iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** VII **Month of publication:** July 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 3 Issue VII, July 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Issues in Internet of Things: A Survey

Prema N[1], Vedavathi N[2], Lovee Jain[3]
Department of Computer Science and Engineering, NIE Institute of Technology, Mysore, Karnataka, India

Abstract---Internet of Things is a new revolution of the Internet. The goal of the Internet of Things is to enable things to be connected anytime, anyplace with anything and anyone ideally using any network and any service. Nowadays, as sensing, actuation, communication, and control become even more sophisticated and ubiquitous, there is a significant overlap in these communities. The Internet of Things is not a single technology, it's a concept in which most new things are connected and enabled. As the Internet of Things continues to develop, further potential can be estimated by a combination with related technology approaches and concepts such as Cloud Computing, Future Internet, Big Data, Robotics, Semantic technologies. All these diverse concepts integrated for communicating with each other to realize Internet of Things leads to increased complexity. However, the Internet of Things is still maturing, in particular due to a number of factors, which limit the full exploitation of the Internet of Things. In this context the research and development challenges to create a smart world are enormous. To provide a basis for understanding open research problems and issues with Internet of Things, a survey has been presented in this paper. The survey introduces challenges in various aspects/concepts of Internet of Things like Security and Privacy, IoT Addressing, Cloud Forensic, Big Data, Enterprise, Server Technology, Data Centre Network and so on. Detailed analysis of these issues would lead to a better exploitation of Internet of Things. Also, detailed introduction to Internet of things and its applications are presented in this paper.

Keywords: IoT, Cloud Computing, Big Data, IoT Addressing, Robotics

I. INTRODUCTION

Internet of Things (IoT) is a concept and a paradigm that considers pervasive presence in the environment of a variety of things/objects that through wireless and wired connections and unique addressing schemes are able to interact with each other and cooperate with other things/objects to create new applications and services. In this context the research and development challenges to create a smart world enormous. Internet of Things is a new revolution of the Internet. Objects make themselves recognizable and they obtain intelligence by making or enabling context related decisions. They can access information that has been aggregated by other things, or they can be components of complex services. Enabling technologies for the Internet of Things such as sensor networks, RFID, M2M, mobile Internet, semantic data integration, IPV6, etc. can be grouped into three categories: (i) technologies that enable "things" to acquire contextual information, (ii) technologies that enable "things" to process contextual information, and (iii) technologies to improve security and privacy. Internet of Things developments implies that the environments, cities, buildings, vehicles, portable devices and other objects have more and more information associated with them and/or the ability to sense, communicate, network and produce new information. The Internet is not only a network of computers, but it has evolved into a network of devices of all types and sizes, vehicles, smartphones, home appliances, toys, cameras, medical instruments and industrial systems, all connected, all communicating and sharing information all the time as presented in Fig 1.

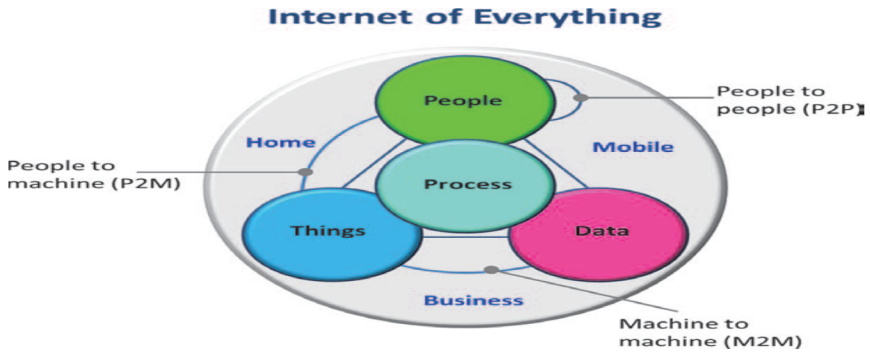


Fig. 1. Internet of Everything

However, the Internet of Things is still maturing, in particular due to a number of factors, which limit the full exploitation of the IoT. Some of those factors are listed below:

No clear approach for the utilization of unique identifiers and numbering spaces for various kinds of persistent and volatile objects at a global scale.

No accelerated use and further development of IoT reference architectures.

Less rapid advance in semantic interoperability for exchanging sensor information in heterogeneous environments.

Difficulties in developing a clear approach for enabling innovation, trust and ownership of data in the IoT while at the same time respecting security and privacy in a complex environment.

Difficulties in developing business which embraces the full potential of the Internet of Things.

Missing large-scale testing and learning environments, which both facilitate the experimentation with complex sensor networks and stimulate innovation through reflection and experience.

Only partly deployed rich interfaces in light of a growing amount of data and the need for context-integrated presentation [1].

II. RELATED WORK

Overcoming the challenges introduced in section1 would result in a better exploitation of the Inter of Things potential by a stronger cross-domain interactivity, increased real world awareness and utilization of an infinite problem -solving space. The following subsections will present elaborated introduction to some of the issues with IoT.

A. Security and Privacy Challenge In Data Aggregation

Security and privacy issues should be considered very seriously since IoT deals not only with huge amount of sensitive data (personal data, business data, etc.) but also has the power of influencing the physical environment with its control abilities. Cyber-physical environments must thus be protected from any kind of malicious attacks. The IoT should autonomously tune itself to different levels of security and privacy, while not affecting the quality of service and quality of experience. Security attacks in autonomic and self-aware IoT systems in safety context (e.g. driving cards) can become even more serious because the implementation of a security threat can impact the safety of a user by disrupting the autonomic process.

If the digitalization and automation of millions of devices will create a whole new security landscape as enterprises attempt to protect themselves, it will also create new opportunities for operational technology security providers. Already, many industry-specific security platforms are being developed for specialist areas like industrialized systems, medical equipment, and air and defense sectors and, in many cases, being integrated into the platforms being developed by equipment providers for those industries. Such solutions are aimed at securing various aspects of specific devices, such as smart meters, or focusing on tackling platform-specific vulnerabilities [1]. The vision of SMARTIE (Secure and Smarter Cities data management) is to create a distributed framework for IoT based applications sharing large volumes of heterogeneous information. This framework is envisioned to enable end-to-end security and trust in information delivery for decision-making purposes following data owner's privacy requirements. SMARTIE will design and build a data-centering information sharing platform in which information will be accessed through an information service layer operating above heterogeneous network devices and data sources and provide services to diverse applications in a transparent manner. It is crucial for the approach that all the layers involve appropriate mechanisms to protect the data already at the perception layer as well as at the layers on top of it. These mechanisms shall cooperate in order to provide a cross-layer holistic approach. SMARTIE will focus on key innovations that strengthen security, privacy and trust at different IoT Layers as depicted in the following table-1 [1].

Volume 3 Issue VII, July 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

TABLE I
SECURITY REQUIREMENTS AT DIFFERENT LAYERS OF IOT

IoT layers	Security requirements
Applications (Intelligent Transportation, Smart Energy, Public Safety, Utilities, Service Providers, etc.)	• Authentication, Authorization, Assurance; • Privacy Protection and Policy Management; • Secure Computation; • Application-specific Data Minimization; • Discovery of Information Sources
Information Services (In-network Data Processing, Data Aggregation, Cloud Computing, etc.)	• Cryptographic Data Storage; • Protected Data Management and Handling (Search, Aggregation, Correlation, Computation);
Network (Networking infrastructure and Network-level protocols.)	• Communication & Connectivity Security; • Secure Sensor/Cloud Interaction; • Cross-domain Data Security Handling
Smart Objects (Sensors for data collection, Actuators)	• Data Format and Structures; • Trust Anchors and Attestation; • Access Control to Nodes • Lightweight Encryption

B. IOT Addressing

Much of the focus around IoT has been on Internet of Things security, but there's another issue administrators must tackle when deploying connected devices: addressing. IPv4 is the leading addressing technology supported by internet hosts. However, IANA, the international organization that assigns IP addresses at global level as recently announced the exhaustion of IPv4 address block. IoT networks, in turn, are expected to include billions of nodes, each of which shall be uniquely addressable. A solution to this problem is offered by the IPv6 standard, which provides a 128-bit address field, thus making it possible to assign a unique IPv6 address to any possible node in the Iot network. Additional reasons for IPv6 are mobile IP support, auto configuration techniques, and build in security features of IPSec [2].

C. Cloud Forensics

Cloud forensics will play a key role in the IoT forensics sphere especially since the data generated from IoT aware and IoT networks are already being, or will increasingly be stored, on cloud locations. This is because cloud solutions offer various benefits including convenience, large capacity, scalability, and on-demand accessibility. However, attacks such as Structured Query Language (SQL) injection, side channel, authentication, man-in-the-middle attacks, and insecure virtual machine deletion, etc. being discovered and exploited in various cloud-related crimes have led to a need for digital forensics in the cloud environment. Cloud forensics is made difficult by the absence of agreements between parties in the cloud which can allow for investigations within and between customer

cloud-based services. In addition, the (sometimes unknown) location of the sources of evidence, as well as inter judiciary disparities can make cloud computing a challenge for Digital Forensic investigators. These threats and challenges to cloud environments will inevitably also apply to the IoT-based forensic investigations. [3]

D. Big Data

The impact of the IoT on storage is two-pronged in types of data to be stored: personal data (consumer-driven) and big data (enterprise-driven). Already in use in key verticals such as healthcare and financial services, big data is transforming how and why companies collect and store data. IT administrators that are already tasked with keeping the storage centers running will also have to figure out how to store protect and make all the incoming data accessible. If, as Gartner, estimated, storage servers are only being used to between 30 and 50 percent of capacity, the physical capabilities are there. Managing them, however, is an entirely different problem. The Internet of Things (IoT) has generated a large amount of research interest across a wide variety of technical areas. These include the physical devices themselves, communications among them, and relationships between them. One of the effects of ubiquitous sensors networked together into large ecosystems has been an enormous flow of data supporting a wide variety of applications. Technical and management challenges abound in this area, including: sensor networks management, and data management, analysis, and visualization. At the same time, new research, tools, and applications in the field of "big data" have been exploding as researchers find new ways of addressing the challenges posed by volume, velocity and variety of data. The convergence of IoT and big data creates new opportunities for interesting and high impact research. Many sensor network data flows exhibit high velocity, distributed streams of heterogeneous data, often from mobile sources, and varying quality. As with previous sources of big data, the challenges exceed the capabilities of existing technologies, processes, and infrastructures. This special issue will provide a forum for researchers to present ideas, innovations, and applications of big data analytics and management to IoT [4].

Topics of interests include (but are not limited to):

Theoretical and computational models for IoT Big data

Methods, theory, and technology for storage and management of real world observation and measurement data

High performance, error tolerant, reliable data transport protocols and standards.

Security, privacy, quality, and trust issues in IoT

Scalable and efficient streaming data structures, architectures, analysis, and visualization algorithms for IoT services and applications.

Distributed sensing, and heterogeneous big data integration and mining in IoT

Energy efficient processing and high performance computing on the IoT big data

Large stream processing, and very large scale semantic event processing for IoT.

E. Storage Management

However, even if the capacity is available now, there will be further demands made on storage and one that will have to be addressed as the need to access this information becomes more important. Businesses will have weighed up the economics of storage against the value of IoT information [4].

F. Server Technologies

The impact of IoT on the server market will be largely focused on increased investment in key vertical industries and organizations related to those industries where IoT can be profitable, or add significant value. Some organizations that manage and consume data collected from a huge array of devices will require additional compute capacity and may well increase server budgets if there is a business case for it [4].

G. Data Center Network

Existing data center WAN (Wide Area Network) links have been built for moderate-bandwidth requirements created by our current use of technology. However, as the amount of data being transferred is set to increase dramatically, the need for expanded bandwidth grows [4].

III. APPLICATIONS

Potential applications of the IoT are numerous and diverse, permeating into practically all areas of every-day life of individuals (the so-called “smart life”), enterprises, and society as a whole. The IoT application covers “smart” environments/spaces in domains such as: Transportation, Building, City, Lifestyle, Retail, Agriculture, and Factory, Supply chain, Emergency, Health care, User interaction, Culture and Tourism, Environment and Energy.

IV. CONCLUSIONS

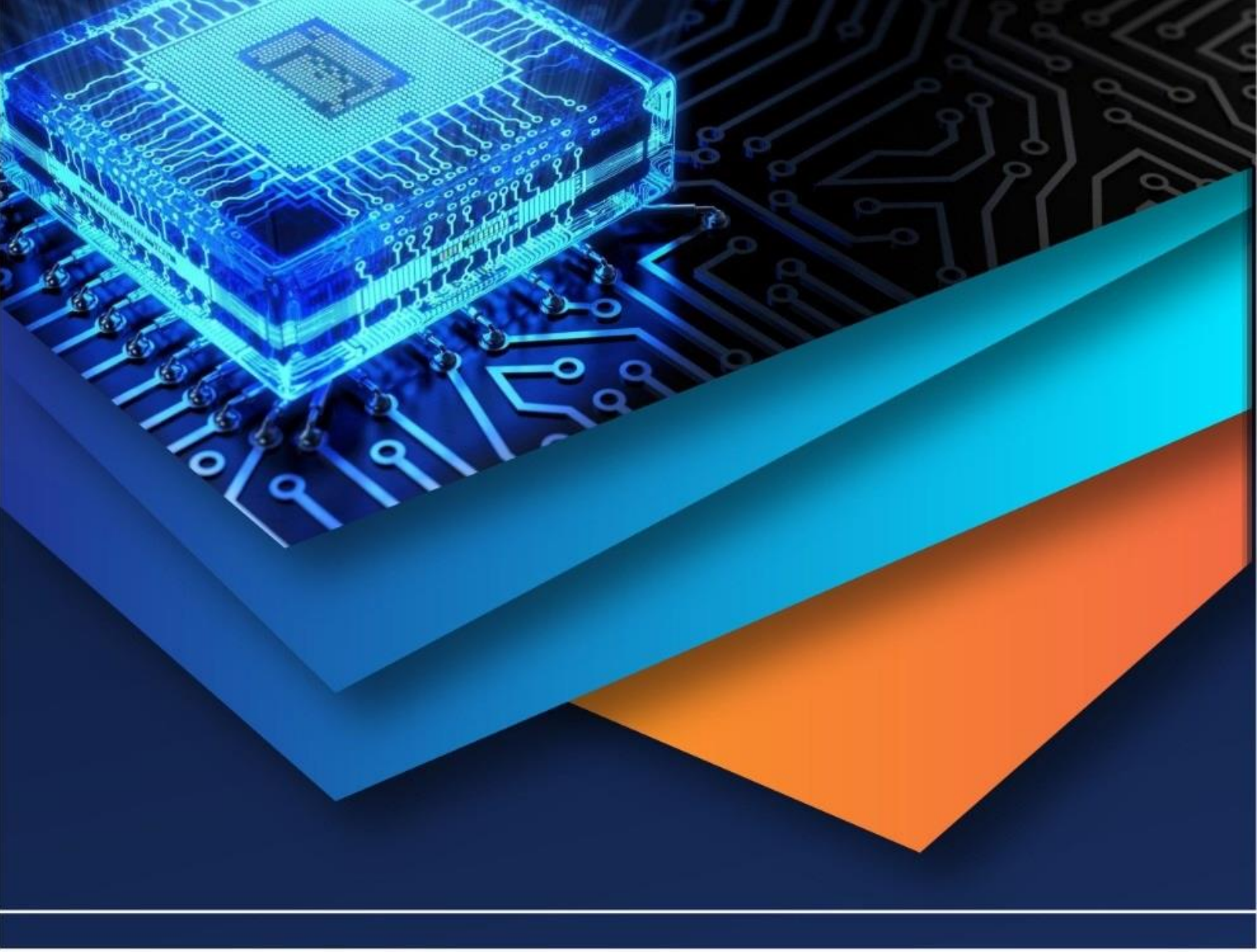
The Internet of Things continues to affirm its important position in the context of Information and Communication Technologies and the development of society. Whereas concepts and basic foundations have been elaborated and reached maturity, further efforts are necessary for unleashing the full potential of IoT. In this paper many of issues that need to be addressed are presented**.**

V. ACKNOWLEDGEMENT

The material of this survey paper is taken from various previously published papers and text book on IoT. Particularly, the major content is from [1].

REFERENCES

[1] Dr. Ovidiu Vermesan, Dr. Peter Friess, Internet of Things – Converging Technologies for Smart Environment and Integrated Ecosystems, Algade, Aalborg, Denmark, River Publishers, 2013.
[2] L.Atzori, A.Iera, and G. Morabito, “The internet of things: A survey,” comput. Netw., vol. 54, no. 15,pp. 2787-2805, 2010
[3] Edewede Oriwoh, David Jazani, Gregory Epiphaniou and Paul Sant. “Internet of Things Forensics: Challenges and Approaches, 9th IEEE International Conference on Collaborative Computing : Networking Applications and Worksharing (collaborateCom 2013).
[4] Internet of Things [online] http://www.cmswire.com
[5] Roman, R., Najera, P., Lopez, J., “Securing the Internet of Things,” Computer , vol. 44,no. 9, pp. 51, 58, Sept. 2011.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY