International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 7 | ISSN : 2456-3307

# A Survey on Internet of Things

**Anjali Sharma, Shankar Sharan Tripathi, Radheshyam Panda**
Department of Computer Science & Engineering, Shri Shankaracharya Engineering College, Bhilai, Chhattisgarh, India

## 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, Many people across the world frequently browsing the internet for their daily requirement like browsing web pages, sending and receiving emails, watching videos, playing music, playing online games, chatting, video calling any many more tasks. Internet of thing helps to make every real thing into virtual things, this is nothing but a real wonder happened by the internet, sensors, and servers because nowadays each people, as well as things, are easily locatable and addressable on the internet. By the help of IoT technology work on behalf of people similar to people. IoT also very helpful for industrial, it is a new trend and technology in a global network.

Peoples are capable to easily communicating and interacting with each other. We can say that the internet of things is nothing but internet of everything. In the Internet of Things, we use centralized architectures for various services, in which central database provide all information, data and according to that data and 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 data, information regularly. 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.

**Figure 1 :** Internet of Things

## APPLICATIONS & USES OF IOT

1. Home security and smart domestic
2. Personal healthcare, healthcare carriers, and healthcare payers
3. Poster boards into IoT enabled boards
4. Interactive gaining of knowledge
5. Learning at any time and anywhere
6. Attendance Monitoring System
7. National Defense
8. Smart Cities
9. City Planning and Control
10. Quickly to Emergencies
11. Responding Production Flow Monitoring
12. Inventory Management
13. Plant Safety and Security
14. Quality Control
15. Logistics and Supply Chain Optimization
16. Research
17. Medical Information Distribution
18. Emergency Care
19. Precision Farming
20. Agriculture Drones
21. Livestock Monitoring
22. Smart Greenhouses
23. Commercial Energy
24. Residential Energy
25. Waste Management
26. Vehicle Tracking
27. Rails & Mass Transit
28. Industrial Transportation
29. Sound Detection
30. Humidity Sensors
31. Environment and Conditioning

## II. 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

## III. RELATED WORK

In 2002, Hongmei Deng, Wei Li, and Dharma P. Agrawal, Routing Security in Wireless Ad Hoc Networks in which a mobile ad hoc network consists of a collection of wireless mobile nodes that are capable of communicating with each other without the use of a network infrastructure or any centralized administration. MANET is an emerging research area with practical applications. However, wireless MANET is particularly vulnerable due to its fundamental characteristics, such as open medium, dynamic topology, distributed cooperation, and constrained capability. Routing plays an important role in the security of the entire network. In general, routing security in wireless MANETs appears to be a problem that is not trivial to solve. In this article they study the routing security issues of MANETs, and analyze in detail one type of attack — the “black hole” problem — that can easily be employed against the MANETs. They also proposed a solution for the black hole problem for ad hoc on-demand distance vector routing protocol.

In 2005, Daniele Puccinelli and Martin Haenggi studied about Wireless Sensor Networks: Applications and Challenges of Ubiquitous Sensing, in which Sensor networks offer a powerful combination of distributed sensing, computing and communication. They lend themselves to countless applications and, at the same time, offer numerous challenges due to their peculiarities, primary the stringent energy constraints to which sensing nodes are typically subjected. The distinguishing traits of sensor networks have a direct impact on the hardware design of the nodes at at least four levels: power source, processor, communication hardware, and sensors. Various hardware platforms have already been designed to test the many ideas spawned by the research community and to implement applications to virtually all fields of science and technology. They are convinced that CAS will be able to provide a substantial contribution to the development of this exciting field.

In 2006, Ye Ming Lu and Vincent W. S. Wong about an energy efficient multipath routing protocol for wireless sensor networks in which the energy consumption is a key design criterion for the routing protocols in wireless sensor networks. Some of the conventional single path routing schemes may not be optimal to maximize the network lifetime and connectivity. In this paper, they proposed a distributed, scalable and localized multipath search protocol to discover multiple node-disjoint paths between the sink and source nodes. They also proposed a load balancing algorithm to distribute the traffic over the multiple paths discovered. They compare our proposed scheme with the directed diffusion, directed transmission, N-to-1 multipath routing, and the energy-aware routing protocols. Simulation results show that their proposed scheme has a higher node energy efficiency, lower average delay and control overhead than those protocols.

In 2008 Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz deals with some security issues over wireless sensor networks (WSNs). A survey of recent trends in general security requirements, typical security threats, intrusion detection system, key distribution schemes and target localization is presented. In order to facilitate applications that require packet delivery from one or more senders to multiple receivers, provisioning security in group communications is pointed out as a critical and challenging goal. Presented issues are crucial for future implementation of WSN.

In 2009, Fadi Hamad, Leonid Smalov and Anne James, "Energy-aware Security in M-Commerce and the Internet of Things" in which Data privacy and security are a major concern for M-commerce and the Internet of Things. Security measures such as encryption may be implemented to protect confidentiality, integrity and availability. Limitations in processing power, battery life, communication bandwidth and memory constrain the applicability of existing cryptography standards for mobile devices. This paper describes an experiment to investigate the computational requirements for some of the most popular cryptographic algorithms with reference to power and resources consumption. Given reliable information on battery consumption, users can make informed decisions on which security schemes to use.

In 2010, Cristina Alcaraz, Pablo Najera, Javier Lopez and Rodrigo Roman, "Wireless Sensor Networks and the Internet of Things: Do They Need a Complete Integration?" in which Wireless sensor networks (WSN) behave as a digital skin, providing a virtual layer where the information about the physical world can be accessed by any computational system. As a result, they are an invaluable resource for realizing the vision of the Internet of Things (IoT). However, it is necessary to consider whether the devices of a WSN should be completely integrated into the Internet or not. In this paper, they tackle this

question from the perspective of security. While they will mention the different security challenges that may arise in such integration process, they will focus on the issues that take place at the network level.

In 2010, Rolf H. Weber, "Internet of Things – New security and privacy challenges" in which The Internet of Things, an emerging global Internet-based technical architecture facilitating the exchange of goods and services in global supply chain networks has an impact on the security and privacy of the involved stakeholders. Measures ensuring the architecture's resilience to attacks, data authentication, and access control and client privacy need to be established. An adequate legal framework must take the underlying technology into account and would best be established by an international legislator, which is supplemented by the private sector according to specific needs and thereby becomes easily adjustable. The contents of the respective legislation must encompass the right to information, provisions prohibiting or restricting the use of mechanisms of the Internet of Things, rules on IT-security-legislation, provisions supporting the use of mechanisms of the Internet of Things and the establishment of a task force doing research on the legal challenges of the IoT.

In 2011,Tobias Heer, Oscar Garcia-Morchon, René Hummen, Sye Loong Keoh, Sandeep S. Kumar and Klaus Wehrle, "Security Challenges in the IP-based Internet of Things" In which A direct interpretation of the term *Internet of Things* refers to the use of standard Internet protocols for the human-to-thing or thing-to-thing communication in embedded networks. Although the security needs are well-recognized in this domain, it is still not fully understood how existing IP security protocols and architectures can be deployed. In this paper, they discuss the applicability and limitations of existing Internet protocols and security architectures in the context of the Internet of Things. First, they give an overview of the deployment model and general security needs. They then present challenges and requirements for IP-based security solutions and highlight specific technical limitations of standard IP security protocols.

In 2011, Debasis Bandyopadhyay and Jaydip Sen, "Internet of Things: Applications and Challenges in Technology and Standardization" in which the phrase Internet of Things (IoT) heralds a vision of the future Internet where connecting physical things, from banknotes to bicycles, through a network will let them take an active part in the Internet, exchanging information about themselves and their surroundings. This will give immediate access to information about the physical world and the objects in it leading to innovative services and increase in efficiency and productivity. This paper studies the state-of-the-art of IoT and presents the key technological drivers, potential applications, challenges and future research areas in the domain of IoT. IoT definitions from different perspective in academic and industry communities are also discussed and compared. Finally some major issues of future research in IoT are identified and discussed briefly.

In 2012, Hui Suo, Jiafu Wan, Caifeng Zou and Jianqi Liu "Security in the Internet of Things: A Review" In the past decade, internet of things (IoT) has been a focus of research. Security and privacy are the key issues for IoT applications, and still face some enormous challenges. In order to facilitate this emerging domain, they in brief review the research progress of IoT, and pay attention to the security. By means of deeply analyzing the security architecture and features, the security requirements are given. On the basis of these, they discuss the research status of key technologies including encryption mechanism, communication security, protecting sensor data and cryptographic algorithms, and briefly outline the challenges.

In 2012, Na Ruan andYoshiaki Hori, "DoS attack-tolerant TESLA-based broadcast authentication protocol in Internet of Things" in which The Internet of Things (IoTs) is an emerging concept referring to networked everyday objects that interconnect to each other via wireless sensors attached to them. TESLA is a source authentication protocol for the broadcast network. Scalability of TESLA is limited by distribution of its unicast based initial parameter. Low energy consumption version of TESLA is μTESLA, which is designed for wireless sensor network (WSN), while cannot tolerate DoS attack. TESLA++ is the DoS tolerant version and is designed for VANET. TESLA++ cannot be accepted by WSN because of its higher consumption of power. To realize secure and robust DoS attack in the hybrid-vehicle sensor network, they provide a TESLA-based protocol against DoS attack with a lower consumption of power. Analysis results demonstrate that using our protocol is better than using μTESLA or TELSA++, respectively.

In 2012, Huansheng Ning and Hong Liu, "Cyber-Physical-Social Based Security Architecture for Future Internet of Things" in which As the Internet of Things (IoT) is emerging as an attractive paradigm, a typical IoT architecture that U2IoT (Unit IoT and Ubiquitous IoT) model has been presented for the future IoT. Based on the U2IoT model, this paper proposes a cyber-physical-social based security architecture (IPM) to deal with Information, Physical, and Management security perspectives, and presents how the architectural abstractions support U2IoT model. In particular, 1) an information security model is established to describe the mapping relations among U2IoT, security layer, and security requirement, in which social layer and additional intelligence and compatibility properties are infused into IPM; 2) physical security referring to the external context and inherent infrastructure are inspired by artificial immune algorithms; 3) recommended security strategies are suggested for social management control. The proposed IPM combining the cyber world, physical world and human social provides constructive proposal towards the future IoT security and privacy protection.

In 2013, Rene Hummen, Hanno Wirtz, Jan Henrik Ziegeldorf, Jens Hiller and Klaus Wehrle, "Tailoring End-to-End IP Security Protocols to the Internet of Things" they designed end to end IP security protocols Recent standardization efforts focus on a number of lightweight IP security protocol variants for end-to-end security in the Internet of Things (IoT), most notably DTLS, HIP DEX, and minimal IKEv2. These protocol variants commonly consider public-key-based cryptographic primitives in their protocol design for peer authentication and key agreement. In this paper, they identify several performance and security issues that originate from these public-key-based operations on resource-constrained IoT devices. To illustrate their impact, they additionally quantify these protocol limitations for HIP DEX. Most importantly, they find that public-key-based operations significantly hamper a peer's availability and response time during the protocol handshake. Hence, IP security protocols in the IoT must be tailored to reduce the need for expensive cryptographic operations, to protect resource-constrained peers against DoS attacks targeting these cryptographic operations, and to account for high message processing times. To this end, they present three complementary, lightweight protocol extensions for HIP DEX: i) a comprehensive session resumption mechanism, ii) a collaborative puzzle-based DoS protection mechanism, and iii) a refined retransmission Mechanism. Our focus on common protocol functionality allows generalizing our proposed extensions to the wider scope of DTLS and IKE. Finally, our evaluation confirms the considerable achieved improvements at modest trade-offs.

In 2013, Rodrigo Roman, Jianying Zhou and Javier Lopez "On the features and challenges of security and privacy in distributed internet of things" in which In the Internet of Things, services can be provisioned using centralized architectures, where central entities acquire, process, and provide information. Alternatively, 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 order to understand the applicability and viability of this distributed approach, it is necessary to know its advantages and disadvantages not only in terms of features but also in terms of security and privacy challenges. The purpose of this paper is to show that the distributed approach has various challenges that need to be solved, but also various interesting properties and strengths.

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, S. Sicari, A. Rizzardi, L.A. Grieco and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead" in which Internet of Things (IoT) is characterized by heterogeneous technologies, which concur to the provisioning of innovative services in various application domains. In this scenario, the satisfaction of security and privacy requirements plays a fundamental role. Such requirements include data confidentiality and authentication, access control within the IoT network, privacy and trust among users and things, and the enforcement of security and privacy policies. Traditional security countermeasures cannot be directly applied to IoT technologies due to the different standards and communication stacks involved. Moreover, the high number of interconnected devices arise scalability issues; therefore a flexible infrastructure is needed able to deal with security threats in such a dynamic environment. In this survey they present the main research challenges and the existing solutions in the field of IoT security, identifying open issues, and suggesting some hints for future research.

In 2015, In Lee & Kyoochun Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises". In which they studied about The Internet of Things (IoT), also called the Internet of Everything or the Industrial Internet, and is a new technology paradigm envisioned as a global network of machines and devices capable of interacting with each other. The IoT is recognized as one of the most important areas of future technology and is gaining vast attention from a wide range of industries. This article presents five IoT technologies that are essential in the deployment of successful IoT-based products and services and discusses three IoT categories for enterprise applications used to enhance customer value. In addition, it examines the net present value method and the real option approach widely used in the justification of technology projects and illustrates how the real option approach can be

applied for IoT investment. Finally, this article they also discusses five technical and managerial challenges.

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.

In 2017, Afreen Fatima Mohammed studied about "Security Issues in IoT" in which The Internet of things (IoT) is the network of various interconnected physical devices, vehicles, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data. It connects devices embedded in various systems to the internet. When devices/objects can represent themselves digitally, they can be controlled or accessed from anywhere. The connectivity then helps to capture more data from more places, ensuring more ways of increasing efficiency and improving safety and IoT security. Data privacy, confidentiality, data integrity is at Potential risk when these devices are connected. As more and more IoT devices are coming in the market, securing IoT systems represents a number of challenges. This paper discusses about various vulnerabilities and threats against IoT and what actions could be taken to provide a more secure IoT.

## IV. CONCLUSION & FURTHER DEVELOPMENT

Internets of things are 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 the applications and various issues related to the Internet of things.

## V. 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]. Daniele Puccinelli and Martin Haenggi, "Wireless Sensor Networks: Applications and

Challenges of Ubiquitous Sensing ",IEEE circuits and systems magazine third quarter 2005.

[3]. Ye Ming Luand Vincent W. S. Wong, "an energy efficient multipath routing protocol for wireless sensor networks" international journal of communication systems, 2007; 20:747-766, in Wiley Inter Science (www.interscience.wiley.com).

[4]. 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.

[5]. Fadi Hamad, Leonid Smalov and Anne James, "Energy-aware Security in M-Commerce and the Internet of Things", IETE TECHNICAL REVIEW | vol 26 | ISSUE 5 | SEP-oct 2009, Pp: 357-362.

[6]. Cristina Alcaraz, Pablo Najera, Javier Lopez and Rodrigo Roman, "Wireless Sensor Networks and the Internet of Things: Do They Need a Complete Integration?", International Workshop on the Security of the Internet of Things (SecIoT10), 2010.

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

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

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

[10]. J. F. Wan, H. H. Yan, H. Suo, and F. Li, "Advances in cyber-physical systems research," KSII Transactions on Internet and Information Systems, 2011, 5(11): 1891-1908.

[11]. M. Chen, J. F. Wan, and F. Li, "Machine-to-machine communications: architectures, standards, and applications," KSII Transactions on Internet and Information Systems, to appear, January 2012.

[12]. 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.

[13]. 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.

[14]. 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

[15]. 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.

[16]. 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

[17]. Rene Hummen, Hanno Wirtz, Jan Henrik Ziegeldorf, Jens Hiller and Klaus Wehrle, "Tailoring End-to-End IP Security Protocols to the Internet of Things" 978-1-4799-1270-4/13/$31.00, 2013 IEEE

[18]. 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.

[19]. 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

[20]. Lee & Kyoochun Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises", Business Horizons (2015) 58, 431—440

[21]. Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari and Moussa Ayyash "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications", IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 17, NO. 4, FOURTH QUARTER 2015

**[22].** 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.

## Author's Profile

**Anjali Sharma ,** B.E., M.Tech. Scholar in E-Security from Shri Shankaracharya Engineering College, Bhilai, India. Research areas are Internet of things, 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,** Head of Department & 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 Internet of things, Mobile ad hoc network, Wireless Sensor Network, its Enhancements, and His research work has been published in many national and international journals.