International Journal of Engineering Trends and Applications (IJETA) – Volume 3 Issue 2, Mar-Apr 2016

RESEARCH ARTICLE OPEN ACCESS

Applications and Challenges Faced By Internet of Things - A Survey

Syed Roohullah Jan, Fazlullah Khan, Nazia Azim, Muhammad Tahir, Shahzad
Department of Computer Science
Abdul Wali Khan University Mardan

Muhammad Safdar
Department of Computer Science
Bacha Khan University, Charsadda.
Pakistan

ABSTRACT

The Internet of Things (IoT) is a vision that broadens the scope of the internet by incorporating physical objects to identify themselves to the participating entities. This innovative concept enables a physical device to represent itself in the digital world. There are a lot of speculations and future forecasts about the Internet of Things devices. However, most of them are vendor specific and lack a unified standard, which renders their seamless integration and interoperable operations. Another major concern is the lack of security features in these devices and their corresponding products. Most of them are resource-starved and unable to support computationally complex and resource consuming secure algorithms. In this paper, we present a survey of various applications which have been made possible by IoT. Furthermore, the challenges faced by these networks are presented in detail.

Keywords:- *IOT,* IETF, CoRE

I. INTRODUCTION

Twenty first century has revolutionized the world of technology. Size of internet has been increasing rapidly with integration of miniaturized embedded devices into the internet world. Automation systems, personal gadgets, smart grid, cell phones and many other devices collaborate with each other and share valuable information about physical world. Internet is moving from traditional workstation and laptops to small embedded devices. We are moving from internet to Internet of Things (IoT) [1] by incorporating a sheer number of physical devices into internet. These objects contain miniature sensor nodes at their core which inherits all the limitations of Wireless Sensor Networks [2-6]. IoT extends internet beyond personal computers, work stations to the world of physical objects. A broad range of appliances are now connecting to internet and provides valuable information. In internet, humans are the main source of generating information ranging from sending emails, capturing videos to messaging and browsing are some to mention. However, in IoT of the future, there will be millions and trillions of smart objects which will collect information, process it and communicate it. IoT relies of a set of distinct technologies which collaborate with each other. The major technologies behind this vision of IoT are Identification, sensing, embedded processing and communication are some to mention [7]. Radio Frequency Identification (RFID) tags are attached to physical world.

objects which contain data about those objects. These small tags are not capable to sense the environment but have the ability to collect data about a product. Internet of Things would not have been possible without them as they provide each object a unique identification to be recognized on the internet. On the other hand, sensor networks are capable to sense the environment based on unique identification provided by RFID tags and can also monitor their location, energy and other parameters. Once data is being sensed, partial processing take place at each object which is further transmitted for various operations to extract valuable information from it.

The Internet Engineering Task Force (IETF) created a working group called Constrained RESTful Environment Group (CoRE) group. This group was assigned the task to define a mechanism using which a large number of small, resource constrained, low power devices, can communicate over lossy networks. This group defined a set of specifications that is known today collectively as Constrained Application

Protocol (CoAP). CoAP is an application-layer that is designed to allow message exchange between resource-constrained devices over resource constrained networks [8-17]. Resource constrained devices are small devices that lack the processing power, memory footprint and speed that we generally expect from our computing devices. These devices often are built using 8-bit microcontrollers or low-cost, general purpose 32-bitmicrocontrollers. Resource constrained networks are network stacks and configurations that do not have the full capabilities of TCP/IP stack and have lower transfer rates. CoAP runs over UDP and not TCP. IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) is an example of such a constrained network configuration setup [18-23]. CoAP provides an HTTP-like request and response paradigm where devices can interact by sending a request and receiving a response. Like the web, devices are addressed using IP address and port number. Access to services exposed by the device is via RESTful URIs. It's very much similar to HTTP, where method type (e.g. GET, PUT), response codes (e.g.404, 500) and content-type are used to convey information. Given the protocol's close similarity to HTTP, it's obvious that it was designed for easy web integration. CoAP does not replace HTTP, instead, it implements a small subset of widely accepted and implemented HTTP practices and optimizes them for M2M message exchange [24-31]. Think of CoAP as a method to access and invoke RESTful services exposed by "Things" over a network.[20].

In this survey paper, we discuss the applications of IoT and the wide range of challenges faced by these networks. The applications of IoT are restricted by various challenges faced by these networks at various layers. The rest of the paper is organized as follows. In Section 2, potential applications are discussed. In Section 3, various challenges faced by these networks are discussed. Finally, the paper is concluded and future research directions are provided in Section 4.

II. APPLICATIONS OF INTERNET OF THINGS

The IoT allows us to use technology to enhance our comfort, improve our energy efficiency, and simplify the tasks that consume our home and work life and give us greater control over our lives. Here, we discuss various applications of an IoT

.

2.1 Connected Home:- A Connected Home can mean different things to different people, but it's essentially a home with one or more (or many) devices connected together in a way that allows the homeowner to control, customize and monitor their environment. That can mean anything from a programmable learning thermostat to a security system of window, door and motion sensors, to the future of smart appliances. The common denominator is that ideally all of these devices should come together into a connected ecosystem that is easy for the homeowner to access and control. If the IoT is fundamentally about making our lives easier and more connected, then the implications for a truly Connected Home are game-changing. For example, do your kids get home before you every day? With the right devices you can know when one of them comes home, or if one leaves. You can make sure that they don't crank down the thermostat to Antarctic levels. You can even keep an eye on who's with them, and get the fridge to remind you via text message to pick up milk on your way home. That's just one example of how a Connected Home can increase control over your life and reassure you about your family's safety. The practical applications are almost infinite [15] [6,8].

1.2 Wearable:-

Wearable technology is a blanket term that covers a vast array of devices that monitors, record and provide feedback on you or your environment. Broadly speaking, you can divide wearables along two lines:

1.2.1 Fitness and Environment:-

Fitness bands and watches and even smart clothes are able to monitor and transmit data on your daily activity levels through step counting, heart rate and temperature.

2.2.2. Health:-

These wearable monitor crucial health factors like oxygen saturation, heart rate and more, and can communicate any results outside of a programmed range to the patient and to her physician.

The two key considerations when it comes to designing a useful wearable are energy efficiency and size. That's why so many wearable manufacturers choose Silicon Labs' 32-bit ultra-low power MCUs and our reliable sensor solutions. These compact components power complex data processing on the chip, reducing the amount of data that has to be transmitted to other devices like your smartphone, all without draining battery life.

2.3 Industrial Automation and Industrial IoT:-

The Internet of Things has profound implications for industrial automation and the industrial internet of things. With wireless connectivity, advanced sensor networks, machine-to-machine communications, traditional industrial automation will become more informed and more efficient than ever before.

Silicon Labs industrial isolation products protect equipment from noisy power planes and communications busses.

- Our custom timing products offer unmatched flexibility in industrial clocks, buffers and oscillators.
- And our isolation, microcontrollers and wireless MCUs provide easy on-ramps to motor control, system interconnects and adding wireless.

2.4 Smart Metering:-

A smart meter is an internet-capable device that measures energy, water or natural gas consumption of a building or home. With Smart Energy Metering, not only do technicians not have to come and physically read your meter, you have access personally to your energy usage so you can see what impact your consumption patterns have on your wallet and on the environment.

2.5 Transportation:-

CoAP protocol is used for tracking the vehicle by fetching the GPS coordinates of the vehicle position at a specific point of time. It monitors the speed of the vehicle by fetching the reading of the accelerometer of the vehicle. A simple symmetric handshaking for various states of the vehicle (Fast moving, slow moving and Rest) is investigated. The overhead incurred during the communication and handshaking is quiet low which suits the requirement of energy constrained devices.

These are just a subset of applications. There are many other applications of IoT. The scope and nature of IoT provides a wide range of opportunities for various applications. Currently, a wide range of research is being conducted to investigate the applications of CoAP and various other IoT protocols for physical objects of daily life.

III. CHALLENGES FACED BY INTERNET OF THINGS

Internet of Things consists of a bunch of physical devices connected with each other. The devices themselves are resource-rich; however, they will not be able to communicate with each other in absence of sensor nodes. The presence of sensor nodes at the core of each physical device makes the device intelligent and enables it to identity itself in the digital world. These sensor nodes are resource-constrained and as a result classify the device as resource-constrained as well [10, 11, 12]. Resource-constrained devices vary from one another in term of space code, RAM and other specifications which affects their capabilities to support HTTP protocol. Resource-constrained devices having 10KBytes of RAM and about 100Kbytes of ROM are not capable to support HTTP (Class 1 devices) while those having 50Kbytes of RAM and around 250Kbytes of ROM support HTTP (Class 2 devices) [13]. However, HTTP requires considerable amount of code space and ROM along with high energy in processing, so Class 1 devices refrain from adapting HTTP. As a result, extremely lightweight protocols such as CoAP need to be developed to make them feasible for IoT. The protocols need to adjust the battery power of each object so that they can operate for months and years for as little as 1 watt.

Another challenging issue for IoT is interoperability [7]. As IoT incorporate a series of devices, hence, interoperability between various devices is a serious issue. Most of these objects have their own underlying hardware and software platforms and as a result, they are not able to communicate with each other. As a result, a common and unified standard for various technologies is required. The use of such a standard will provide seaming-less operations.

The devices require a scalable application layer for interoperable communication. Moreover, a common programming model is required, which will enable programmers to focus only on application development rather than the hassle of worrying about underlying platform architecture. In [14], the authors proposed an innovative solution to cope with these challenges by curbing the installation of application code on the embedded systems. Rather, they suggest that application code should run on the cloud and only firmware and network stack will be nested in the core of each embedded device. Running applications on cloud will serve two major purposes: ample memory space availability on the nodes and most importantly, developer will not have to worry about the hardware architecture[17]. The latter will help to develop applications on cloud which will enhances communication between heterogeneous nodes irrespective of any programming language. RESTful operations will be performed on the nodes to communicate with the hardware and perform various operations. Cloud operation will enhances communication between nodes from different manufacturers and will provide an interoperable communication between them. Now a NetDuino board will not require a custom protocol to communicate with TMote or Berkeley mote as everything is running on the code. Only Firmware and RESTful operations (PUT, DELETE, GET, and POST) will all that be implemented on the node. Application code is shifted to cloud. In-network data processing consume considerable amount of a node resources, these operation will also need to be shifted to a powerful devices in order to ease the burden on these nodes[21].

The Quality of Service (QoS) provisioning in an IoT framework is another challenging issue which needs to be addressed. To provide QoS, two parameters are of high importance: Reliability and Timely delivery of data. Reliability is provided by transmitting CON messages (message type in CoAP) which need to be acknowledged. When a sender transmits a CON message to the server for resource observation (resources such as temperature etc. resides on a server), it waits for an acknowledgement by using Stop-and-Wait retransmission algorithm. In Resource observation, timeliness is maintained by using "Observe" option. This option enables the subscriber/listener to sequence the notification.

In resource observation, an observer registers itself with a resource residing on a server [15]. The subject (server) notify each observer when the state of the resource changes. This reduces the number of transmission flowing in the network which in turn improves the efficiency, reliability, energy consumption, bandwidth utilization and other QoS metrics of the network. Resource observation provides reliability by exchanging CON messages which need to be acknowledged. As far as timeline requirement is concerned, the Observe option helps the observers in sequencing the resources. Though, this option helps the subscribers/observers to check the validity of the notifications. However, it does not guarantee timely delivery of notification (carrying resources) to the observers. This will have severe consequences in real time application where a minor delay in notification will make it useless[22-30].

The presence of diverse range of devices at the core of IoT poses various security threats. Integrating everyday objects into the internet require various communication models. This requirement is likely to add some very ingenious and innovative malicious models [16]. It is of utmost importance that such models should be prevented or at least mitigating options should be in place to tackle their undesirable effects. To develop a secure solution in the internet of things context is much more difficult due to varying and unpredictable nature of objects, many of whom are to be connected for the first time in the internet. It is very important to understand the characteristics and features of things and underlying embedded technologies to combat various malicious models. Existing security and lightweight cryptographic algorithms are to be assessed and adapted in the internet of things environment. However, such profiling of these protocols and algorithms might not necessarily comply with their domain of applications and might results in undesirable outcomes. Any protocol or algorithm has their intended domain of applications and specification. Modification of protocol features might deviate from its original use of intend as many internet-based protocols were not designed for internet of things objects. Recent work can found in [31-41].

Heterogeneity plays a vital role in infrastructure protection. Highly constrained sensor nodes scattered in a battle field require a robust communication channel to communicate with cellular and wireless devices like smartphones. Cryptographic algorithms are required to secure communication between these entities. However, due to battery power nature of these devices, the algorithms need to be computationally simple and fast efficient. AES algorithm might suit a small subset of IoT devices; however, they might not be suitable for extremely constrained RFID tags. Symmetric algorithms are the best options rather than asymmetric algorithms as they are computationally simple and suit these tags etc [22] [42-47]. IoT devices need to use the existing internet standards to communicate with each other. However, all of them are not resource oriented. Hence existing security protocols need to be adapted and modified. In short, the challenges faced by IoT are summarized as follows:

• Sensing a complex environment: Innovative ways to sense and deliver information form the physical world to the cloud

• Connectivity: Variety of wired and wireless connectivity standards are required to enable different applications needs.
• Power is critical: Many IoT applications need to run for years over batteries and reduce the overall energy consumption.
• Security is Vital: Protecting user's privacy and manufacturers IP, detecting and blocking malicious activities.
• IoT is complex: IoT application development needs to be easy for all developers, not just to exports.
• Cloud is important: IoT applications require end-to-end solutions including cloud services.

IV. CONCLUSION

Internet of things incorporates a wide range of devices. The presence of miniature sensor nodes at the core of each device provides seamless and interoperable communication. Although, a wide range of applications exist, however, communication is still at risk in these applications. These networks face various challenges which need to be addressed in order to broaden the scope of IoT. These networks have the potential to enable communication between devices, which were not previously connected with the internet.

REFERENCES

[1] Luigi Atzori, Antonio Iera and Giacomo Morabito *"The internet of things: A survey*." Computer networks 54.15 (2010): 2787-2805.

[2] Khan. F., Bashir, F. (2012). *Dual Head Clustering Scheme in Wireless Sensor Networks*. in the IEEE International Conference on Emerging Technologies (pp. 1-8). Islamabad: IEEE Islamabad.

[3] Syed Roohullah Jan, Khan. F., Zaman. A., (2015) *The Perception of students about Mobile Learning at University Level*. in the khgresearch.org NO. CONTENTS PAGE NOTurkey, pp.97

[4] Usman, Mohammed Joda and Zhang, Xing and Chiroma, Haruna and Abubakar, Adamu and Gital, Abdusalam Ya'u, "*A Framework for Realizing Universal Standardization for Internet of Things*" Journal of Industrial and Intelligent Information, Vol.2, 2014

[5] Khan. F., Nakagawa. K. (2012). *Cooperative Spectrum Sensing Techniques in Cognitive Radio Networks*. in the Institute of Electronics, Information and Communication Engineers (IEICE), Japan, Vol -1, 2.

[6] M. A. Jan, P. Nanda, X. He, Z. Tan and R. P. Liu, "*A robust authentication scheme for observing resources in the internet of things environment*" in 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 205-211, 2014, IEEE.

[7] Khan. F., Nakagawa, K. (2012). *Performance Improvement in Cognitive Radio Sensor Networks*. in the Institute of Electronics, Information and Communication Engineers (IEICE) , 8.

[8] Z.Shelby, K.Hartke, and C. Bormann. "*The constrained application protocol (CoAP)." (2014)*.

[9] M. A. Jan, P. Nanda and X. He, "*Energy Evaluation Model for an Improved Centralized Clustering Hierarchical Algorithm in WSN*," in Wired/Wireless Internet Communication, Lecture Notes in Computer Science, pp. 154–167, Springer, Berlin, Germany, 2013.

[10] Khan. F., Kamal, S. A. (2013). Fairness Improvement in long-chain Multi-hop Wireless Adhoc Networks. International Conference on Connected Vehicles & Expo (pp. 1-8). Las Vegas:

a. IEEE Las Vegas, USA.

[11] M. A. Jan, P. Nanda, X. He and R. P. Liu, "*Enhancing lifetime and quality of data in cluster-based hierarchical routing protocol for wireless sensor network*", 2013 IEEE International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC & EUC), pp. 1400-1407, 2013.

[12] Jabeen. Q., Khan. F., Khan, Shahzad, Jan. M. A., (2016). *Performance Improvement in Multihop Wireless Mobile Adhoc Networks*. in the Journal Applied, Environmental, and Biological Sciences

(JAEBS), Print ISSN: 2090-4274 Online ISSN: 2090-4215

[13] Z.Shelby, and C.Bormann. "*6LoWPAN: The wireless embedded Internet*". Vol. 43, John Wiley & Sons, 2011.

[14] Khan. F., Nakagawa, K. (2013). *Comparative Study of Spectrum Sensing Techniques in Cognitive Radio Networks*. in IEEE World Congress on Communication and Information Technologies (p. 8). Tunisia: IEEE Tunisia.

[15] Khan. F., (2014). *Secure Communication and Routing Architecture in Wireless Sensor Networks*. the 3rd Global Conference on Consumer Electronics (GCCE) (p. 4). Tokyo, Japan: IEEE Tokyo.

[16] M. A. Jan, P. Nanda, X. He and R. P. Liu, "*PASCCC: Priority-based application-specific congestion control clustering protocol*" Computer Networks, Vol. 74, PP-92-102, 2014.

[17] Khan. F., (2014). Fairness and throughput improvement in mobile ad hoc networks. in the 27th Annual Canadian Conference on Electrical and Computer Engineering (p. 6). Toronto, Canada: IEEE Toronto.

[18] Mian Ahmad Jan and Muhammad Khan, "*A Survey of Cluster-based Hierarchical Routing Protocols*", in IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol.3, April. 2013, pp.138-143.

[19] C.Bormann, A. P. Castellani, and Z. Shelby. "*Coap: An application protocol for billions of tiny internet nodes.*" IEEE Internet Computing 2 (2012): 62-67.

[20] Khan. S., Khan. F., (2015). Delay and Throughput Improvement in Wireless Sensor and Actor Networks. 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW) (pp. 1-8). Riyadh: IEEE Riyad Chapter.

[21] Khan. Shahzad, Khan. F., Jabeen. Q., Arif F., Jan. M. A., Khan. S.A (2016). *Performance Improvement in Wireless Sensor and Actor Networks*. in the Journal Applied, Environmental, and Biological Sciences Print ISSN: 2090-4274 Online ISSN: 2090-4215

[22] Mian Ahmad Jan and Muhammad Khan, "*Denial of Service Attacks and Their Countermeasures in WSN*", in IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol.3, April. 2013.

[23] M. A. Jan, P. Nanda, X. He and R. P. Liu, "*A Sybil Attack Detection Scheme for a Centralized Clustering-based Hierarchical Network*" in Trustcom/BigDataSE/ISPA, Vol.1, PP-318-325, 2015, IEEE.

[24] M. Kovatsch, ""Firm firmware and apps for the internet of things", Proceedings of the 2nd Workshop on Software Engineering for Sensor Network Applications, pp. 61-62, ACM, 2011.

[25] Jabeen. Q., Khan. F., Hayat, M.N., Khan, H., Syed Roohullah Jan, Ullah, F., (2016) A Survey : Embedded Systems Supporting By Different Operating Systems in the International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 2 Issue 2, pp.664-673.

[26] Syed Roohullah Jan, Syed Tauhid Ullah Shah, Zia Ullah Johar, Yasin Shah, Khan. F., " An Innovative Approach to Investigate Various Software Testing Techniques and Strategies", International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 2 Issue 2, pp.682-689, March-April 2016. URL : http://ijsrset.com/IJSRSET1622210.php

[27] Khan. F., Khan. F., Jabeen. Q., Jan. S. R., Khan. S., (2016) Applications, Limitations, and Improvements in Visible Light Communication Systems in the VAWKUM Transaction on Computer Science Vol. 9, Iss.2, DOI: http://dx.doi.org/10.21015/vtcs.v9i2.398

[28] Syed Roohullah Jan, Khan. F., Muhammad Tahir, Shahzad Khan., (2016) "Survey: Dealing Non-Functional Requirements At Architecture Level", VFAST Transactions on Software Engineering, (Accepted 2016)

[29] M. A. Jan, "*Energy-efficient routing and secure communication in wireless sensor networks*," Ph.D. dissertation, 2016.

[30] Syed Roohullah Jan, Faheem Dad, Nouman

Amin, Abdul Hameed, Syed Saad Ali Shah, " Issues In Global Software Development (Communication, Coordination and Trust) - A Critical Review", International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 2 Issue 2, pp.660-663, March-April 2016. URL : http://ijsrset.com/IJSRSET1622207.php

[31] Azim. N., Majid. A., Khan. F., Tahir. M., Safdar. M., Jabeen. Q., (2016) Routing of Mobile Hosts in Adhoc Networks. in the International Journal of Emerging Technology in Computer Science and Electronics (in press)

[32] Azim. N., Qureshi. Y., Khan. F., Tahir. M., Syed Roohullah Jan, Majid. A., (2016) Offsite One Way Data Replication towards Improving Data Refresh Performance. in the International Journal of Computer Science and Telecommunications (in press)

[33] Azim. N., Majid. A., Khan. F., Tahir. M., Syed Roohullah Jan, (2016) People Factors in Agile Software Development and Project Management. in the International Journal of Emerging Technology in Computer Science and Electronics (in press)

[34] Azim. N., Khan. A., Khan. F., Syed Roohullah Jan, Tahir. M., Majid. A. (2016) Offsite 2-way Data Replication towards Improving Data Refresh Performance. in the International Journal of Engineering Technology and Applications (in press)

[35] Azim. N., Ahmad. I., Khan. F., Tahir. M., Majid. A., Syed Roohullah Jan, (2016) A New Robust Video Watermarking Technique Using H.264/AAC Codec Luma Components Based On DCT. in the International Journal of Advance Research and Innovative Ideas in Education (in press)

[36] Syed Roohullah Jan, Ullah. F., Khan. F., Azim. N, Tahir. M. (2016) Using CoAP protocol for Resource Observation in IoT. in the International Journal of Engineering Technology and Applications (in press)

[37] Tahir. M., Syed Roohullah Jan, Khan. F., Jabeen. Q., Azim. N., Ullah. F., (2016) EEC: Evaluation of Energy Consumption in Wireless Sensor Networks. in the International Journal of Engineering Technology and Applications (in press)

[38] Tahir. M., Syed Roohullah Jan, Azim. N., Khan. F., Khan. I. A., (2016) Recommender System on Structured Data. in the International Journal of Advance Research and Innovative Ideas in Education (in press)

[39] Tahir. M., Khan. F., Syed Roohullah Jan, Khan. I. A., Azim, N., (2016) Inter-Relationship between Energy Efficient Routing and Secure Communication in WSN. in the International Journal of Emerging Technology in Computer Science and Electronics (in press)

[40] Safdar. M., Khan. I. A., Khan. F., Syed Roohullah Jan, Ullah. F., (2016) Comparative study of routing protocols in Mobile adhoc networks. in the International Journal of Computer Science and Telecommunications (in press)

[41] Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2015, August). *DPBSV--An Efficient and Secure Scheme for Big Sensing Data Stream*. InTrustcom/BigDataSE/ISPA, 2015 IEEE (Vol. 1, pp. 246-253). IEEE.

[42] Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2015). *A Dynamic Key Length Based Approach for Real-Time Security Verification of Big Sensing Data Stream*. In Web Information Systems Engineering–WISE 2015 (pp. 93-108). Springer International Publishing.

[43] M. A. Jan, P. Nanda, X. He and R. P. Liu. 2016. *A Lightweight Mutual Authentication Scheme for IoT Objects*, IEEE Transactions on Dependable and Secure Computing (TDSC), "Submitted".

[44] M. A. Jan, P. Nanda, X. He and R. P. Liu. 2016. *A Sybil Attack Detection Scheme for a Forest Wildfire Monitoring Application*, Elsevier Future Generation Computer Systems (FGCS), "Submitted".

[45] Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2016). *A dynamic prime number based efficient security mechanism for big sensing data streams*. Journal of Computer and System Sciences.

[46] M. A. Jan, P. Nanda, M. Usman and X. He. 2016. *PAWN: A Payload-based mutual Authentication scheme for Wireless Sensor Networks*, in 15th

IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-16), “accepted”.

[47] M. Usman, M. A. Jan and X. He. 2016. *Cryptography-based Secure Data Storage and Sharing Using HEVC and Public Clouds*, Elsevier Information sciences, “accepted”.