A Survey of Security Issues in Internet of Things

Pooja Sharma[1], Shankar Sharan Tripathi[2], Radheshyam Panda[3]

[1, 2]*Department of Computer Science & Engineering, Shri Shankaracharya Engineering College, Bhilai, (C.G.)*

***Abstract* :-** Nowadays, internet of things (IoT) has been the main focus to advance research fields. Security, reliability, authenticity, and privacy are the major issues for the internet of things. The challenges are to avoid the development of such models to ease and bound their impact In order to make possible this emerging field. In the Internet of Things, we use centralized architectures for services, in which central database provide all information and according to that information, centralized system proceed further. In other words, we can say that in IOT all the nodes are collaborating in dynamically in the network for exchanging their information. Alternatively, centralized distributed architectures, where entities at the edge of the network exchange information and collaborate with each other in a dynamic way, can also be used. In this paper, we discuss the research status of security and privacy of IOT and various challenges also.

Keywords: - Internet of things, Security, Privacy, Trust, Web.

I. INTRODUCTION

Nowadays, internet is widely being used by people across the globe as a part of their daily lives. The internet is being used for all purposes ranging from web browsing and emails, to online entertainment consisting of online music, videos, games and many more such applications. Internet of things helps diminish the boundaries between real and virtual worlds, and is as such one of the many wonders brought forth by the internet. Not only does this enable locating and addressing people, but also real things through internet. Another major emerging trend of IoT application is the industries, which is enabled by the global network of people and things.

Internet of things can be described as a network of everything right from real people to the everything that is a part of the real world. IoT is based upon a centralized architecture that uses a centralized database to provide information, and the system processes the data to proceed accordingly to provide the desired results.

How IoT works is by dynamically collaborating the nodes in a network for data exchange. An alternate system consists of centralized distributed architectures where entities at the edge of the network exchange information and collaborate with each other dynamically.

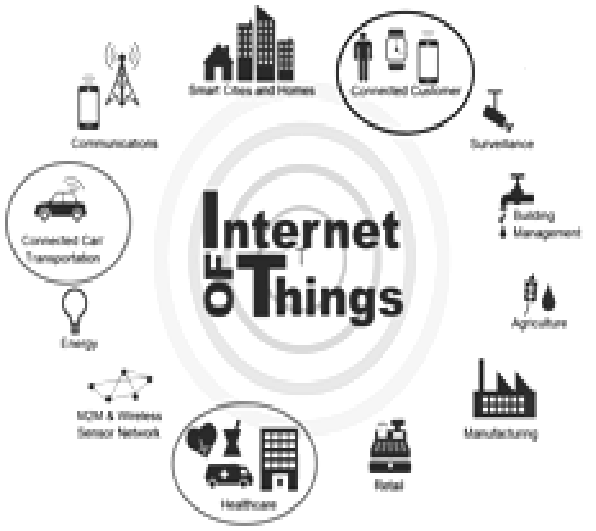

Figure 1: Internet of Things.

II. APPLICATIONS & USES OF IOT

1. **Home security and smart domestic**
   Use of RFID, sensors, smart tech and nanotech for better security, detecting changes in physical status of domestic things through network and connectivity.
2. **Personal healthcare, healthcare carriers and healthcare payers**
   Remote monitoring of patients through M2M based IoT systems which provides connectivity by the use of personal healthcare devices.
3. **Poster boards into IoT enabled boards**
   Use of IoT for enabling better functionality in standard poster boards.
4. **Interactive gaining of knowledge**
   IoT enables better global connectivity to provide better access to information from across the globe.
5. **Attendance Monitoring System**
   Utilization of technologies such as RFID for monitoring attendance at educational and corporate organizations.
6. **National Defense**
   Integration of sensor systems, actuators and control systems to make the existing military infrastructure more effective and efficient.
7. **Smart Cities**
   Use of IoT for better traffic management, pollution control, better usage of infrastructure,

and providing better safety and security for citizens.

8. **Quick response to Emergencies**
   Reducing response times for emergency responders by using of IoT for emergency hotlines, better traffic management, location tracking etc.
9. **Responding Production Flow Monitoring**
   Use of IoT sensors for monitoring production processes, and even initiating new orders, mitigate machine damage in production etc.
10. **Inventory Management**
    Use of IoT technologies to enable use of digital shelves, real time inventory management by using RFID, and Robo Carts guided by sensors and cameras.
11. **Plant Safety and Security**
    Monitoring of employees through wearables to measure various health parameters, monitoring of industrial equipment to analyze unsafe practices and contain them.
12. **Quality Control**
    Monitoring operational parameters of equipment such as temperature, pressure, speed etc. in real time to identify when these parameters trend beyond the prescribed value that can result in substandard production.
13. **Logistics and Supply Chain Optimization**
    Monitoring supply chain, tracking of vehicles, real time inventory management and automation of processes to increase accuracy and efficiency.
14. **Medical Information Distribution**
    Distribution of accurate real time medical information to patients and medical professionals to facilitate better medical treatment and improve daily life.
15. **Precision Farming**
    Generate data by the use of sensors to enable monitoring of livestock and storage, field observation, tracking of farm vehicles etc.
16. **Agriculture Drones**
    Use of IoT to develop automated farming by the use of technologies such as agricultural drones that can help in crop spraying, crop health assessment, screening and planting crops, soil analyses etc.
17. **Smart Greenhouses**
    Developing greenhouses that can work with minimum human interference by using technologies such as automated drip irrigation that can work by measuring soil moisture levels, provision for automated growing lights that work by measuring available natural light etc.
18. **Commercial Energy**
    Minimizing use of energy through addressing all consumption points for cost saving and output optimization.
19. **Residential Energy**
    Analysis and optimization of domestic energy consumption through monitoring energy requirements through the entire household as well as at the device level, and delivering functionalities such as automated switch off of devices, diming of lights when natural light is available, etc.
20. **Waste Management**
    Enabling a system of tracking and better waste collection systems to help manage large amounts of waste in a much more efficient way with the help of technologies such as smart waste bins that can collect and transfer data.
21. **Vehicle Tracking**
    Tracking of vehicle location as well as various parameters such as speed, fuel efficiency, performance etc. through sensors and real time transmission of this data through a network to enable real time tracking of vehicles used for personal, industrial, security or emergency purposes.
22. **Rails & Mass Transit**
    Enabling M2M communication between trains facilitates efficient utilization of equipment, tracks and stations and also reduces safety risks while providing better convenience for passengers by maintaining better operational efficiency of trains.
23. **Industrial Transportation**
    Use of IoT to track movement of industrial resources and providing better safety, cost effectiveness, and reducing transport time by collecting and analyzing data from transport vehicles by use of sensors.
24. **Sound Detection**
    Use of sensors to detect and identify sounds and their origin to be used for applications such as drone detection, gunshot identification, seismic detection etc.
25. **Environment and Conditioning**

III. IOT SECURITY CHALLENGES

1. Ensure data privacy and integrity
2. Manage device updates
3. Ensure high availability
4. Authorize and authenticate devices
5. Secure constrained devices
6. Secure communication
7. Secure web, mobile, and cloud applications

IV. RELATED WORK

In 2002, the work done by Hongmei Deng, Wei Li , and Dharma P. Agrawal shows Routing security in Wireless Ad Hoc Networks consisting of a collection of wireless mobile nodes, where nodes have the capability of communicating with each other without using network infrastructure, or any centralized administration. One

such emerging research area with practical applications is MANET, or Mobile Ad Hoc Network. Wireless MANET, however, has a certain vulnerability given its fundamental characteristics, consisting of Dynamic Topology, open medium, distributed cooperation, and constrained capability. A major part is played by Routing for securing the network. Routing security remains a problem area in wireless MANETs. The article explores the routing security issues of MANETs. One particular type of attack that the article deals with is the "black hole" problem. Such problems can be easily employed against MANETs. The article also explores the solution for this problem for ad hoc on-demand distance vector protocol.

In 2005, Martin Haenggi and Daniele Puccuneli conducted a study on Wireless Sensor Networks: Applications and Challenges of Ubiquitous Sensing. Here, Sensor networks are used for a powerful combination of distributed sensing, computing and communication. But they offer numerous challenges rising from the peculiarities, such as sensing nodes are subjected to stringent energy constraints. The sensor networks, due to their distinguished traits, have an impact on the hardware design of the nodes at four different levels: the power source, processor, communication hardware, and the sensors. Hardware platforms have been designed to test and implement applications to all fields science. CAS has been found to be able to contribute substantially to the development of this field.

In 2006, Vincent W. S. Wong and Ye Ming Lu, published the study about multipath routing for wireless sensors that was energy efficient. Here, energy consumption is a key design criterion for the routing protocols. Conventional single path routing may not always be optimal to maximize the network connectivity and lifetime. The study suggested a distributed, scalable and localized multipath search protocol that discovered multiple node-disjoint paths between the sink and source nodes. The proposal consisted of a load balancing algorithm that distributed the traffic over the multiple paths discovered. The proposed scheme showed a higher node energy efficiency, lower average delay and control overhead.

In 2008 Bojan M. Bakmaz, Zoran S. Bojkovic, and Miodrag R. Bakmaz dealt with security issues over wireless sensor (WSNs) in their study. The study presents a survey dealing with recent trends in general security requirements, intrusion detection system, typical security threats, target localization and key distribution schemes. Provisioning security in group communications stands out as a critical goal to facilitate applications that require packet delivery from senders to multiple receivers. Issues presented play a crucial role in the implementation of WSN.

In 2009, Lenoid Smalov, Fadi Hamad, and Anne James published their work "Energy-aware security in M-Commerce and the Internet of Things". The study presents data privacy and security as major concerns for M-commerce and Internet of Things. Encryption is one of the security measures that can be implemented to protect confidentiality, integrity and availability. But limitations in processing power, communication bandwidth, battery life and memory act as constrain the application of existing cryptography standards for mobile devices. The study presents an experiment that investigates the power and resource consumption computational requirements in reference to the power and resource consumption for the existing cryptographic algorithms. Users can decide on the usage of security schemes based on the given reliable information on power consumption.

In 2010, Pablo Najera, Rodrigo Roman, Javier Lopez and Cristina Alcaraz published their work titled "Wireless Sensor Networks and the Internet of Things: Do they need a complete Integration?". The study showed WSNs behaving as a digital skin, which provides a virtual layer allowing access to information about the physical world to any computational system. They proved invaluable for realizing the vision of IoT. However, it raises the question whether the devices of WSNs need to be completely into the internet. The paper tackles the question from security perspective. Various security challenges are presented, but the focus remains on issues taking place at the network level.

In 2010, Rolf H. Weber, published "Internet of Things – New Security and Privacy Challenges", presenting how the security and privacy of the stakeholders is impacted by internet based technical architecture facilitating the exchange of services and goods in global supply chain networks. The study states the significance of measures to ensure the architecture's resilience against attacks, access control and client privacy. A legal framework needs to be established, preferably by an international legislator, taking into account the underlying technology, and supplemented by private sector to be easily adjustable for their specific needs. The legislation must encompass the right to information, rules to regulate IT-security, provisions to restrict as well as supporting the use of mechanisms of IoT, and provision of a task force to investigate the legal challenges of IoT.

In 2011, Oscar Garcia-Morchon, Tobias Heer, Sve Loong Keoh, René Hummen, Klaus Wehrle and Sandeep S. Kumar presented "Security challenges in the IP-based Internet of Things". They use the term Internet of Things as a reference to using Internet Protocols for human – to –thing or thing – to – thing communications in embedded networks. Although the security needs in this domain are well recognized, there is still uncertainty regarding deploying of existing architectures and IP security protocols. The paper discussed the limitations and applicability of internet protocols and security

architectures with reference to IoT. They present an overview of the deployment model, the security needs. The paper then goes on to discuss specific limitations of standard IP security protocols.

In 2011, Jaydip Sen and Debasis Bandopadhyay presented their work titled "Internet of Things: Applications and Challenges in Technology and Standardization". The paper presents a future where the Internet can be used to connect physical things, like bicycles or banknotes, through a network allowing exchange of information about themselves and the surroundings. This will increase the productivity and efficiency of innovative services by granting them immediate access to information about the physical world. The paper covers state-of-the-art IoT developments, and simultaneously presents the challenges and scope as well as the issues of future research in the IoT domain. The different definitions of IoT from different perspectives of academic and industrial communities are compared.

In 2012, Jiafu Wan, Hui Suo, Jiangi Liu and Caifeng Zou presented "Security in the Internet of Things: A review". A lot of research has been done on IoT in the last decade. Security and privacy issues remain to be the major challenge in this area. The paper discussed in brief the progress of research on IoT from the perspective of security. The authors review the security architectures and features, and present the security requirements in IoT. The status of research in key areas of security such as encryption, protection of sensor data, communication security and algorithms of cryptography are discussed and the challenges in these areas are outlined.

In 2012, Yoshiaki Hori and Na Ruan presented "DoS attack-tolerant TESLA-based broadcast authentication protocol in Internet of Things". Their work views IoT as an emerging concept where networked objects are interconnected via wireless sensors. TESLA works as a source authentication protocol for broadcast network. But it has limited scalability owing to its unicast based initial parameter distribution. µTESLA is a version of TESLA that consumes lower energy. It is designed specifically for WSNs. It, however, fails to tolerate DoS attacks. A DoS tolerant version of TESLA is TESLA++. But since it has a higher power consumption, TESLA++ only works for VANET and not WSN. The authors present a TESLA based protocol against DoS attack, which consumes lower power, to secure the hybrid vehicle sensor network against DoS attacks. Analysis suggests that this protocol proves to be more efficient than µTESLA or TESLA++ in securing networks.

In 2012, Hong Liu and Huansheng Ning presented the work titled "Cyber-Physical-Social Based Security Architecture for Future of Internet of Things". They present U2IoT (Unit IoT and Ubiquitous IoT) model as the future of IoT. Their work presents a cyber-physical-social based security architecture (IPM). The architecture deals with Physical, Information as well as management security perspectives demonstrating that architectural abstraction support the U2IoT model. The authors establish an information security model that describes mapping relations among U2IoT, security layer and security requirements, while also infusing additional intelligence and social layer into IPM. Artificial immune algorithms are used to inspire physical security that refers to the external context and inherent infrastructure. They also suggest recommended security strategies for social management control. The authors present a constructive proposal for the future of IoT security by bringing together the physical world, the cyber world, and the human society.

In 2013, Hanno Wirtz, Rene Hummen, Klaus Wehrle, Jan Henrik and Jens Hiller presented "Tailoring End-to-End IP Security Protocols to the Internet of Things", where they presented end to end IP security protocols. Recent efforts generally have focused on lightweight IP security protocols providing end-to-end security for IoT. A few such protocols are HIP DEX, DTLS and minimal IKEv2. The general consideration for these protocol designs is the public-key-based cryptographic primitives for key arrangement and peer authentication. The authors of this paper identify and discuss the performance and security issues originating from public-key-based operations on IoT devices that are resource constrained. The authors quantify these protocol limitations for HIP DEX, and illustrate the impact of these issues. A key finding here is the hampering of a peer's availability and response time by public-key-based operations during the protocol handshake. Hence, to protect the resource constrained peers against DoS attacks that target cryptograpgic operations, and to account for high message processing times, the IP security protocols must be tailored such that it reduces the need for expensive cryptographic operations. To facilitate this, the authors present three complementary protocol extensions for HIP DEX- i) a comprehensive session resumption mechanism, ii) a puzzle based collaborative mechanism for DoS protection, and iii) a refined retransmission mechanism. The proposed extensions can be generalized to wider scope of DTLS and IKE owing to the focus on common protocol functionality. Evaluations have confirmed considerable improvements at modest trade-offs.

In 2013, Jianying Zhou, Javier Lopez and Rodrigo Roman presented their work titled "On the Features and Challenges of Security and Privacy in Distributed Internet of Things". They proposed the provisioning of services using centralized architectures inn IoT. The central entities can acquire, process and provide information. They also proposed an alternative of distributed architecture, where entities at the edge of the network exhibit information exchange and dynamic collaboration. The viability of such distributed approach can only be understood by knowing its advantages and

disadvantages, in terms of features as well as in terms of security and privacy. The authors present in their paper the various challenges faced with the distributed approach that need to be worked on, while also elaborating the various interesting propertied and strengths of such approach.

In 2014, Athanasios V. Vasilakos, Qi Jing, Dechao Qiu and Jiafu Wan presented "Security of the Internet of Things: Perspectives and Challenges". Here they present their analysis about how IoT is playing and ever-expanding role that spans over from the traditional equipment to even general household objects such as WSN and RFID. But the great potential of IoT also raises some challenges when it comes to security. The paper focuses generally on these security challenges, among other things. Since it is based on the internet, IoT is also faced with the general internet security challenges. The paper focuses on security challenges at each layer of IoT seperately, i.e. the perception layer, transportation layer, and the application layer, while finding the solutions to these challenges at each layer. The paper also discussed the security issues of IoT as a whole, while also focusing upon and analyzing the security challenges of cross-layer heterogenous integration. The paper finally draws a comparison between the security issues of traditional networks and the security issues of IoT.

In 2014, Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu and Dechao Qiu, "Security of the Internet of Things: perspectives and challenges" analysis about Internet of Things (IoT) is playing a more and more important role after its showing up, it covers from traditional equipment to general household objects such as WSNs and RFID. With the great potential of IoT, there come all kinds of challenges. This paper focuses on the security problems among all other challenges. As IoT is built on the basis of the Internet, security problems of the Internet will also show up in IoT. And as IoT contains three layers: perception layer, transportation layer and application layer, this paper will analyze the security problems of each layer separately and try to find new problems and solutions. This paper also analyzes the cross-layer heterogeneous integration issues and security issues in detail and discusses the security issues of IoT as a whole and tries to find solutions to them. In the end, this paper compares security issues between IoT and traditional network, and they also discussed opening security issues of IoT.

In 2014, A. Rizzardi, S. Sicari, A. Coen-Porisini, and L. A. Grieco published "Security, Privacy and Trust in Internet of Things: The Road Ahead". The authors characterize IoT byb heterogeneous technologies, concurring to the provision of innovative services in domains of application. Here, fulfilment of privacy and security requirements play a vital role. These include data confidentiality, access control, and privacy and trust among users and things. Traditional countermeasures for security fail when applied to IoT technologies because of a number of factors, such as the involvement of different standards and communication stacks. There are scalability issues too, that need to be tackled when it comes to interconnecting of a large number of devices. Conclusively, there is a need of a flexible infrastructure that can deal with security threats given the dynamic nature of the such environment. The authors present the main challenges faced when it comes to research and explore the existing solutions in the field of IoT, and thus suggesting hints for the scope of future research in this field.

In 2015, Kyoochun Lee and In Lee published "The Internet of Things (IoT): Application, Investments, and Challenges for Enterprise". Here they study IoT as Industrial Internet, and envision a new paradigm of global network of machines and devices that have the capability of interacting with each other. They recognize IoT as one of the most vital areas if technology that is gaining vast attention from a range of industries. The authors recognize five technologies from of IoT that play the most essential parts for the development of IoT based products. Further, they discuss three IoT categories that can enhance customer value when it comes to enterprise application. The authors also explore the net present value method and the real option approach that is used for justification of technology projects and it illustrates how this approach can be used for IoT investment. Finally, the article shines some light on the managerial challenges.

In 2015, Mohsen Guizani, Moussa Ayyash, Mohammed Aledhari and Al-Fuqaha published "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications". Here they primarily survey present the survey about IoT while emphasis remains on enabling technology and application issues. The latest developments in RFID, smart sensors, IP, and communication technology enable IoT further. The premise is to enable sensors to collaborate without any human involvement. The recent developments in Internet, mobile and machine-to-machine technologies have acted as the primary phase of IoT. In the future, IoT can be expected to enable applications through establishing connections between physical objects to support intelligent decision making. The authors start with a horizon overview of IoT, then going on to review how IoT has enabled technologies, protocols and applications. The authors provide a thorough summary of the protocols that are relevant to IoT and the application issues faced. The survey brings the application developers and researchers at par with the different protocols and how these fit together to deliver functionalities without the RFCs and standards specifications. They also explore the challenges faced by IoT and summarize the recent literature and related research work. The article also explores how IoT is related to other emerging technologies such as big data analysis, cloud and fog computing etc. Another area

explored is the need for integration of the different IoT services. Finally, the paper presents how different protocols fit together to deliver IoT services as desired, by detailing of service use-cases to illustrate this.

In 2015, Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari and Moussa Ayyash "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications" in which they survey about the Internet of Things (IoT) with emphasis on enabling technologies, protocols, and application issues. The IoT is enabled by the latest developments in RFID, smart sensors, communication technologies, and Internet protocols. The basic premise is to have smart sensors collaborate directly without human involvement to deliver a new class of applications. The current revolution in Internet, mobile, and machine-to-machine (M2M) technologies can be seen as the first phase of the IoT. In the coming years, the IoT is expected to bridge diverse technologies to enable new applications by connecting physical objects together in support of intelligent decision making. This paper starts by providing a horizontal overview of the IoT. Then, they give an overview of some technical details that pertain to the IoT enabling technologies, protocols, and applications. Compared to other survey papers in the field, our objective is to provide a more thorough summary of the most relevant protocols and application issues to enable researchers and application developers to get up to speed quickly on how the different protocols fit together to deliver desired functionalities without having to go through RFCs and the standards specifications. They also provide an overview of some of the key IoT challenges presented in the recent literature and provide a summary of related research work. Moreover, they explore the relation between the IoT and other emerging technologies including big data analytics and cloud and fog computing. They also present the need for better horizontal integration among IoT services. Finally, they present detailed service use-cases to illustrate how the different protocols presented in the paper fit together to deliver desired IoT services.

V. CONCLUSION & FURTHER DEVELOPMENT

Internets of Things is one of the prominent as well as fastest growing technologies. It is very useful for modern life, helps to improve the quality of life, reliable, rapid accessible and flexible also. In this paper we discussed about the applications and various issues related to Internet of things.

REFERENCES

[1] Hongmei Deng, Wei Li, and Dharma P. Agrawal, Routing Security in Wireless Ad Hoc Networks, IEEE Communications Magazine, Pp: 70-75, October 2002.

[2] Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz, "Security Issues in Wireless Sensor Networks", International journal of communications Issue 1, Volume 2, 2008.

[3] K Renuka and G. Murali, "providing security for multipath routing protocol in wireless sensor networks", International Journal of Research in Engineering and Technology, eISSN: 2319-1163 | pISSN: 2321-7308.

[4] Rolf H. Weber, "Internet of Things - New security and privacy challenges", computer law & security review 26 (2010) 23-30.

[5] Debasis Bandyopadhyay and Jaydip Sen, "Internet of Things: Applications and Challenges in Technology and Standardization", Springer, Wireless Pers Commun (2011) 58:49-69.

[6] R. H. Weber, "Internet of things - new security and privacy challenges," Computer Law & Security Review, vol. 26, pp. 23-30, 2010.

[7] G. Yang, J. Xu, W. Chen, Z. H. Qi, and H. Y. Wang, "Security characteristic and technology in the internet of things," Journal of Nanjing University of Posts and Telecommunications (Natural Science), vol. 30, no. 4, Aug 2010.

[8] Z. H. Hu, "The research of several key question of internet of things," in Proc. of 2011 Int. Conf. on Intelligence Science and Information Engineering, pp. 362-365.

[9] Hui Suo, Jiafu Wan, Caifeng Zou and Jianqi Liu "Security in the Internet of Things: A Review", IEEE, 2012 International Conference on Computer Science and Electronics Engineering, Pp:648 -651

[10] Na Ruan andYoshiaki Hori, "DoS attack-tolerant TESLA-based broadcast authentication protocol in Internet of Things", IEEE, 2012 International Conference on Selected Topics in Mobile and Wireless Networking, Pp: 60-65.

[11] Huansheng Ning and Hong Liu, "Cyber-Physical-Social Based Security Architecture for Future Internet of Things", scientific research,Advances in Internet of Things, 2012, 2, 1-7

[12] Rodrigo Roman, Jianying Zhou and Javier Lopez "On the features and challenges of security and privacy in distributed internet of things" 2013 Elsevier, Computer Networks xxx (2013) , Pp: 1-14.

[13] Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu and Dechao Qiu, "Security of the Internet of Things: perspectives and challenges", Springer, online june 2014, DOI 10.1007/s11276-014-0761-7

[14] Afreen Fatima Mohammed studied about "Security Issues in IoT", 2017 IJSRSET | Volume 3 | Issue 8 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099 Pp: (3) 8 : 933-940.

BIOGRAPHIES

Pooja Sharma , B.E., M.Tech. Scholar in E-Security from Shri Shankaracharya Engineering College, Bhilai, India. Research areas are Wireless ad hoc Network, wireless sensor network & its enhancement.

Shankar Sharan Tripathi, Asst. Professor in Dept. of Computer Science & Engineering at Shri Shankaracharya Engineering College, Bhilai. India. Having wide experience in the fields of teaching. Research areas are Mobile ad hoc network, Wireless Sensor Network, its Enhancements, and His research work has been published in many national and international journals.

Radhe Shyam Panda, Asst. Professor in Dept. of Computer Science & Engineering at Shri Shankaracharya Engineering College, Bhilai. India. Having wide experience in the fields of teaching. Research areas are Mobile ad hoc network, Wireless Sensor Network, its Enhancements, and His research work has been published in many national and international journals.