ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

IoT Middleware for Device Privacy on Big Data

Sallauddin Mohmmad [1], Mohammad Sirajuddin [2] ,Shabana [3]

Assistant Professor, Dept of Computer Science & Engineering, SR Engineering College,Warangal,Telangana,India[1]

Assistant Professor, Dept of Computer Engineering, Vaageswari College of Engineering, Karimnagar, Telangana, India[2]

Assistant Professor, Dept of Computer Science & Engineering, SR Engineering College, Warangal, Telangana, India[3]

ABSTRACT: IoT nothing but billions of internet-connected 'things' will generate massive amounts of data.An increasing number of IoT devices and solutions are able to capture significant amount of information.That information from IoT will drive radical changes in datacenters and will require new Big Data strategies. By having Big Data technologies, organizing and storing large volumes of data has become easier. IoT will be a large number of heterogeneous networked devices, which are producing massive or big data in a detonative fashion. However approaches to deriving insights from such data involve collating large volumes of data for processing. It will creates significant privacy challenges to obtain maximum outcome from IoT ecosystem, we must find ways to derive insights from data generated by IoT devices without violating data subject's privacy.

IoT solutions capture different type of data from different sources. Such type of data been copied into data repositories such as Big Data servers. That data shoud not be available for anyone exept data owner if require. By doing this only the IoT solutions can gain the privacy on Big Data.Each data origin could require different privacy preserving techniques . privacy would become impossible for the data analysts to bare such type of complex Big Data manually. Therefore, we trust that there should be a middleware platform that allows data analysts to target on data analysis and knowledge discovery where the middleware individually handles the usage of privacy-preserving techniques appropriately.

The IoT middleware platform should be able to autonomously link different privacy-preserving techniques in order to support privacy. The ideal IoT middleware should be able to analyse these new data analytical components and examine their potential impact towards privacy of user and where such components can be run ,for example on edge devices or in the Big Data. will focus on developing novel efficient and scalable privacy-preserving algorithms that scale across IoT and Big Data processing technologies such as stream processing systems, SQL/NoSQL datastores and batch processing systems etc.while adapting to uncertain data sizes ,velocity and variety. This will be achieved by exploiting the inherent workload and resource performance features of Big Data processing technology for scaling privacy preserving algorithm.

KEYWORDS: IoT , Big Data , Privacy, Middleware, SQL/NoSQL

I. INTRODUCTION

Big Data refers to large set of complex data, but it isn't wholly about size. Rather, it's defined based on three primary characteristics, also known as the 3Vs: volume, variety, and velocity. Volume relates to the data's size (terabytes, petabytes, or zettabytes)[4]. Variety refers to the type of data and its source (sensors, devices, social networks, the Web, mobile phones, and so on). Velocity means how frequently the data is generated (for instance, every millisecond, second, minute, hour, day, week, month, or year). It is widely believed that cloud computing provides a promising platform for storing and processing Big Data.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

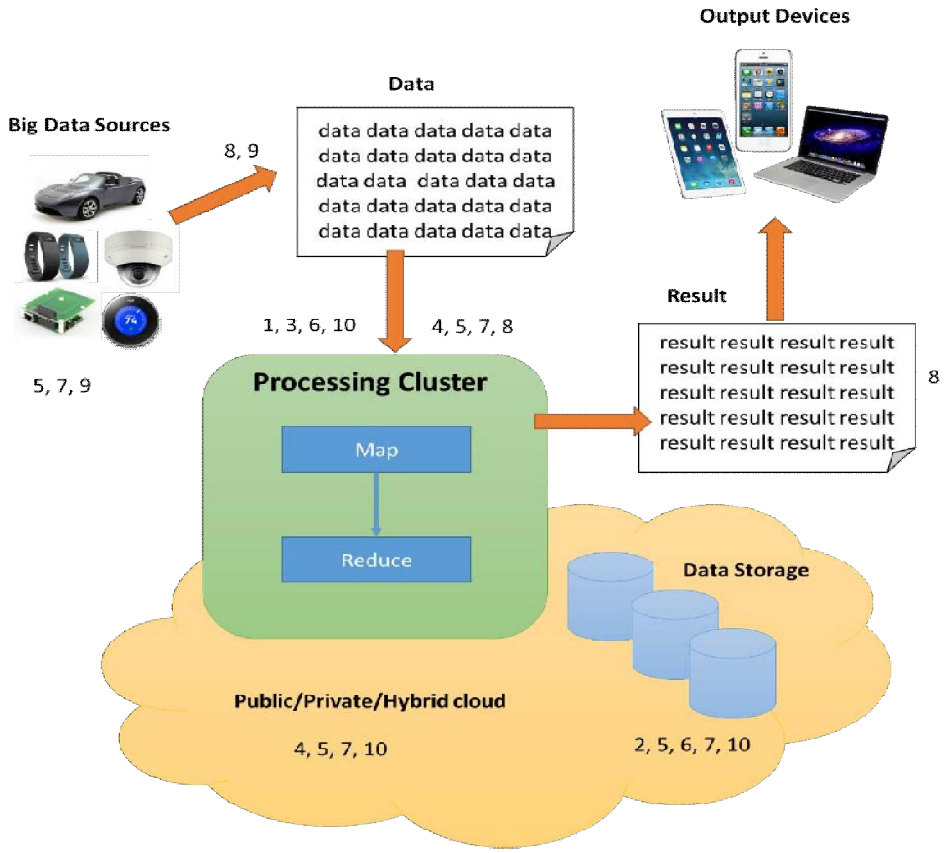
International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Internet of Things (IoT) is a network of networks in which a massive number of objects, sensors, or devices are connected through the ICT infrastructure to provide value-added services. The IoT connects people and things anytime, anyplace, with anything and anyone, ideally using any path or network and any service . By 2020, 50 to 100 billion devices will be connected to the Internet and generating big data for analysis and knowledge extraction.

Even though data collected by individual devices might provide insufficient information, aggregated data from numerous physical devices and virtual sensors can provide a wealth of knowledge for important application areas, including disaster management, customer sentiment analysis, smart cities, and bio-surveillance. Data collection and analysis in IoT applications has many objectives. However, the data collected by smart IoT devices can contain sensitive personal information based on the application type and the data source. Therefore, such data must be managed carefully to avoid any user privacy violations[3]. Here, we briefly discuss the importance of addressing IoT privacy challenges and present survey results that consolidate public opinion towards IoT solutions and their impact on user privacy. We also examine the research challenges that must be addressed for the IoT to become a pleasant experience for users and businesses, and highlight leading research in this field.



It is important to understand that different IoT solutions capture different types of sensor data in different contexts (e.g. households, factories, roads). Some IoT products may capture more private information (e.g. individual customer focused products) and others may capture less private information (e.g. enterprise or industry focused products). The second important fact is that, typically, these IoT products focus on achieving a single objective and data always move within the solution boundaries[1]. Therefore, due to the fact that the data does not leave the product boundaries, the privacy risk related to these products are limited. However, there is a significant amount of useful knowledge and insights that can be derived by combining, processing, and analysing the data collected by different IoT products [4]. It is more valuable if data collected by multiple data owners can be processed together.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

These security and privacy challenges cover the entire spectrum of the Big Data lifecycle sources of data production (devices), the data itself, data processing, data storage, data transport and data usage on different devices.A particular aspect of Big Data security and privacy has to be related with the rise of the Internet of Things (IoT). IoT, defined by Oxford 1 as "a proposed development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data", is already a reality – Gartner estimates that 26 billion of IoT devices will be installed by 2020, generating an incremental revenue of $300 billion (Rivera & van der Meulen, 2014). The immense increase in the number of connected devices (cars, lighting systems, refrigerators, telephones, glasses, traffic control systems, health monitoring devices, SCADA systems, TVs, home security systems, home automation systems, and many more) has led to manufacturers to push to the market, in a short period of time, a large set of devices, cloud systems.

It is clear that Big Data present interesting opportunities for users and businesses, however these opportunities are countered by enormous challenges in terms of privacy and security (Cloud Security Alliance, 2013). Traditional security mechanisms are insufficient to provide a capable answer to those challenges. Connectivity will become in the IoT a kind of commodity,available to all at a very low cost and not owned by any private entity. In this context, there will be the need to create the right situation-aware development environment for stimulating the creation of services and proper intelligent middleware to understand and interpret the information, to ensure protection from fraud and malicious attack (that will inevitably grow as Internet becomes more and more used) and to guarantee privacy.

The IoT middleware platform should be able to autonomously link different privacy-preserving techniques in order to support privacy. The ideal IoT middleware should be able to analyse these new data analytical components and examine their potential impact towards privacy of user and where such components can be run ,for example on edge devices or in the Big Data. Such IoT middleware will eliminate a significant burden on data analysts and it will also reduce the human error that could lead to user privacy violations[10].One major privacy challenge in the IoT is to develop technologies that request consent from users in an efficient and effective manner. This research will need to combine principles and techniques from human- computer interaction and cognitive sciences.

The middleware is defined as a software layer or a set of sub-layers interposed between the technological and the application levels. The middleware architectures proposed in many projects for the IoT often follow the Service Oriented Architecture (SOA) approach. The adoption of the SOA principles allows for decomposing complex systems into applications consisting of an ecosystem simpler and with well defined components. The use of common interfaces and standard protocols is common in such systems. However typical SOAs fail to provide the loose coupling and proper separation between types and instances that are needed in domains that involve "things" (e.g. home automation). For instance two light appliances may offer the same type of service (turning light on and off) but different actual services, if only because they are located in different rooms. These loose coupling and proper separation between types and instances are however well known in Component Based Software Engineering (CBSE) approaches.

II. RELATED WORK

Managing data volumes and providing privacy is an integral part of IoT-middleware. It is believed that there will be trillions of objects which will be part of this enormous network and hundreds of Exabytes will be stored or exchanged among the objects which might be a Big data. explosion of the amount of data collected and exchanged. Therefore it is imperative to get novel methods to find, fetch, and transfer data. Here challenges involve in querying, indexing, process modelling, and transaction handling. These data can be identification data, positional data, environmental data, historical data and descriptive data as presented in. That is why managing these voluminous data is an important module of IoT-middleware. Storage Manager module realizes the persistent storage and administration of information in the middleware. It can integrate any kind of storage into the middleware,address those storages as virtual devices and it stores the data as string. The main constraint of this middleware is that the storage device should also be running the same middleware. On the other hand there is an existence of a RDBMS (Relational Data Base ManagementSystem). The Information Sharing Module of the middleware is responsible for collecting, filtering, storing and extracting queried data from the database. The agents in middleware, as proposed in [11], acquire knowledge by utilizing available data mining algorithms and dynamically reconfigure the data management

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

architecture on the basis of this knowledge. These agents infer (also collaboratively) new configuration plan based on this acquired knowledge. Whereas in [2], storage layer is in-charge of providing and managing persistent storage for data streams. Query processing is done by the Query Manager (QM) which includes the query processor and query repository for efficient management of the data Middleware has been defined as computer software that has an intermediary function between the various applications of a computer and its operating system . In our case, we are interested in middleware that is specifically designed or adapted to provide capabilities for IoT device privacy on Big data process. There are a number of existing surveys of IoT middleware.

We looked at typical IoT middleware such as ISMP ,AURA, ASPIRE GSN , HYDRA, TinyDB,WISeMid etc.some example middleware softwares in IoT are

AURA: One of our objectives in this assignment is to find the possibility of improving the ease of configurations and deployment in an IoT-based system. AURA aims to providehig h-level APIs to interact with each device, which can facilitate device configurations for end-users. AURA middleware‟s aim is relevant to our objectives, so we review its architecture.AURA is a middleware that supports interacting with complex devices (e.g. digital cameras, PDAs, etc.), and their integration. AURA defines a proxy, called personal AURA that enables users to use a device independent of their physical locations.

TinyDB: TinyDB middleware was the first project to propose the idea of abstracting from devices. TinyDB allows end-users to interact with devices without knowing about the details of the devices specification, such as the communication protocols that are supported by these devices. Since we are looking for a way to abstract from details of devices to facilitate interactions with them, this topic can be relevant to our work. TinyDB provides a Domain Specific Language (DSL) for end-users to interact with devices. Its DSL is a query language that supports selection, join, projection, and aggregation to work with an embedded sensing environment. This DSL allows an end user to get information about the time, place, type and method of sampling in an embedded sensing environment.

Hydra: Hydra is a well-known middleware framework for IoT-based system . This middleware covers almost all the functional components. To provide the ease of deployment and configuration, we are looking for a Service Oriented Architecture that interacts with devices in a loosely couple way. The reason is, a loosely couple IoT-based system can support better system maintainability and extendibility in case of handling changes in the type an number of devices. As Hydra is a SOA-based middleware, and supports many required functionalities to support an IoT-based system.

WISeMid:WISeMid is an energy-aware middleware for integrating wireless sensor networks and Internet. In an IoT-based system, saving energy in interaction among devices is important, because they usually have limited power suppliers. Also, IoT-based system is IP-based communication. Therefore, as the WISeMid middleware considers both IP-based communication and energy awareness factors, we review this middleware.

Such kind of all IoT middleware softwares will not support for expected privecy of device on Big Data processing.For example AURA can change its configuration automatically when user tasks or the environment changes. Furthermore, AURA has been designed to provide a platform-independent description of the user‟s tasks that allows the user to use different applications in different locations without changing the configuration. However, the technical details to interact with physical devices are out of the scope of the AURA project. Thus, AURA should not support the ease of deployment in terms of abstracting the format of required data to interact with devices.

Hydra makes an abstraction over devices so an end-user does not need to know the etailed information to configure the devices. Moreover, Hydra ease the deployment process by providing an interface to interact with the considered devices as service providers at deployment time. For devices that do not have a sufficient computing power to be a service provider, Hydra uses a proxy that allows these devices to interact with the Hydra middleware through the IP protocol.

TinyDB is defined to be used together with TinyOS, which is a software suite. It is designed to facilitate the access to the lowest level of hardware in an energy efficient way. TinyDB only supports TinyOS-based devices. Therefore, service deploying in TinyDB depends on the operating system that is supported by the required devices. The end-user needs to know the device specifications before working with devices in TinyDB.

WISeMid focuses on integrating the Internet and wireless sensor network at service level by providing transparency of access. Location and technology. By providing these transparencies, this middleware can provide ease of deploying, because we do not need to have the detail information such as address of sensors to deploy a service.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

To satisfy application requirements and provide ease of configuration and deployment for an IoT based system privacy on Big Data, middleware requires having a uniform way to communicate with different service providers (e.g. devices). Furthermore, single middleware that includes: federated identity (for users and devices), policy-based access control, user managed access to Big Data, enable privacy and security.

.

III. PRIVACY CHALLENGES

Today, consumers of online services are aware that when they use free online services (e.g., email, social networking, and news feeds), they automatically become the data sources of the business, who can analyse this data to improve customer satisfaction. Even worse, the data can be sold to third party for further analysis. However, in the future IoT era it is likely that service providers will adopt one of the two following models[2]. First, some consumers may willingly pay for consuming the services with the aim of protecting their privacy. Second, some consumers may offer to give away data, of course under some limitations and conditions, in return for consuming services free of any charge.

Data collected through smart wearable and smart home devices can be used to generate contextually [2] enriched information. Device owners should remain in charge of such data at all- time despite they may give access to their data to external parties temporarily in order to accomplish a specific task. Consequently, the IoT era poses significant privacy challenges, especially due to sheer scale of the IoT. The EU Commission report on the IoT, CERP-IoT [10], has identified security and privacy as a major IoT research challenge, including privacy preserving technology for heterogeneous device sets on Big data, models for decentralised authentication, trust, energy-efficient encryption, data protection technologies, security and trust for cloud computing, data ownership, legal and liability issues, repository data management, access and use rights, rules to share added value, responsibilities, liabilities, artificial immune systems solutions for IoT, secure, low cost devices, integration into, or connection to, privacy preserving, frameworks, and privacy policies management. In the subsequent text, we introduce and discuss some of the major IoT privacy challenges on Big data [15]. A summary of research questions are presented in the Supplemental Material section.

3.1.USER CONSENT ACQUISITION: In the IoT, user consent is about acquiring the required level of permission from the users and non-users who are affected by the devices or services. In the traditional Web, the method of receiving user consent is through the privacy terms and policies presented to the users through paragraphs of long text. Recently, with the emergence of social media and mobile apps, consent acquiring mechanisms have changed. Researchers [9] have found that the current methods of asking user consent in social media platforms, such as Facebook are ineffective and most of the users underestimate the authorization given to the third party applications. In some cases, developers may not provide accurate information to the users for the consenting decision. In other cases, developers may provide accurate information.however, the users would be unable to understand exactly what the consent entails for the lack of technical knowledge. One of the major privacy challenges in the IoT is to develop technologies that request consent from users in an efficient and effective manner. This is a challenging task due to the fact that every user has very limited time and limited technical knowledge to engage in the process. Such research will need to combine principles and techniques of the human computer interaction and cognitive sciences. Control, Customization, and Freedom of Choice: In the IoT, the data owner must have full control on data, allowing the users to delete or move data from one service provider to another at any time.

3.2.Anonymity Technology: Network communication interfaces typically have MAC addresses that can be used to trace back the data communication paths. The combination of multiple MAC addresses of multiple devices will help create unique fingerprints and a unique profile where analytics can be used to extract knowledge. Consequently, user location can easily be tracked. It is important to discover new technologies that can anonymize data communication paths to protect user privacy. Due to the usage of large number of sensors and service, it is challenging to anonymise multi- dimensional data. Specially, it is easy to build fairly unique profiles that may enable knowledge extraction for a particular user. Currently, the network communication technologies do not preserve the anonymity of the users. Newer IoT platforms will be required to adopt technologies, such as Tor (torproject.org) that is a technology that conceals user location. In essence, a comprehensive anonymization framework is required to facilitate end-to-end anonymity in the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

IoT. Such a 4framework must ensure anonymity at different levels, such as data modelling, storage, routing, communication, analytics, and aggregation.

3.3.Security: Even though a detailed discussion on IoT security [12] is out of the scope this article, it is important to mention that standardization and certification would be the foundation of security. Moreover, all of the stakeholders have the responsibility to secure the infrastructure, the data collection and transfer process, as well as the people using the devices. Device manufactures will need to upgrade or patch the firmware and software. Moreover, such updates must be pushed onto the devices and must be automatically installed with minimum user intervention. It may also be the owner responsibility to make sure that their IoT devices and software systems remain up-to-date. Security need to be ensured throughout the data flow within the IoT.

The major security problem of IoT is related to authentication and data integration. To do the authentication, we need data exchange between authentication servers and devices. This makes a problem when an application use passive RFID tags in an IoT-based system, because a passive RFID does not have the capability of handling many communications with an authentication server. This problem has not been solved yet .IoT Middleware platform has some critical functionalities, such as aggregating and filtering the received data from the hardware devices, performing information discovery,providing access control and privacy to the devices for applications on small data set.Such tool HYDRA,AURA, TinyDB,WiseMID are provided user privacy with minimum overhead on Big Data.Better achievemet of user privacy of IoT systems on big data can't possible by existing Tools.Existing technologies and regulations are not sufficient to support a privacy-preserved Big Data management life cycle.

IV. PRIVACY THREATS

The evolving nature of the IoT regarding technologies and features as well as the emerging new ways of interaction with the IoT lead to specific privacy threats and challenges. This section presents our classification of those threats.

4.1 Identification

Identification denotes the threat of associating a (persistent) identifier, e.g. a name and address or a pseudonym of any kind, with an individual and data about him. The threat thus lies in associating an identity to a specific privacy violating context and it also enables and aggravates other threats, e.g. profiling and tracking of individuals or combination of different data sources. The threat of identification is currently most dominant in the information processing phase at the backend services of our reference model, where huge amounts of information is concentrated in a central place outside of the subject's control. In the IoT also the interaction and collection phase will become relevant, as the impact of the volving technologies and interconnection and interaction features aggravates the threat of identification.For example surveillance camera technology is increasingly integrated and used in non-security contexts, e.g. for analytics and marketing . As facial databases (e.g. from Facebook) become available also to non-governmental parties like marketing platforms [12], automatic identification of individuals from camera images is already a reality.The increasing (wireless) interconnection and vertical communication of everyday things, opens up possibilities for identification of devices through fingerprinting. It was recognized already for RFID technology that individuals can be identified by the aura of their things [11]. speech recognition is widely used in mobile applications and huge data-bases of speech samples are already being built. Those could potentially be used to recognize and identify individuals, e.g. by governments requesting access to that data [2]. With speech recognition evolving as a powerful way of interaction with IoT systems (Table I) and the proliferation of cloud computing for processing tasks, this will further amplify the attack vector and privacy risks.

Identity protection and, complementary, protection against identification is a predominant topic in RFID privacy , but has also gained much attention in the areas of data anonymization ,and huge data privacy-enhancing identity management . Those approaches are difficult to fit to the IoT: Most data anonymization techniques can be broken using auxiliary data, that is likely to become available at some point during the IoT evolution. Identity management solutions, besides relying heavily on expensive crypto operations, are mostly designed for very confined

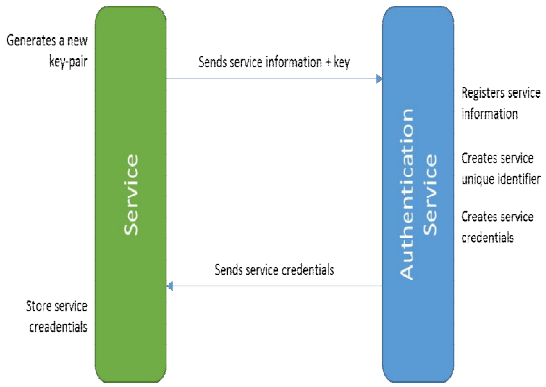
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

environments, like enterprise or home networks and thus difficult to fit to the distributed, diverse and heterogeneous environment of the IoT.



4.2. Localization and Tracking

Localization and tracking is the threat of determining and recording a person's location through time and space. Tracking requires identification of some kind to bind continuos localizations to one individual. Already today, tracking is possible through different means, e.g. GPS, internet traffic, or cell phone location. Many concrete privacy violations have been identified related to this threat, e.g. GPS stalking [8], disclosure of private information such as an illness [5], or generally the uneasy feeling of being watched [3]. However, localization and tracking of individuals is also an important functionality in many IoT systems. These examples show that users perceive it as a violation when they don't have control over their location information, are unaware of its disclosure, or if information is used and combined in an inappropriate context.

4.3.Privacy-violating interaction and presentation

This threat refers to conveying private information through a public medium and in the process disclosing it to an unwanted audience. It can be loosely sketched as shoulder-surfing but in real-world environments.Many IoT applications, e.g. smart retail, transportation,and healthcare, envision and require heavy interaction with the user. In such systems, it is imaginable that information will be provided to users using smart things in their environment e.g. through advanced lighting installations, speakers or video screens. Vice versa, users will control systems in new intuitive ways using the things surrounding them, e.g. moving, touching and speaking to smart things.This becomes a threat to privacy when private information is exchanged between the system and its user.

4.4. Inventory attack

Inventory attacks refer to the unauthorized collection of information about the existence and characteristics of personal things. With the realization of the All-IP and end-to-end vision, smart things become query-able over the Internet. While things can then be queried from anywhere by legitimate entities (e.g. the owner and authorized users of the system), non-legitimate parties can query and exploit this to compile an inventory list of things at a specific place, e.g. of a household, office building, or factory. Even if smart things could distinguish legitimate from illegitimate queries, a fingerprint of their communication speeds, reaction times and other unique characteristics could potentially be used to determine their type and model. With the predicted proliferation of wireless communication technology, fingerprinting attacks could also be mounted passively, e.g. by an eavesdropper in the vicinity of the victim's house. Since inventory attacks are mainly enabled by the increasing communication capabilities of things, the threat arises in the information collection phase of our reference model.

V. CONCLUSION

In existind system IoT Middleware platform has some critical functionalities, such as aggregating and filtering the received data from the hardware devices, performing information discovery,providing access control and privacy to the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

devices for applications on small data set.Such tool HYDRA,AURA, TinyDB,WiseMID are provided user privacy with minimum overhead on Big Data.Better achievemet of user privacy of IoT systems on big data can't possible by existing Tools.Existing technologies and regulations are not sufficient to support a privacy-preserved Big Data management life cycle.

We consider that profiling remains one of the most severe threats: Our analysis shows that it is greatly aggravated and that other threats like identification or tracking, though each provoking different very specific privacy violations, add to its dangers by supplying even more linkable data. At the same time, business models that depend heavily on profiling have enjoyed tremendous success and so the trend for big data continues, fueled by the IoT's central promise for fine-grained and ubiquitous data collection. Here, the challenge consists in designing privacy-aware solutions for the IoT that allow to balance business interests and customers' privacy requirements.

We also consider privacy-violations in the interaction and presentation phase an important future threat, because of the corresponding interaction mechanisms with smart things and systems that are just evolving and are rather unique to the IoT. The involved technical challenges have hence received little attention in the related work so far and require new ways of using technology as well as a fair amount of foresight and sensitivity for privacy implications.

Future research efforts will focus on developing novel efficient and scalable privacy preserving algorithms that efficiently scales across IoT data processing technologies (SQL/NoSQL datastores, batch processing systems, and stream processing systems) while adapting to uncertain data sizes and data variety. This will be achieved by exploiting the inherent workload and resource performance features of big data processing technology for scaling privacy preserving algorithms.Therefore, we trust that there should be a middleware platform that allows data analysts to target on data analysis and knowledge discovery where the middleware individually handles the usage of privacy-preserving techniques appropriately.

REFERENCES

[1] L. Atzori, A. Iera and G. Morabito, "The Internet of Things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787-2805, #oct# 2010.
[2] C. Perera, A. Zaslavsky, P. Christen and D. Georgakopoulos, "Context Aware Computing for The Internet of Things: A Survey," Communications Surveys Tutorials, IEEE, vol. 16, no. 1, pp. 414-454, 2013.
[3] A. Zaslavsky, C. Perera and D. Georgakopoulos, "Sensing as a Service and Big Data," in International Conference on Advances in Cloud Computing (ACC-2012), Bangalore, India, 2012.
[4] C. Eaton, D. Deroos, T. Deutsch, G. Lapis and P. Zikopoulos, Understanding Big Data, McGraw-Hill Companies, 2012.
[5] D. Miorandi, S. Sicari, F. D. Pellegrini and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks , vol. 10, no. 7, pp. 1497-1516, 2012.
[6] R. Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms," Xamax Consultancy Pty Ltd, 21 October 2013.
[7] G. Danezis, J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. L. Métayer, R. Tirtea and S.Schiffner, "Privacy and Data Protection by Design - from policy to engineering," EuropeanUnion Agency for Network and Information Security (ENISA), Crete, 2014.
[8] Evans D. The Internet of Things - How the Next Evolution of the Internet Is Changing Everything.CISCO white paper 2011;
[9] David K, Jefferies N. Wireless visions: A look to the future by the fellows of the wwrf. Vehicular Technology Magazine, IEEE dec 2012;
[10] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," Computer Networking, vol. 54, no. 15, 2010.
[11] J. Rodin in the foreword to B. Katz, J. Bradley, The Metropolitan Revolution: How Cities and Metros Are Fixing Our Broken Politics and Fragile Economy. (Brookings Institution Press, Washington DC, 2013).
[12] RetrievedfromAgrawal, D., Das, S., & El Abbadi. Big data and cloud computing. In Proceedings of the 14thInternational Conference on Extending Database Technology - EDBT/ICDT '11 (p. 530). New York,New York, USA: ACM Press.2011.
[13] H. Ulusoy et al. "Vigiles: Fine-Grained Access Control for MapReduce Systems,",International Congress on Big Data (BigData Congress) pp.40-47 2014 IEEE.
[14] d. boyd, K. Crawford, Critical Questions for Big Data, Information, Communication and Society 15: 662-679 (2012).