or specialized hardware equipment which is quite useful in resource constrained environment. The mesh of network of IoT devices gives rise to Big data and so that it's substance may not be undermined it is pertinent to ensure that it is safe from malicious users. There is an uptick in the usage of analytics

in Big data with Big data analytics frameworks coming to the forefront. In [17] authors have proposed an IoT big data analytics framework to overcome the challenges of storing and analyzing large amount of data. Author in [18] proposed an IoT-based cyber physical system supporting information analysis. In [19] authors have analyzed the traffic management systems. The wealth of information encompassed in the Big data is at risk due to DDoS attacks with wormhole and blackhole being the primary miscreants among them. There has been a paradigm shift towards ensuring the safety of Big data by organizations as they strive to stay atop the competition. Big data analytics can come to our rescue as is evident with the scale of work in this direction. The approach proposed makes use of data analytics to detect the presence of a supposed wormhole and can aid in prevention of DDoS attacks.

4. PROPOSED WORK

The proposed technique consists of a modified routing table to detect and overcome these attacks along with use of data analytics to identify malicious and malignant nodes and isolating them to prevent further damage to the network and to stop them from adversely impacting the network throughput. A conglomerate of simulators shall be used for the implementation of the newly formed technique. The proposed DOS attack detection algorithm will be implemented in the hypothetical network and the volume of Big data generated at specified alternating intervals of time will be broadcast and deviation from the same will be a good indicator of malignant nodes which will be simulated as participants in Wormhole Attack in the said network to analyze and verify the critical findings of the proposed detection algorithm. The ease of implementation and accuracy of detection are the key identifiers of an efficient DOS attack detection algorithm. These are the key parameters on which we will evaluate our implementation of the proposed DOS attack detection algorithm on the IoT routing protocols. On careful analysis of the diverse wormhole attacks a common pattern is observed wherein a path is showcased between the colluder nodes which make up a wormhole and all the other nodes choose a path which lies through this spiteful path. If we keep a track of these changes, we are able to detect a wormhole / blackhole link as soon as it comes up and make necessary amends. All this could be achieved if we give the nodes the capability of sharing and analyzing the routing tables of each other. The hop count is a good indicator of the presence of a potential wormhole and or a blackhole in the IOT network. In case the hop count is indicative of something malicious there could be a couple of considerations which are as follows: Consideration 1) The network exists and has been configured and the wormhole nodes infiltrate later. Consideration 2) The wormhole nodes were present when the network was being setup. A quick drop in the hop count is indicative of a potential wormhole and or a blackhole in the system. The proposition of a modified routing table is capable of detecting suspicious links, confirmation of wormhole existence and isolation of confirmed wormhole nodes. The approach will be applied to various routing protocols prevalent in IOT such as DSR, AODV and OLSR. The modification of proposed routing table technique could very well result in reduced memory usage and conservation of processing time. On the discovery of a likely wormhole we still need to confirm if it actually is the wormhole. This is confirmed by performing a series and a variety of tests. The results of these tests will convey adequate information about the existence of a wormhole link formed by the colluder nodes. Proceeding this way our aim is to send these colluder nodes which form a wormhole link into isolation. This approach offers us with a chance to identify the suspected wormhole links in the network before they start disrupting the network. This minimizes the damage which could be done to the network by these wormhole links. It is still possible that a number of paths and nodes have a high percentage of usage, however if the same nodes are figuring again and again then this indicates the presence of a possible wormhole in the network.

COMPARATIVE DISSOLUTION OF WORMHOLE DETECTION TECHNIQUE					
METHODOLOGY USED	*MOBILITY*	*FAULT TOLERANCE*	*SYNCHRONIZATION*	*RESOURCES NEEDED*	*QOS*
Packet Leashes Technique	*Bound with maximum transmission distance*	*Less as synchronization is required*	*Less synchronization*	*More resources are required as synchronized clocks are needed*	*Delay up to leash factor*
DELPHI technique	*No need*	*Moderate due to large packet size*	*No synchronization is needed.*	*Less resources are needed as packet size increases.*	*Delay*
SECTOR technique	*No need to Time synchronization*	*Low due to synchronization requirements*	*No synchronization is needed.*	*More as synchronization is needed*	*No delay*
Proposed new technique	*Not required*	*More*	*No synchronization is required.*	*Minimal resources are required as routing table undergoes modification*	*No delay*
SAW	*Delay is observed*	*Low due to maintenance of neighbor information*	*No synchronization is required.*	*Medium as neighbor data is needed*	*Not required*
DAW	*Not considered*	*Moderate but better than SAW*	*Not considered*	*Medium and better as compared with SAW*	*Delay parameters*
Directional antennas	*Less due to the signal strength constraints of antennas*	*Less due to signal issues*	*Low synchronization*	*More resources as required as directional antennas are needed.*	*Delay*

Table 1: *Comparative dissolution of wormhole Techniques*

5. CONCLUSION AND FUTURE WORK

The IoT devices are responsible for generating a wealth of information classified as Big data which is the prime concern of an organisation. A DOS attack severely hampers the productivity and security of a network of IoT devices and hence puts the Big data at risk. The prime DOS attacks include Wormhole attack and although there exists certain techniques for the detection of the same, yet

efficient detection of these attacks can lead to an improved and more secure IoT network which results in increased network throughput. The proposed technique consists of a modified routing table to detect and overcome these attacks along with use of data analytics to identify malicious and malignant nodes and isolating them to prevent further damage to the network and to stop them from adversely impacting the network throughput. The key points of the proposed technique should be outlined and defined in a clear and concise manner. Also, the proposed technique will be implemented on the AODV and DSR IoT routing protocols and a parallel will be drawn on the implementation on the corresponding routing protocols and certain existing techniques of DOS attack detection. A conglomerate of simulators inclusive of but not limited to NetSim, IBM Bluemix and NS3 may be used to carry out the establishment of a hypothetical IoT network which models a real world network of IoT devices. The proposed DOS attack detection algorithm will be implemented in the hypothetical network and the volume of Big data generated at specified alternating intervals of time will be broadcast and deviation from the same will be a good indicator of malignant nodes which will be simulated as participants in the Wormhole attack in the said network to analyze and verify the critical findings of the proposed detection algorithm. The ease of implementation and accuracy of detection are the key identifiers and indicators of an efficient DOS attack detection algorithm. These are the key parameters on which we will evaluate our implementation of the proposed DOS attack detection algorithm on the IoT routing protocols. A parallel needs to be drawn on the various attack detection techniques with our detection mechanism and a comparison in terms of efficiency, effect on network throughput, congestion, ease of traffic control, packet delivery times and consumption of network resources should be carried out. The technique will also be analyzed in terms of adaptability to changing factors. The proposed DOS attack detection algorithm seems to perform better on the above parameters at the outset but a thorough analysis of the same needs to be carried out in order to confirm this hypothesis.

6.REFERENCES

[1] Hameed, Sufian, Faraz Idris Khan, and Bilal Hameed. "Understanding security requirements and challenges in Internet of Things (IoT): A review." Journal of Computer Networks and Communications 2019 (2019)

[2] Neerugatti, Vikram, and Rama Mohan Reddy. "Acknowledgement Based Technique for Detection of the Wormhole Attack in RPL Based Internet of Things Networks." Asian Journal of Computer Science and Technology 8, no. S3 (2019): 100-104

[3] Gaddour, Olfa, and Anis Koubâa. "RPL in a nutshell: A survey." Computer Networks 56, no. 14 (2012): 3163-3178

[4] Pongle, Pavan, and Gurunath Chavan. "Real time intrusion and wormhole attack detection in internet of things." International Journal of Computer Applications 121, no. 9 (2015)

[5] Chiu, Hon Sun, and King-Shan Lui. "DelPHI: wormhole detection mechanism for ad hoc wireless networks." In 2006 1st international symposium on Wireless pervasive computing, pp. 6-pp. IEEE, 2006

[6] Dai, Hong-Ning, Kam-Wing Ng, Minglu Li, and Min-You Wu. "An overview of using directional antennas in wireless networks." International journal of communication systems 26, no. 4 (2013): 413-448

[7] Raju, V. Karthik, and K. Vinay Kumar. "A simple and efficient mechanism to detect and avoid wormhole attacks in mobile ad hoc networks." In 2012 International Conference on Computing Sciences, pp. 271-275. IEEE, 2012

[8] Li, M. Yifeng Zhou Louise Lamont. "Wormhole Attack Detection Based on Distance Verification and the Use of Hypothesis Testing for Wireless Ad Hoc Networks." (2009)

[9] Shreenivas, Dharmini, Shahid Raza, and Thiemo Voigt. "Intrusion Detection in the RPL-connected 6LoWPAN Networks." In Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, pp. 31-38. ACM, 2017

[10] Eriksson, Jakob, Srikanth V. Krishnamurthy, and Michalis Faloutsos. "Truelink: A practical countermeasure to the wormhole attack in wireless networks." In Proceedings of the 2006 IEEE International Conference on Network Protocols, pp. 75-84. IEEE, 2006

[11] Song, Ning, Lijun Qian, and Xiangfang Li. "Wormhole attacks detection in wireless ad hoc networks: A statistical analysis approach." In 19th IEEE international parallel and distributed processing symposium, pp. 8-pp. IEEE, 2005

[12] Azer, Marianne, Sherif El-Kassas, and Magdy El-Soudani. "A full image of the wormhole attacks-towards introducing complex wormhole attacks in wireless ad hoc networks." arXiv preprint arXiv:0906.1245 (2009)

[13] Chen, Tao, Haiping Huang, Zhengyu Chen, Yiming Wu, and Hao Jiang. "A secure routing mechanism against wormhole attack in IPv6-based wireless sensor networks." In 2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP), pp. 110-115. IEEE, 2015

[14] Perazzo, Pericle, Carlo Vallati, Dario Varano, Giuseppe Anastasi, and Gianluca Dini. "Implementation of a wormhole attack against a rpl network: Challenges and effects." In 2018 14th Annual Conference on Wireless On-demand Network Systems and Services (WONS), pp. 95-102. IEEE, 2018

[15] Ahsan, Muhammad Saad, Muhammad Nasir Mumtaz Bhutta, and Moazam Maqsood. "Wormhole attack detection in routing protocol for low power

lossy networks." In 2017 International Conference on Information and Communication Technologies (ICICT), pp. 58-67. IEEE, 2017

[16] Khan, Faraz Idris, Taeshik Shon, Taekkyeun Lee, and Kihyung Kim. "Wormhole attack prevention mechanism for RPL based LLN network." In 2013 Fifth International Conference on Ubiquitous and Future Networks (ICUFN), pp. 149-154. IEEE, 2013

[17] Bashir, Muhammad Rizwan, and Asif Qumer Gill. "Towards an IoT big data analytics framework: smart buildings systems." In 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), pp. 1325-1332. IEEE, 2016

[18] Lee, Jay, Hossein Davari Ardakani, Shanhu Yang, and Behrad Bagheri. "Industrial big data analytics and cyber-physical systems for future maintenance & service innovation." Procedia Cirp 38 (2015): 3-7

[19] Rizwan, Patan, K. Suresh, and M. Rajasekhara Babu. "Real-time smart traffic management system for smart cities by using Internet of Things and big data." In 2016 international conference on emerging technological trends (ICETT), pp. 1-7. IEEE, 2016