ISSN (Print) : 2319-8613
ISSN (Online) : 0975-4024

Security & privacy in IoT Data Provenance

Adarsh.T.K[1], Dr. R Jebakumar[2]
[1]Research Scholar, Department of CSE , [2]Asso.Professor Department of CSE,
SRM University, Chennai, India
adarshtk@gmail.com
rrjeba@gmail.com

***Abstract*— IoT has become most emerging trend in engineering and technology, that has bring relevant change in industries. IoT has many applications like healthcare, agriculture etc. Since IoT deals with huge number of objects that need to generate and consume different types of data and entity. The need of security and privacy challenges should enforced. The data provenance deals with detecting creation and propagation of data, The main purpose of the paper is to address security and privacy issues by implementing data provenance in IoT. To this end we will mention different challenges to meet security and privacy in IoT data provenance**

Keywords — Inrernet of Things; IoT, data Provenance

I. INTRODUCTION

The Internet of Things (IoT), place were all the objects of different kinds from smart phones, sensors or devices are with network enabled objects can communicate with each other and makes a part of Internet. Due to the evaluation IoT have change massively the quality of many existing systems in all aspects by making intelligent devices. The main aim of IoT is to make internet more and more reliable to the users by connecting wide range of devices. Internet of Things is very useful in storing, processing the huge amount of data in the efficient and reliable way which can be easily interpreted there comes the important of data provenance in IoT.

The term data provenance to refer to the process of tracing and recording the origins of data and its movement[1], Provenance is now an acute issue in all domains since the data generated is from wide variety of device that are connected through IoT. The necessity of provenance need in scientific domain, Business domain, health etc. In brief data provenance in IoT is an emerging area that ensure the need of protected and secure data.

This paper provides particular attention towards issues of security and privacy in IoT data provenance. To ensure security and privacy in the interaction of massive heterogeneous devices it is very difficult to achieve provenance data. Provenance is one kind of metadata that tracks the steps by which the data was derived and can provide significant value, The term trustworthiness of data is highlighted and aims to achieve through current challenges

In this paper, we provide a detailed view of current data provenance research in the scientific and business that need protection of data and challenges faced . The rest of paper is structured as follows: section 2 provides an overview of IoT. Section 3 describes the security and privacy issues in IoT. Section 4 data provenance Challenges and techniques. Section 5 Proposed Works Finally the paper concludes in Section 6.

Overview of IoT

A definition for the IoT would be: “Group of infrastructures interconnecting connected objects and allowing their management, data mining and the access to the data they generate. [2] Things or objects in real world to communicate with each other. Sensors, RFID tags, actuators, mobile phones, etc. are used to connect real world things together. Now IOT application range from environmental monitoring, home automation to medical and healthcare systems, transportation to energy and infrastructure management and so on. Figure 1 shows other major application of IoT. There are three IOT components that enables global computing:[3] (1) Hardware that is made up of sensors and embedded communication hardware. (2) Middleware that is on demand storage and computing tools for data analytics. (3) Presentation it is used to understand visualization and interpretation which can be designed for different application.

II. SECURITY & PRIVACY ISSUES IN IoT

There are enormous number of protocols and technologies are available to address most of the security issues but due to the unique characteristics of IoT makes its difficult to implement the major threats are physical, identity fabrication etc. Typical security goal like Confidentiality, Integrity and Availability etc. also apply to IoT. This section consist of two parts: in general privacy and security features in IoT and Challenges.

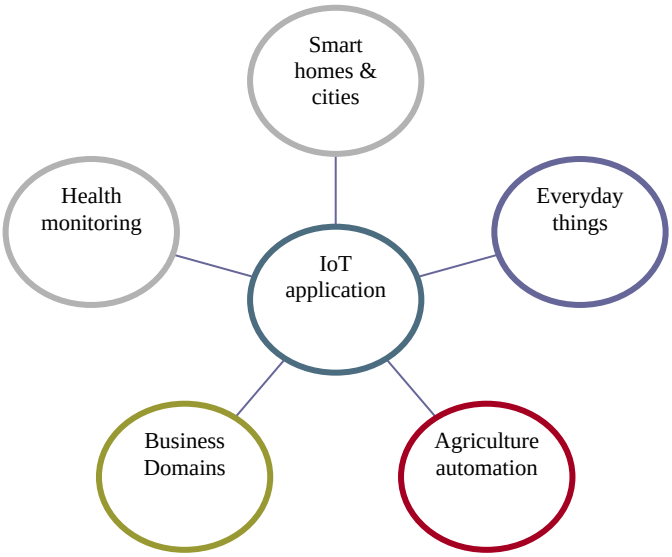

Figure 1. IoT applications

A. *Privacy & Security Features of IoT*

Privacy is a very broad and diverse notion for which offers many definitions and perspective. With the increasing use and efficiency of electronic data processing information privacy has become the predominant issue today. In the case of health care system biological data should need its own privacy. But due to the heterogeneous [6]property of IoT it becomes most difficult. Hence we must take care while deals with this kinds of data. Here some security principles that should be enforced to achieve a secure communication framework

1) Confidentiality:

A very important parameter to ensure that the data is secure and only available to authorized users. Since wide variety of entities are involved in communication it deals with how data will be managed for example in health care systems more number of subjects are involved in the data collection so it should not relieve to neighboring users.

2) Integrity

Accuracy of data is very important that is during the time of transmission data should not be altered. IoT is based on many devices this part also given a care. This feature can given only by end to end security. There are number of protocol are there but due to the low computational power at IoT nodes make this difficult task.

3) Availability

The availability of not only the data but also the devices to service is also another important factor it should reach to service when it need. There are many barriers to achieve this including physical and technical barriers

B. *Privacy & Security Challenges*

- Common encryption protocols, are very expensive when running on devices with limited computing capabilities
- An sensitive information should have well protected like personal health data that communicated through verity of heterogeneous devices .
- DoS which make the device, resource or network unavailable to authorized users.
- An active attack directly stops the service while the passive kind monitors [7]IoT network information without hindering its service.
- the amount of data that will be revealed, and who will be responsible for managing these applications

To face these challenge one solution is data provenance techniques in the following section data provenance is discussed to meet the security and privacy in IoT data provenance

III. DATA PROVENANCE

Provenance-aware system has the ability to keep track of ownership of data, origin from when and where, It can be defined as the process of detecting the lineage and the derivation of data and data objects data provenance provide wide range of application like estimating the level of quality and trust of data, audit trail, debugging, reusability and reproducibility, and analyzing performance bottlenecks. It can also be used in areas such as ownership, security, citation, and copyright In the following sections provides challenges in provenance and techniques for data provenance

A. Challenges in Data Provenance – IoT

A digital library is a large and heterogeneous collection of on-line documents and databases so its very complicated to to find the linage and derivation of data. There are several challenges facing while implementing data provenances in IoT systems. The following are some of major challenges faced

1) To ensure provenance datasecurity

Unauthorized access of data lead to exploitation of sensitive information so provenance data need confidentiality another point it also protect identity of objects. In certain applications provenance of data more sensitive than objects. Trustworthy data [11] is another basic need to attain provenance to attain secure sophisticated measure are available like signed hashes but it is very difficult to implement in IoT systems.

2) Data processing and storage

In IoT the data transmissed and consumed in very large amount due to increaing number of participants hence huge amount of data will tansmited to achieve efficent storage and processing is difficult due to space complexicity and energy computation.The concept of meta data is used to determne information provenance so tracing data object in big data is become very difficult, [14] conssumption of network banwidth in another issue faced to avoid performance of system

3) Indexing provenance

The IoT system likely to large it is very difficult to look each and every data and find name, to avoid this searching datasets of attributes can done to found in meta data depending up on the user the query will change depending u on the goal, another way is indexing can be done in few cases Data Citation can be done but it required efficient lookups in all dimensions to retrieve data.

4) Interoperability of heterogeneous data:

IoT application are usually dynamic and uniqueness due to involved different variety of objects the aggregation of variety of data is major issued faced. Another major challenge is environment is changing so to ensure proper key management and protocol required. Therefore it is very important to achieve interoperability among other objects

B. Data Provenance Techniques

There are different method are implemented in previously here in our paper we will discuss few relevant technology mean while some other are discarded by the relevance of data provenance achieved . A summary is mention in table 1

1) Lineage Information Program

Lanter designed a Lineage Information Program (LIP) the study of lineage in GIS applications. Lineage gives a notion of the quality of GIS datasets based on the source data GIS applications use a cartographic model to transform and derive spatial layers LIP [15] uses a data structure called frame which describes the metadata of a spatial layer. Three types of frames are available: source frame, containing quality information about the source layers, such as scale and projection; command frame, with the commands used to derive intermediate and product layers; and product frames that has metadata specific to the product layers

The information in the lineage meta-database can be interrogated interactively using command-line queries, and LIP traverses the stored semantic network to answer the queries. Lineage can also identify equivalent layers in order to remove redundancy in the database.

2) Chimera

It is a prototype implementation of a Virtual Data Grid (VDG) that manages the derivation and analysis of data objects in collaboratory environments Chimera tracks provenance in the form of the data derivation steps for datasets and uses it for on-demand regeneration of derived data. The lineage in Chimera is represented in virtual data language VDL that is managed by a virtual data catalog (VDC) service. The VDC maps the VDL to a relational schema and stores it in a relational database accessible through SQL queries. Lineage information can be retrieved from the VDC using queries written in VDL

3) Provenance Aware Service-oriented Architecture

The Provenance Aware Service Oriented Architecture (PASOA) project is building a provenance infrastructure for recording, storing and reasoning over provenance using an open provenance protocol in e-science communities. Goal of PASOA identifies several requirements for a provenance system such as verifiability, reproducibility of the process, accountability, scalability and preservation of provenance system. The Provenance Recording Protocol (PReP) are divided into four phases: negotiation phase, invocation phase, provenance recording phase, and termination phase, during which the actors agree upon a provenance service to record the provenance. Provenance Recording for Services (PReServ) is a web service implementation of the PReP protocol that stores the provenance either in memory, in a relational database, or in the file system

4) PUFs and wireless link finger prints

A PUF is a physically disordered system that maps a set of challenges to a set of responses based on the underlying physical micro structure of the device and it is very difficult to clone and wireless finger print in any of the wireless channel parameters such as the received signal strength indicator (RSSI) may uniquely identify a wireless link between two parties . the received signal strength indicator (RSSI) [16]values of a wireless channel can be used as the fingerprint of a wireless link. However, their technique requires the device to store a secret key and depends on the public key infrastructure

TABLE I. SUMMARY OF DATA PROVENANCE TECHNIQUES

characteristic	**Techniques**			
	LIP	***Chimera***	***PASOA***	***PUF & wireless finger print***
Domain	GIS	Astronomy	Health care	Generic
Frame work	Command processing	Service Oriented	Service Oriented	Physical objects
Application of provenance	Nformational	Audit; Data Regeneration	Re-enactment	Update propagation
Storage	Meta Database	Relational DB	File System	Lineage Server
Provenance collection	commands	User defines derivations	Manual	Inverse query
Representation scheme	Frames	Virtual Data Language	Annotations	Frames

IV. PROPOSED WORK

IoT has been tremendous development in recent years in industries as a result intelligent system become vital part of day today life how ever security challenge of IoT still become relevant research area at the same time data provenance play a vital role in security and privacy, in the following discussion make secure IoT data provenance.

1) Establishing trustworthiness

Trust should established between both parties for the effective communication one of the method is creating an access control frame work in transmission phase of IoT. With the help of key or token we can provide trust, the key or token is created by manufacture for the identification of devices. the generation of key part of identification of device. After establishing trust then the part of privacy is quiet easy, in proposed work a hand shake key is developed, after validating key with both parties connection is authenticated. This mechanism ensure the authority to consume provenance data

2) Authentication Unit(AU)

In this section major role is to provide security in order to this a Authentication Unit is get in to action this is commonly part of a gateway. AU operate in two phases: connection establishment phase and data transfer phase. During the connection establishment phase a key is generate by a device including time location and false number will send to AU that will communicate with receiver and make sure that it is a authorized device, and during second phase the data will transmitted only between authenticated devices. Hence the ownership of data is more protected through AU.

V. CONCLUSION

The purpose of the work in this paper is to provide a secure and privacy in IoT data provenance we explore several open research question and find need of data provenance is all field including research, health etc. Due to the advancement of IoT however it find interesting to achieve provenance data that achieve all challenges. A basic privacy and security mechanism is proposed to attain the provenance in IoT

REFERENCES

[1] Muhammad M Aman , Kee Chaing Chua, Biplab Sikdar, Secure Data Provenance for Internet Of Thing, IoTPTS'17, April 02 2017, Abu Dhabi, United Arab Emirates
[2] M. N. Aman et. al.,"Physical Unclonable Functions for IoT Security," Proceedings of ACM AsiaCCS IoTPTS, June 2016.
[3] Adel Alkhalil , Rabie A Ramadan, IoT Data Provennce iimplementation Challenges , University, Cairo, Egypt, and College of Computer Science and Engineering, Hail UProcedia Computer Science 109C (2017)1134–1139
[4] Mahmoud, R.; Yousuf, T.; Aloul, F.; Zualkernan, I. Internet of things (IoT) security: Current status, challenges and prospective measures. 2015 10th Int. Conf. Internet Technol. Secur. Trans. 2016, 336–341.
[5] Yogesh L. Simmhan, Beth Plale, Dennis Gannon, A Survey of Data Provenance Techniques, Computer Science Department, Indiana University, Bloomington IN 47405
[6] Introducing Secure Provenance in IoT: Requirements and Challenges, Sabah Suhail, Choong Seon Hong Department of Computer Science and Engineering, Kyung Hee University, Yongin,Korea978-1-5090-5091-8/16 $31.00 © 2016 IEEE
[7] E. Bertino, "Data Security and Privacy in the IoT," Proc. EDBT, March 2016
[8] Gubbi, J.; Buyya, R.; Marusic, S. Internet of Things (IoT): A vision, architectural elements, and future directions. Futur. Gener. Comput. Syst. 2013, 29, 1645–1660.
[9] Rose, K.; Eldridge, S.; Lyman, C. The internet of things: an overview. Internet Soc. 2015, 53.
[10] Abdmeziem, R.; Tandjaoui, D. Internet of Things: Concept, Building blocks, Applications and Challenges. arXiv , 2014.. Eason, B. Noble, and I.N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529-551, April 1955. (references)
[11] A Systematic Study of Security Issues in Internet-of-Things (IoT), International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC 2017)
[12] Radomirovic S. Towards a Model for Security and Privacy in the Internet of Things.1st International Workshop on the Security of the Internet of Things, Tokyo, Japan, 2010.
[13] Ko, Ryan KL, and Mark Will.Progger: An Efficient, TamperEvident Kernel-Space Logger for Cloud Data Provenance Tracking, Cloud Computing (CLOUD), 2014 IEEE 7th International Conference on. IEEE, 2014.
[14] Hussain, S. R., Wang, C., Sultana, S., & Bertino, E. (2014,December).Secure data provenance compression using arithmetic coding in wireless sensor networks, In PerformanceComputing and Communications Conference (IPCCC), 2014 IEEE International (pp. 1-10). IEEE.
[15] Hussain, S. R., Wang, C., Sultana, S., & Bertino, E. (2014,December).Secure data provenance compression using arithmetic coding in wireless sensor networks, In PerformanceComputing and Communications Conference (IPCCC), 2014 IEEE International (pp. 1-10). IEEE.
[16] Ruben Mayer, Boris Koldehofe, and Kurt Rothermel," Predictable Low-Latency Event Detection with Parallel Complex Event Processing", IEEE INTERNET OF THINGS JOURNAL, VOL. 2, NO. 4, AUGUST 2015