© 2018 IJSRSET | Volume 4 | Issue 10 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

IOT in Big Data Challenges and Opportunities

Izaz Khan*[1], Muhammad Awais*[1], Hussain Khan[1], Muhammad Ikram[1], Amir Sohail[1]
*[1]Department of Computer Science Abdul Wali Khan University, Mardan, KPK, Pakistan

ABSTRACT

Internet of Things (IoT), which build a huge network of billions or trillions of "Things" communicating with one another, are facing many practical and application challenges. The relationship between big data and IoT will be explained. We investigate the domain by discussing various opportunities brought about by data in the IoT paradigm, and also challenges & role of big data. The development in the various areas of Wireless Sensors and Internet of things has been sponsoring to generate large volume of data known as Big Data. Many more challenges has a tailback for IOT in big data, this paper reviews the open challenges, roles and prospect of IOT and Big Data.
Keywords : Internet of Things, Big Data.

I. INTRODUCTION

As of now we are living in an era of IOT. IoT is rendering senses to the nonliving things being. Today Internet become a part of our life and touched almost every corner of the globe P. Sethi and S. R. Sarangi [1]. Since massive data have been generated by huge amounts of distributed sensors, how to attain, integrate, store, process and use these data has become a serious and important problem for enterprises to achieve their business goals. As a consequence, both of researchers and engineers are faced a challenge of handling these massive heterogeneous/homogeneous data in highly distributed environments. The collected data from the WSN is used for decision making. The data generated by the millions of sensors produce big data. Big data sources are commonly (Dr.T.Abdul Razak. ,etal. ,August 2014)[8],digitally generated, passively produced, automatically collected and continuously analyzed, Gathering large volume and variety of data are more useful in different types of IOT applications. In smart house applications, variety of sensors are deployed and data generated by the sensors are collected in order to analyze the data for deriving useful information. Big data is described as 3V characteristic namely: Variety, Velocity, Volume, The volume of data generated cannot be handled by the traditional databases. One of the promising approaches to tackle the issues of the big data could be to enable synergies among communications, computing and caching components of future wireless IoT networks [21]. Velocity refers the speed at which the data is generated to meet the demands of the industries and variety means the various formats of the data from the heterogeneous resources. Big data then comes from a variety of sources, in very large amounts, and often in real-time settings. This trend is largely driven by the pervasive diffusion and adoption of mobile devices, social media tools, and the Internet of Things (IoT) enabled by radio frequency identification (RFID, uses electromagnetic fields to automatically identify and track tags attached to objects. The tags contain electronically-stored information.) And other RF-related tracking and sensor devices. There are various definitions of the Internet of Things, but it is generally accepted as defined by the RFID group as "the worldwide network of interconnected objects uniquely addressable based on standard communications protocols" P. Sethi and S. R. Sarangi [1]. Forecasts for the number of connected devices on the Internet of Things for the year 2020 vary considerably, from 26 billion (Gartner) [2], to 30 billion (ABI Research) [3], to 50 billion (Cisco) [4], to 75 billion (Morgan Stanley) [5]. Regardless of which prediction is closest to reality, it is generally believed that an Internet of Things will become ubiquitous in the coming decade which will generate massive amounts of data that must be analyzed in order to generate value for individuals, organizations, entire industries and ultimately society. And the widespread popularity of IoT has made big data analytics challenging because of the processing and collection of data through different sensors in the IoT environment. Moreover, implementing IoT and big data integration solutions can help address issues on storage, processing, data analytics, and visualization tools. It can also assist in improving collaboration and communication among various objects in a smart city [20].Stochastic models are probabilistic models and are usually used to capture the explicit features and dynamics of the data traffic. The commonly used stochastic models are Markov models, time series, geometric models, and Kalman filters. Transport protocol used. Querying, collecting, storing and analyzing of such data brings the challenges for the research community.

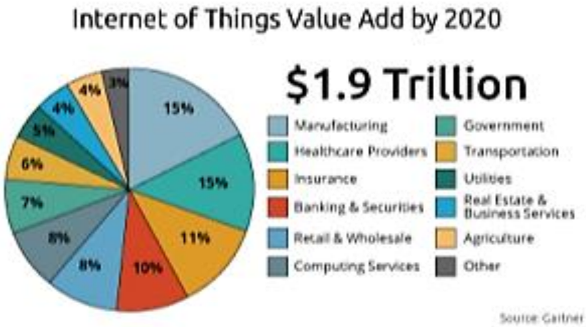
II. Role of Big data in IOT

Big data technologies can offer data storage and processing services in an IoT environment, while data analytics allow business people to make better decisions. IoT applications are the major sources of big data. IoT as the next revolutionary technology by benefiting from the full opportunities offered by the Internet technology. Ciufo [11] stated that these devices "talk" to one another and to central controlling devices. Such devices deployed in different areas may collect various kinds of data, such as geographical, astronomical, environmental, and logistical data. Big data analytics at the cloud center can easily integrate the data collected using distributed sensors and aggregator nodes while exploiting correlation among the data-sets [12]. In terms of computing platforms, edge computing and cloud computing are considered as key solutions for handling big data analytics. The fog/edge computing can be enabled in the existing cloud-based networks by introducing an intermediate layer, called fog/edge layer, which may comprise of several edge servers distributed over various places such as shopping centers, parking areas and bus stations. The edge server can be regarded as a low-capacity version of the cloud server and has communication, computing and data storage capabilities. it is beneficial to offload much of the computational tasks to the cloud. On the other hand, it is advantageous to handle delay-sensitive tasks at the edge-side. Another important aspect which can be exploited in the proposed framework is that cloud processing can utilize the history/delayed information available at the cloud-center in order to infer certain decisions for the edge processing without the need of waiting for the instantaneous data collected from IoT nodes. Due to massive amount of IoT data and continuously increasing number of service requests, power consumption for operating servers in the cloud center is rapidly increasing [23]. Therefore, it is crucial to investigate suitable strategies to reduce energy consumption in the edge-cloud coordinated platform. On the other hand, it is important to guarantee the latency requirements while delivering services to the end users. This section explains the role of big data and analytics in different IoT applications, including smart grids, smart healthcare, smart transportation, and smart inventory systems [17], [18], [19]. Table 1 summarizes the benefits of big data and analytics in IoT applications.

TABLE I : Benefits of Data Analytics for IoT Applications

IoT Application	Benefits of Data Analytics
Smart Transportation	(a) Reduce the number of accidents by looking into the history of the mishaps (b) Minimize traffic congestion (c) Optimize shipment movements (d) Ensure road safety
Smart Healthcare	a) Predict epidemics, cures, and disease (b) Help insurance companies make better policies (c) Pick up the warning signs of any serious illnesses during their early stages
Smart Grid	(a) Help design an optimal pricing plan according to the current power consumption (b) Predict future supply needs (c) Ensure an appropriate level of electricity supply
Smart Inventory System	(a) Detect fraudulent cases (b) Strategically place an advertisement (c) Understand customer needs (d) Identify potential risks

IoT (the Internet of Things) refers to the automated intelligent control and command of connected devices over vast regions via sensors and other computing capabilities. At its core, IoT is a fairly simple concept to grasp. It's all about making out products smarter. IoT is on its path to becoming one the biggest technological revolutions the world has ever seen. By 2021, the amount of revenue generated by IoT technology is expected to be in the figures north of $300 plus billion, and this is just a tip of the iceberg. One of the most critical components of the IoT process is data. For connected devices to perform commands, data has to be sent to a centralized location say gateway or the cloud where it's processed and sent back to the sensors of these devices. It is, therefore, imperative to have an efficient way of collecting small amounts of data and transmitting this data to the centralized location for processing, and sending it back to the sensors all in real-time. Taking into account the type, the enormous explosion in numbers and capabilities of these devices and sensors, the size of the data that needs processing can be extremely large (volume), fast (velocity), and diverse (variety) all characteristics associated with big data. The role of big data on the Internet of Things is tremendous, but the most visible applications will be in analytics, data security, and data storage fronts. Article Author: Mark Palmer [6].



III. Challenges

Architecture Challenge : The basic requirement with respect to architecture is Data centers capable to manage this extra flow of heterogeneous data. IOT covers wide range of devices from smart devices to different types of sensors such as mobile, camera, chemical sensor etc. These devices can be connected using wireless medium or ad-hoc manner. Low latency and location awareness requirements, the emerging IoT platform requires the support for seamless mobility and ubiquitous coverage which cannot be fully supported by cloud computing. Failure of any device leads to the architectural challenge.

Sensing data. Advanced sensors and their hosting devices (e.g. mobile phones, health monitors) are connected in a cyber-physical system to measure time and location of humans, movement of auto mobiles, vibration of machine, temperature, precipitation, humidity and chemical changes in the atmosphere (Lohr 2012). The Internet of Things (IoT, Camarinha-Matos, Tomic, and Graça 2013) captures this new domain and continuously generates data streams across the globe with geographical footprints from interconnected mobile devices, personal computers, sensors, RFID tags and cameras (Michael and Miller 2013; Van den Dam 2013) [9].These Sensor device sense enormous data all time, and deliver information from this physical world of data and then store it. Sensing huge volume of data is very complex task. As the bandwidth of IoT terminals could vary from kbps to mbps from sensing simple value to video stream, requirements on hardware are diverging.

Energy Sustainability: In the future, we use different techniques for scavenging energy to prolong wsn life time. Energy-efficient and self-sustainable systems will be key enhancing issues to the IoT. Big data eat energy due to which most of the power lost. Huge data harvest energy as sensor nodes continuously processing and transferring the data. Efficiency in processing and communication must also be decreased. Energy harvesting will be the key factors for the roll-out of autonomous wireless systems. Charging of global IoT terminals, power consumption of global IoT access points and gateways, as well as the power consumption of IoT data processing in IoT infrastructures will be one of the dominant power consumers in the future world.

Self-Organization: Mobile IoT users frequently collect and broadcast packet bundles within communication range of each other. The cloud intervenes only when computations of high complexity need to be delegated from resource-constrained IoT devices, but does not frequently participate in the distributed content bundle generation and authentication.

Cost: According to IDC, spending on the internet of things was at $737 billion in 2016 and forecasted to grow at an annual rate of 15.6%, reaching $1.29 trillion in 2020.IOT and big data both are costly. Alot of effort required. Deployment of IoT and processing of big data using sensor node is a challenging task. Since a considerable measure of unstructured data may require differing limit and get to frameworks, there will be a lot of cost involved in the same. By using on the web Big Data application, an extensive measure of associations can significantly diminish their IT cost. Cost of the node implementation, energy consumed, development involved and deployment of the same would be a difficult task.

Data analysis: Data analysis is a larger-scale challenge, too. For example, the goal of a wearable device could be to alert medical staff to anomalies in vital signs. In that case, waiting for a centralized batch process to run across a large data center to find irregularities is extremely inefficient. An alternative design is to place anomaly detection closer to the network's edge. Cisco's big data architecture includes the concept of a fog node, which sits on the edge of a network or cloud provider's point of presence. The term fog is a hat tip to the concept of the cloud. The node connects to a network entry point either at the customer's site or within Cisco's Jasper cloud network. The proximity of the fog node to the data allows fast data analysis. The node detects anomalies and acts upon them as information is collected, and optimizes the data set before it uploads to a central database. Due to ever-increasing demand for data content, the transmission of massive amount of data to the cloud creates a huge burden on the communication bandwidth of wireless networks. Furthermore, this results in intolerable latency and degraded service to the end-users. Storage challenges are posed by the volume, velocity and variety of big data.

Management: Since the nodes are autonomous and deployed in human unattended places, self-configuration is required in the integration. It includes the construction of routing, allocation of addresses, identifying the faulty nodes and configuring themselves. Internet is not supporting and hence these needs to be addressed efficiently. Enormous amount of data are generated from heterogeneous sources. These streams of data may be in different ways for different purposes. The generated data can be categorized as structured and unstructured data. Amount of data collected will be enormous. Recent stats tell that every minute, 300 million emails are sent, 3.8 million Facebook likes are generated, send's thousand's tweets, and many images are uploaded to Facebook. By 2020, it's estimated this number will increase billion's so to manage this big data center's would be involved and so expectedly real time sensor's would be required .The collected data is required to store, analyze and process in an efficient manner. The data needs to be integrated. Data needs to be preprocessed before storing into the storage mechanism. Since the data is real time, continuous one, communication is resource intensive. Key problems in management of data includes storing, analyzing, data dissemination and filtering. We need advanced applications for the aggregation and filtering. Another challenge in big data is efficient representation of structured and unstructured data. Quality of Service: Since the sensor nods are energy constraint devices, resource utilization of heterogeneous devices becomes part of the QOS. Sensor networks need to be supplied with the required amount of bandwidth so that it is able to achieve a minimal required QoS. In WSN, sudden changes in the topology leads to the reconfiguration and introduces delay. Novel approaches should be designed to ensure the Quality of Service for the convergence.

Privacy and Security Challenge: Compared with traditional networks, security and privacy issues of IoT become more prominent [22]. Much information includes privacy of users, so that protection of privacy becomes an important security issues in IoT. Because of the combinations of things, services, and networks, security of IoT needs to cover more management objects and levels than traditional network security, and how to provide secured connections to the massive number of heterogeneous IoT devices having different levels of processing capabilities. Privacy issues arise when a system is compromised to inferior restore personal information using big data analytic stools, although data are generated from anonymous users. Existing security architecture is designed from the perspective of human communication, may not be suitable and directly applied to IoT system. Using existed security mechanisms will block logical relationship between things in IoT. IoT needs low-cost- and M2M-oriented technical solutions to guarantee the privacy and the security. In many use cases, the security of a system has been considered as a general feature. Related research shall focus on privacy control. Low cost, low latency, and energy-efficient cryptography algorithms and related flexible hardware will be essential for sensor or device. With regard to data generated through IoT, the following security problems can emerge. (a) timely updates - difficulty in keeping systems up to date, (b) incident management - identifying suspicious traffic patterns among legitimate ones and possible failure to capture unidentifiable incidents, (c) interoperability - proprietary and vendor specific procedures will pose difficulties in finding hidden or zero day attacks, (d) and protocol convergence - although IPv6 is currently compatible with the latest specifications, this protocol has yet to be fully deployed. Therefore, the application of security rules over IPv4 may not be applicable to protecting IPv6.To protect the IoT generated data, some new security and privacy mechanisms are required. Current security technologies are based on static datasets, while data is changing dynamically. Traditional security and privacy technologies do not completely consider some important characteristics of a large amount of data generated by IoT, such as data pattern and variation of data. Thus, it has become a challenging task to design and implement new privacy and security mechanisms in this complex circumstance.

IV. Related Work

In order to handle massive unstructured datasets, NoSQL databases and distributed file systems have been suggested. Map Reduce have been proposed in order to handle group aggregation tasks like website ranking. Moreover, in terms of system-level solution, open-source software frameworks like Hadoop have been proposed to integrate data storage, data processing and other modules. Another important aspect which can be exploited in the proposed framework is that cloud processing can utilize the history/delayed information available at the cloud-center in order to infer certain decisions for the edge processing without the need of waiting for the instantaneous data collected from IoT nodes.

Atzori, et al. [7] provide a useful starting point for thinking about behavioral, organizational and business issues related to adoption, and challenges of the Internet of Things. They point out that the IoT is a confluence of a number of different fields merging together to create the promise of connected smart devices that will impact many areas of our daily lives and impact peoples' behavior as a result. Due to the complex synergy of various fields they note different paradigmatic views where each represents a different vision of the Internet of Things. A "Things oriented" perspective views the IoT as a network of identifiable objects. This view has grown out of the considerable work done on RFID technology over the past two decades [13,14]. More tagged and sensing devices will be connected to the Internet of Things providing unprecedented visibility into processes and remote environments. Moving beyond an RFID-enable view is a much more advanced "Internet oriented" vision of the Internet of Things which is best summarized as a "world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participates in business processes. Services are available to interact with these 'smart objects' over the Internet, query and change their state and any information associated with them, taking into account security and privacy issues". This vision incorporates machine-to-machine communication over a public infrastructure between smart devices that have the ability to alter internal and external states. The third perspective is a "Semantic oriented" Internet of Things which assumes that with a very large number of devices connecting to the IoT it will be necessary to exploit big data analytics and machine learning tools to make sense of all the data. With this background Atzori, et al. [7] then highlight enabling technologies for these visions and note that standards development, addressing schemes, security and privacy are technical issues that need to be addressed. Gubbi et al. [10] seizes upon the Internet-centric paradigm discussed above to build a framework where cloud-based software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS) capabilities enable the various smart devices connected to the Internet of Things. With smart devices in a bottom layer (hardware) connected to various applications sitting in a top layer (software), the cloud-enabled middle layer (services) uses SaaS, PaaS and IaaS as an interface to deliver functional value. Again the emphasis is on solving the technical problems related to developing the IoT with little thought to the issues of incentives to adopt, sharing of value across network users, and measurement of ultimate impact. Shakiba et al., [14] observes that in the last decade of RFID research, the vast majority of work on RF and sensor technologies has been addressing the important technical issues and not the behavioral, organizational or business issues

V. Opportunity of IoT in Big Data

The 'internet of things' (IoT) and 'big data' are two of the most-talked-about technology topics in recent years, which is why they occupy places at or near the peak of analyst firm Gartner's most recent Hype Cycle for Emerging Technologies. The IoT is a fast-growing constellation of internet-connected sensors attached to a wide variety of 'things'. Sensors can take a multitude of possible measurements, internet connections can be wired or wireless, while 'things' can literally be any object (living or inanimate) to which you can attach or embed a sensor. If you carry a smartphone, for example, you become a multi-sensor IoT 'thing', and many of your day-to-day activities can be tracked, analyzed and acted upon. Big Data & IoT are like brothers. They ca not do anything without each other. These fields are related to each other. IOT will bring lots of data and that will need to be processed, analyzed to derive insights using Big Data's capacity only and that will again flow back to the devices to the users finally. The IoT will create a huge network of billions or trillions of "Things" communicating each other. The IoT is not subversive revolution over the existing technologies, it is comprehensive utilizations of existing technologies, and it is the creation of the new communication modes. The biggest idea for future is that should benefit the world, creating knowledge from such huge amount of heterogeneous data. This will also be bought in new lifestyle from today then we can see in future with such advancement in technology .Decades before we never knew anything about social media, millions of apps for smartphones, etc. but now we are already aware of what advancement it has bought to the new world . Mobile data and the IoT, which are generating large amounts of data, would benefit from the adoption of a big data infrastructure able to store and process information in current IoT infrastructures. As for geography data, a major trend seems to be to offer efficient integration among geographic data with records from the domain. The IoT blends the virtual world and the physical world by bringing different concepts and technical components together: pervasive networks, miniaturization of devices, mobile communication, and new ecosystem. The IoT implies a symbiotic interaction between the real/physical and the digital/virtual worlds: physical entities have digital counterparts and virtual representation; things become context aware and they can sense, communicate, interact, and exchange data, information, and knowledge. New opportunities will meet business requirements, and new services will be created based on real-time physical world data. Everything from the physical or virtual world will possibly be connected by the IoT. Connectivity between the things shall be available to all with low cost and may not be owned by private entities. For IoT, intelligent learning, fast deployment, best information understanding and interpreting, against fraud and malicious attack, and privacy protection are essential requirements. For IoT we need lot of of to train the model for that we need a place where we can store all the data, and such kind of data is known as big data. On another side there is no use of big data if we cannot utilize is anywhere. [16]. Pranjal Saxena, Passionate Machine Learner.

The growth of Internet of Things (IoT) is rapidly increasing the amount of data generated, and industry experts warn that the current river of unstructured data will soon turn into a flood. Alarmingly, a recent study highlighted concerns that most proposed data. Gartner [15] cautions that IoT specialists who are tasked with IoT strategies and managing data governance, "are not prepared for the information-related implications of the Internet of Things. The IoT will challenge their capabilities, skills, processes and tools with complexity and scale, as well as new governance implications," said Gartner which predicted information management must become a core competency in the future.

Capabilities to handle data management overload are key

Gartner identified a key IoT requirement in the future will be data management capabilities. Specifically, it highlights the need for an ability to manage distributed data architectures that execute governance processes while simultaneously supporting analytics. With its expectation that 25% of IoT implementations will be abandoned in the early stages, the report recommends using an "information capabilities framework" as a template for enterprises struggling with the surge in data. This approach begins by assessing the information value through metadata analysis, and then data governance rules are applied. After this, the data can be sifted and integrated into the larger enterprise system. A major challenge for IoT data manages will be reconsidering organizational storage capacity, and analyzing the conditions that users will access the IoT data. The flood of unstructured IoT information will soon overwhelm existing data storage capacity and that existing storage can only be expanded so much.

"A limited ability to cost-effectively scale existing storage approaches will create a bottleneck," said Gartner.

A major data management rethink is needed

IT managers to rethink the traditional centralized data collection approach, due to the highly dispersed nature of IoT data generation and consumption. "With the highly distributed architectures required for most IoT solutions (many things, many places where data is generated, many platforms on which data is processed, and many consumption points to which data must be delivered), the historical approach to centralized collection of data is under pressure. Organizations must support a more distributed data architecture, because IoT solutions are inherently distributed.

VI. CONCLUSION

IoT is one of the biggest sources of big data, IoT interacts with big data when voluminous amounts of data are needed to be processed, transformed, and analyzed in high frequency [16-32]. With the emerging concept of "computing everywhere and anywhere", Internet of things applications are rapidly increasing nowadays. Wireless sensors are providing back-end services for detecting the context and collecting the data from IOT objects. As the numbers are increasing, a massive amount of data has been generating from these sources. There are many problems result in the integration of IOT and WSN and handling large volume of data. In this paper, various applications of IOT and the integration of IOT in Big data challenges are also discussed. Various challenges pertaining to the collection of Big Data generated by wireless sensor networks are also studied. Finally, we concluded that existing big IoT in big data opportunity remained in their early stages of development. In the future, real-time analytics solution that can provide quick insights will be required. It is hoped that there will be new technologies new researches. We hope that with the help of research communities it will solve the throng of problem fast.

VII. REFERENCES

[1]. Khan, F., ur Rehman, A., Usman, M., Tan, Z., & Puthal, D. (2018). Performance of Cognitive Radio Sensor Networks Using Hybrid Automatic Repeat ReQuest: Stop-and-Wait. Mobile Networks and

Applications, 1-10. https://doi.org/10.1007/s11036-018-1020-4

[2]. Alam, M., Trapps, P., Mumtaz, S., & Rodriguez, J. (2016). Context-aware cooperative testbed for energy analysis in beyond 4G networks. Telecommunication Systems. doi:10.1007/s11235-016-0171-5

[3]. Khan, F., Rahman, F., Khan, S., & Kamal, S. A. (2018). Performance Analysis of Transport Protocols for Multimedia Traffic over Mobile Wi-Max Network Under Nakagami Fading. In Information Technology-New Generations (pp. 101-110). Springer, Cham.

[4]. Alam, M., Albano, M., Radwan, A., & Rodriguez, J. (2013). CANDi: context-aware node discovery for short-range cooperation. Transactions on Emerging Telecommunications Technologies, 26(5), 861–875. doi:10.1002/ett.2763

[5]. Khan, F., & Nakagawa, K. (2013). Comparative study of spectrum sensing techniques in cognitive radio networks. In Computer and Information Technology (WCCIT), 2013 World Congress on (pp. 1-8). IEEE.

[6]. Alam, M., Mumtaz, S., Saghezchi, F. B., Radwan, A., Rodriguez, J. (2013). Energy and Throughput Analysis of Reservation Protocols of Wi Media MAC. Journal of Green Engineering, 3(4), 363–382. doi:10.13052/jge1904-4720.341

[7]. Alam, M., Yang, D., Huq, K., Saghezchi, F., Mumtaz, S., & Rodriguez, J. (2015). Towards 5G: Context Aware Resource Allocation for Energy Saving. Journal of Signal Processing Systems, 83(2), 279–291. doi:10.1007/s11265-015-1061

[8]. Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2014). PASCCC: Priority-based application-specific congestion control clustering protocol. Computer Networks, 74, 92-102.

[9]. Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2015, August). A sybil attack detection scheme for a centralized clustering-based hierarchical network. In Trustcom/BigDataSE/ISPA, 2015 IEEE (Vol. 1, pp. 318-325). IEEE.

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

[11]. Jan, M., Nanda, P., Usman, M., & He, X. (2017). PAWN: a payload-based mutual authentication scheme for wireless sensor networks. Concurrency and Computation: Practice and Experience, 29(17).

[12]. Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2013, November). Enhancing lifetime and quality of data in cluster-based hierarchical routing protocol for wireless sensor network. In High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC_EUC), 2013 IEEE 10th International Conference on (pp. 1400-1407). IEEE.

[13]. Khan, F. (2014, May). Fairness and throughput improvement in multihop wireless ad hoc networks. In Electrical and Computer Engineering (CCECE), 2014 IEEE 27th Canadian Conference on (pp. 1-6). IEEE.

[14]. Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2018). A Sybil attack detection scheme for a forest wildfire monitoring application. Future Generation Computer Systems, 80, 613-626

[15]. Jan, M. A., Nanda, P., & He, X. (2013, June). Energy evaluation model for an improved centralized clustering hierarchical algorithm in WSN. In International Conference on Wired/Wireless Internet Communication (pp. 154-167). Springer, Berlin, Heidelberg.

[16]. Usman, M., Jan, M. A., & He, X. (2017). Cryptography-based secure data storage and sharing using HEVC and public clouds. Information Sciences, 387, 90-102.

[17]. Usman, M., Jan, M. A., He, X., & Nanda, P. (2016, August). Data sharing in secure multimedia wireless sensor networks. In Trustcom/BigDataSE/I SPA, 2016 IEEE (pp.

590-597). IEEE

[18]. Khan, F., Khan, M., Iqbal, Z., ur Rahman, I., & Alam, M. (2016, September). Secure and Safe Surveillance System Using Sensors Networks-Internet of Things. In International Conference on Future Intelligent Vehicular Technologies (pp. 167-174). Springer, Cham.

[19]. Usman, M., Yang, N., Jan, M. A., He, X., Xu, M., & Lam, K. M. (2018). A joint framework for QoS and QoE for video transmission over wireless multimedia sensor networks. IEEE Transactions on Mobile Computing, 17(4), 746-759.

[20]. Khan, F., ur Rahman, I., Khan, M., Iqbal, N., & Alam, M. (2016, September). CoAP-Based Request-Response Interaction Model for the Internet of Things. In International Conference on Future Intelligent Vehicular Technologies (pp. 146-156). Springer, Cham.

[21]. Fida, N., Khan, F., Jan, M. A., & Khan, Z. (2016, September). Performance Analysis of Vehicular Adhoc Network Using Different Highway Traffic Scenarios in Cloud Computing. In International Conference on Future Intelligent Vehicular Technologies (pp. 157-166). Springer, Cham.

[22]. Jan, M. A., Khan, F., Alam, M., & Usman, M. (2017). A payload-based mutual authentication scheme for Internet of Things. Future Generation Computer Systems.

[23]. Usman, M., He, X., Lam, K. K., Xu, M., Chen, J., Bokhari, S. M. M., & Jan, M. A. (2017). Error Concealment for Cloud-based and Scalable Video Coding of HD Videos. IEEE Transactions on Cloud Computing.

[24]. Yang, N., Usman, M., He, X., Jan, M. A., & Zhang, L. (2017). Time-Frequency Filter Bank: A Simple Approach for Audio and Music Separation. IEEE Access, 5, 27114-27125.

[25]. Usman, M., Jan, M. A., He, X., & Alam, M. (2018). Performance evaluation of High Definition video streaming over Mobile Ad Hoc Networks. Signal Processing, 148, 303-313.

[26]. Jabeen, Q., Khan, F., Hayat, M. N., Khan, H., Jan, S. R., & Ullah, F. (2016). A Survey: Embedded Systems Supporting By Different Operating Systems. International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Print ISSN, 2395-1990.

[27]. Usman, M., Jan, M. A., He, X., & Nanda, P. (2018). QASEC: A secured data communication scheme for mobile Ad-hoc networks. Future Generation Computer Systems.

[28]. Jan, M. A., Tan, Z., He, X., & Ni, W. (2018). Moving Towards Highly Reliable and Effective Sensor Networks.

[29]. Jan, M. A., Jan, S. R. U., Alam, M., Akhunzada, A., & Rahman, I. U. (2018). A Comprehensive Analysis of Congestion Control Protocols in Wireless Sensor Networks. Mobile Networks and Applications, 1-13.

[30]. Alam, M., Ferreira, J., Mumtaz, S., Jan, M. A., Rebelo, R., & Fonseca, J. A. (2017). Smart Cameras Are Making Our Beaches Safer: A 5G-Envisioned Distributed Architecture for Safe, Connected Coastal Areas. IEEE Vehicular Technology Magazine, 12(4), 50-59.

[31]. Jan, M.A., Usman, M., He, X., &, Rehman, A.U. (2018). SAMS: A Seamless and Authorized Multimedia Streaming framework for WMSN-based IoMT. IEEE Internet of Things Journal, doi: 10.1109/JIOT.2018.2848284

[32]. M. A. Jan, S. R. Jan, M. Usman, M. Alam. (2018), State-of-the-Art Congestion Control Protocols in WSN: A Survey, IoT EAI, DOI: 10.4108/eai.26-3-2018.154379