Privacy Agents for IoT Cloud Communication

Syed Khuram Shahzad, Muhammad Waseem Iqbal and Nadeem Ahmad
The Department of Computer Science & Information Technology, The University of Lahore, Lahore, Pakistan

Keywords: Privacy, Trust, Internet of Things, Agents, IoT Architecture.

Abstract: Internet of Things (IoT) has been shaped to a phenomenon from some technical framework. The smart environment based on IoT has been introduced by the construction of smart cities, offices, universities and factories. These smart environments consist of smart devices replacing simple appliances from our home and workplaces. With this interconnected environment we are connected, accessible and smartly managed through intelligent systems. These intelligent systems work on our personal, historical and current data. This data sharing brought new challenges of the privacy preservation of individuals living in this smart world. This paper provides a study of the issues related to the data sharing through these smart devices over service providing cloud. It proposes communication architecture by introducing an intermediate layer of data sharing control consisting of privacy agents. It also includes a methodology to define a customized privacy policy for different personal properties within different business models.

1 INTRODUCTION

The era has been bringing in smart device in our daily life replacing simple electronic device. These smart devices are no longer independent stand alone household item but it is a part of bigger network named Internet of Things (IoT). The IoT can use any medium or solution to communicate over network like tagging (RFID, NFC etc.), embedded smart service capabilities like smart phones or smart TV. All variants of technical applications of smart device have common function of being identified by unique ID, communication over networks and capability of acquiring services from network servers. Moreover they form household and business infrastructures of smart environment. IoT has become the part of daily life even household appliances are forming household network of the smart devices (Chamberlain, 2016). There are very common examples of tracking, GPS facility in vehicles and video on-demand and other entertainment facilities at home (Crabtree, 2016). With facilitation the information and service sharing, the smart environment brings new challenges of personal privacy assurance in data sharing. The more we use IoT for personal and domestic purpose, the more we share our personal information over this network. This paper discusses the privacy threats in communication between personal smart devices and cloud environment. It suggests a mediatory layer for privacy preservation and access control with defined privacy and trust policy. The next section of this paper provides a summarized view of historical work and problem identification. The methodology states the privacy matrix, the privacy preservation agents and overall architectural view. The model provided in methodology is discussed by implementing at three different scenarios in the section of discussion over business model. The conclusion and future work is provided in the last section of the paper.

2 LITERATURE REVIEW

IoT is understood as a world of objects connected with each other. Radio Frequency Identification (RFID) and sensor network technologies will be used normally for collecting information from surrounding environment (Gubbi, 2013) (Sundmaeker, 2010) (Al-Sakran, 2015). In 2020, it is estimated that there will be around 26 billion units connected together in IoT. The Cisco Company claimed in a study, that smarter cities will produce $1.9 trillion value from IoT (Bradley, 2015). The massive data will produce new challenges for personal security and privacy. IoT, usually, has limited processing and storage capacity with some

Shahzad, S., Iqbal, M. and Ahmad, N.
Privacy Agents for IoT Cloud Communication.
DOI: 10.5220/0006286502390245
In *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017)*, pages 239-245
ISBN: 978-989-758-245-5

challenging issues like reliability, security, privacy and performance. The integration of IOT with cloud will expand the processing and storage capacity over the network. The Cloud will also benefit from IoT by delivering extensive services in more distributed manner (Babu, 2015). Considering the privacy issue, there are efforts under go to reduce the privacy threats some of the researches talk about providing privacy layers in communications like gateways (Medaglia, 2010) or rule mining for information sharing from household networks (Crabtree, 2015).

2.1 Privacy Issues

Whenever there is discussion over IoT the privacy is listed at the top from introduction of RFID to latest research (Henze, 2014). The threats to the privacy are being revealed in many forms and levels like data storage, ownership, communication protocols, access control to the identification attribute and trust in legal and technical terms (Perera, 2015) (Ziegeldorf, 2014). Consequently many solutions are proposed for respective privacy threats (Alpár, 2016). Here we focus on the data sharing over IoT cloud communication. Researchers have defined two major techniques for access control and data sharing while communication at IoT. The first method is to provide an intermediate layer for privacy control between device and public cloud including severs & other devices (Williams, 2014), while the second method talks about attribute level authentication for different devices and users (Aazam, 2014). The first methods providing the privacy layer doesn't look deep for the service request and attributes shared that can block some service acquisition. It is focused at the trust policy development for information sharing over public network. The second method provides too much technical details to be managed by the end user. This methodology talks about the individual privacy policy (Kozlov, 2012). Here we need a trade off approach which can not only facilitate user for managing all the attribute level access control but also assist them to perform the task. Here we argue that the trust policy and privacy policy should not be detached from each other. The distance between these two policies can bring unwanted results or they are not workable together. So it is required that the trust policy should have capacity to imply the rules defined at user level in his privacy policy.

2.2 Web Trust Models

Privacy over any network has been an issue since the birth of network. Privacy is the concern related to the unauthorized or harmful access of data even at standalone device (Cranor, 1999) (Rubin, 1998) (Grandison, 2001) (Glen, 2000). Within a network environment the threat has been strengthen due to connected environment allowing access to any machine form any remote site. Many privacy and trust models have been developed in early 90s for World Wide Web (WWW). The privacy models avoid any unauthorized access by providing security layers at the data sent to WWW. While on the other hand the trust models provide the ranking and validation of all trusted destinations over internet. This ranking of the internet node, including websites and servers nodes, describes the assurance model to the privacy (Grandison, 2001) (Glen, 2000). Similar trust models developed and applied for IoT (Sicari, 2015). We have adopted the same model for ranking the service providers over cloud to share the required information with service requests. Considering the available trust models for IoT, The ranking methodology and technical details are not discussed in the current writing. These ranking enable the device and privacy engine to determine the secure destination to share any kind of information with minimum privacy threat.

3 METHODOLOGY

To resolve the problems of privacy and personal information sharing, we introduced network architecture with a privacy layer. It is not possible to disconnect the person from smart environment or create total new replica for privacy issues. This can control the access of shareable and non-shareable attributes of requesting device from cloud. This filtration and access identification is achieved through a classification of all device properties. The classification schema is part of request-response protocol of smart device-cloud communication (Smart net). It will assist user to categorize all the properties while default classes and categorized list with complete privacy policy will be provided by the device at initial installation while user can change them according to their needs.

3.1 Privacy Matrix

Here we develop a matrix of all device properties shared over smart net while rendering any services. We have developed few classification and ranking mechanism to limit a risky and unnecessary sharing of personal information. We have made

classification of different personal information that need to be shared over web. The provided classification list some basic classes while it can be enhances by introducing new classes at same level or vertically by subclasses. This privacy matrix provides a table to develop a privacy policy at user level (Mattern, 2010). On the other has the privacy layer between devices and cloud keeps the trust policy defining trusted, blacklisted and public node over cloud.

3.1.1 Personal Identification Properties (PIP)

These properties include the information that can be used for identification of persons that smart device is belonged. It includes the identification of person or business at whose name the device is registered. This information is required for some contractual matters like purchase and maintenance contracts. It includes name, date of birth, social security number or taxation identification. There are some business properties similar to personal information or defined as subclass that list also some other business values like buyer's Credit Card details at purchasing a mobile phone contract, Driving License information of smart car owner (Santucci, 2010). At current model these are considered as PIP.

3.1.2 Location Properties

These are properties that can be used to trace a device in terms of spatial measures. It may be static values of street address or dynamic latitude, longitude measurements.

3.1.3 Device Properties

These properties include properties related to the device it includes static device identification properties or variant of device status properties. Device identification properties include, brand, model and serial number, while the status properties include the working status of the device like OS, networks, storage application installed etc (Mattern, 2010) (Santucci, 2010) (Medaglia, 2010).

In current framework, we have attached the properties classification module with the device. Considering the properties classification an access control protocol has be devised for sharing these properties over cloud. The properties from the privacy matrix is hidden, shared or replicated by soft identities from the requested servers.

3.2 Trust Points and Ranking Cloud Nodes

The properties classification is not enough to make an automated decision mechanism for information sharing over cloud. It is also depends at the trust policy of smart net. The policy also ranked the servers and other nodes over web as simple public server, trusted server and blacklisted servers (Weber, 2010).

The privacy agent can rank (in a ranking table) some clouds nodes as trusted servers based on signatures, user ranking and other factors. All the servers of private network associated to the device and privacy agent will be ranked as trusted server.

All the unranked cloud service providing nodes can be treated as public servers.

The privacy agent may create a list of black listed servers to avoid any service request to be sent there.

3.3 Privacy Layers

Once the attributes of personal information are categorized and servers are ranked, the Privacy Layer model is formed to map the property classes to the ranked server. These layers define the access level according to the property classification and trust ranking of servers as shown in Table 1. The higher level of trust we define the more access privileges will be provided for the property classes. These privacy layers spans from the device to black listed nodes over cloud, mapping full access to all property classes to no access at all respectively. The first layer is defined as the device layer, residing at the device level. All properties belonged to any of above defined class in can be accessed and used at this level. Further user level access protocols (Admin, Power user, Operator etc.) can be defined at device level. We have not established any user level privacy that is mostly defined with the smart device. All of the properties categorized as private, stay within device layer and never shared over network. Majority of the physical properties of devices like some of the personal identification or device identification properties are limited to this level and never shared to the network.

The layer above device layer is defined as local network layer. This layer includes all the nodes device registered at the agent forming a local network. Information like local IP, identification properties stays within the local network (LAN). While the privacy agent may produce some soft identities for the properties required to request a

service from any node above LAN. The local network level information sharing is done with a smart environment developed in small residential or business areas.

The third level of access is the private network (VPN) layer. It can be created for some environment for specific smart enterprise over cloud. This private network includes all agents and server nodes for all devices registered to the enterprise network. Mostly the business information is shared over this level. While rendering service out of the private network may define some other soft identities for these business properties (Weber, 2010).

There may exist some other trusted node or servers over cloud based on signatures and user ranking other than the private network. The next access layer Trusted Nodes Layers that allow of requesting these nodes and provided access to the provided attributes.

Table 1: Access Layers.

Access Layer	Access Level (0 - lowest)
Device Layer	5 (Full Access)
Local Network Layer	4
Private Network (VPN) Layer	3
Trusted Network Layer	2
Cloud Layers	1
Blocked Layer	0 (No Access)

The top most level of access is the public cloud layer. It includes all trusted and public server at which a service request can be sent. Only the attributes categorized as public or soft identities can be shared over this layer.

These access layers protocols excludes black-listed server while there will no request sent to these server or cloud nodes. A Blocked Layer may be created for all black listed that can be an invisible layer for communication.

The device layer and blocked layer have defined access to all properties. All intermediate layers may vary access level with the context including service types and business model defined in the discussion section. All the attributes are tagged with that authorization level while none of the attributes can be tagged with blocked layer access. The complete model including properties classification, network nodes ranking an associated privacy layers provide a platform to build a privacy matrix for any device or group of devices. Quantification of the privacy matrix provides us a privacy policy for each device or group of devices. The access level tags can be associated with individual of attributes or any defined class of attributes according to the privacy policy. Moreover soft-identities with higher access level can be used replacing all identification properties to provide access to most levels of cloud layers (Friess, 2013).

3.4 Privacy Agents

The agent is somewhat intelligent that make it similar to a privacy server while the smart devices act like a client. There is no explicit privacy request and response protocol adopted but the privacy agent provides services of proxy, gateway (Medaglia, 2010) and domain controlling enabling it to work as server for the local network. This component of the communication architecture is the backbone of whole privacy preservation model designed in current study. It also ensures the privacy by sharing information over network according to the defined privacy policy for each request sent from device to cloud.

3.4.1 Agents Components

The privacy agent has three major types of components as shown in Figure 1.

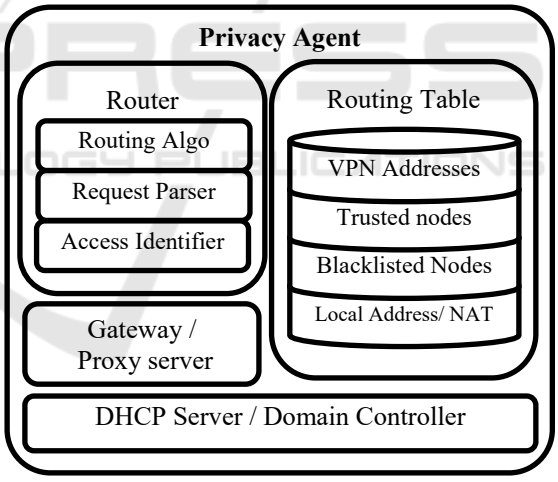

Figure 1: Components of Privacy Agent.

Network related components enable this agent to register all devices as local network with domain controlling protocols. The component above local network management component is used for request analysis and access identification.

The next component is used to routing the request to the server or cloud layer according to specified access. This component is somewhat intelligent using simple decision tree mechanism based on the least access level provided with the

updated request with all required attributes either original values or soft-identities

The third component is the database in conventional filing system with specific indices storing routing tables. The access controller identifies access of all properties and attributes by the associated access level tags with them. These attributes are tagged at client level by the device.

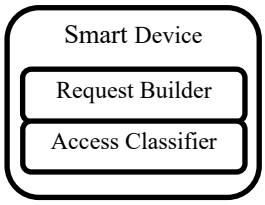

Figure 2: Privacy components in Smart Device.

Here we have established the Access classifies and request builder component to tag the attributes and build the service request respectively. Figure 2 provide the components of the smart device. These components reside just before the communication layer of smart devices. The attributes access classification vary based on the business model and service types, e.g. for some security services the location properties may be tagged as local network level access while same properties may be defined public for location based service requests (Babar, 2010).

3.4.2 Network Architecture

With the detailed description of privacy agents and privacy matrix the network architecture explanation will provide whole concept and working of proposed privacy framework. Here Figure 3 provides an overview of the network including a privacy layer. The bottom layer is the local network layer of smart devices registered to a privacy agent. The privacy agents collectively form a privacy layer. Above that the privacy layer, privacy agents connect the devices with service cloud with specified authorization and access privileges. The cloud resides as the top layer consisting of all kind of server nodes and defined VPNs. These server nodes are presented in Figure 3 as Trusted Node (TN), Public Node (PN) and Blacklisted Nodes (BN). These layers forms different level of access as described in privacy layers based on trust level.

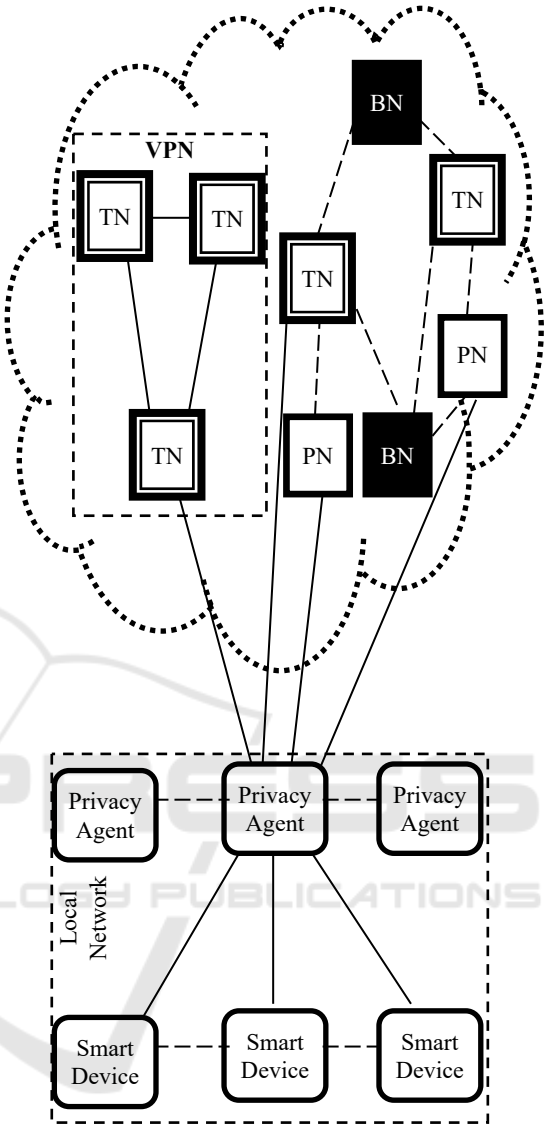

Figure 3: The IoT Cloud Architecture with Privacy Layer.

4 DISCUSSION OVER BUSINESS MODELS

The explored framework of the research has been applied for three basic business models.

The first model defines the Service Based Privacy Agent. These agents are connected to all service provider of similar services like Security services, Health services, location based service etc. With the specialized agents, the classification of properties is done depending of the need of service. If an agent is specialized for location based service

location properties must be required to share with the servers. This business model use mostly trusted servers and server ranking by the users. In the current scenario the devices are registered over these privacy agents irrespective of device location and other association. Thus these privacy agents or are also ranked by the users with history and their profiles. This scenario is described in Figure 3 with all server nodes (trusted and public nodes) without forming any VPN.

Next two business models use a VPN as a private cloud based on either location or enterprise. The second model defines all the access privileges over a VPN based on a location, where privacy agents are associated with any location e.g. a locality or town. In experimentation we have developed one for a model residential scheme. The idea is to have privacy agents for some smart environment a campus, city etc. where the residents of the locality use provided locality services.

The third business model provides maximum access mostly at the VPN of a specific enterprise over cloud. It uses an Enterprise Privacy Agent currently this architecture is mostly used for smart communication devices. It provides access and authentication agents for brand specific devices or applications. These enterprises have created their own cloud service like Google, SAMSUNG, SIEMENS and IBM. Other than device manufacturing devices, there are service providing organizations that have built their own cloud architecture like Amazon. The majority of the information floats through their specific VPN, while rendering a third party service there is an access control protocol required. Only few public defined attributes or alternative soft-identities are floated with the services request outside the VPN.

There may be some other hybrid approaches of enterprise agents and service specific agents, with any organization provide specific kind of services through their own cloud or user registers at different enterprise agents for different kind of services to get improved quality of services.

5 CONCLUSION AND FUTURE WORK

The problem described earlier was not questioning all the privacy issues but only the information sharing over cloud via service request. The answer was found by development of an intermediate privacy layer with a trust policy and user defined privacy policy at device level. It provides the merger of two method intermediate layer induction and attribute level access control. Default access control policies and device attributes classification can be provided with the deployment of the device to assist user at initial configuration. Moreover it enabled the smart environment to develop uniform privacy matrix for the uniform context like a specific smart enterprise, smart campus or smart residential block with similar devices and user needs. This research still have many privacy question unanswered like security measures (Medaglia, 2010) during communication e.g. data & request encryption methods, legal standings and binding of the privacy providing agents. These and many other questions are needed to answer in the future work. We will continue our work in these directions. It is also possible to define intelligent privacy agents by defining dynamic the privacy matrix, history enabled profiling of cloud nodes etc.

ACKNOWLEDGEMENTS

This contribution is presented with the acknowledgements of the Higher Education Commission of Pakistan (HEC). HEC is the higher education organizing body that has funded this research contribution presentation.

REFERENCES

Chamberlain, A., Crabtree, A., 2016. Searching for music: understanding the discovery, acquisition, processing and organization of music in a domestic set-ting for design. In *Personal and Ubiquitous Computing*, 20 (4), pp. 559–571.

Crabtree, A., Lodge T., Colley, J., Greenhalgh, C., Mortier, R., Haddadi H., 2016. Enabling the new economic actor: data protection, the digital economy, and the Databox, In *Personal and Ubiquitous Computing*, pp. 1–11.

Crabtree A., Rodden, T., Tolmie, P., Mortier, R., Lodge, T., Brundell, P., Pantidi, N., 2015. House Rules: The collaborative nature of policy in domestic networks, In *Personal and Ubiquitous Computing*, 19(1), pp. 203–215.

Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M., 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. In *Future Generation Computer Systems*, 29(7), 1645–1660.

Sundmaeker, H., Guillemin, P., Friess, P., Woelfflé, S., 2010. Vision and challenges for realising the Internet of Things. In *Cluster of European Research Projects on the Internet of Things*, European Commission.

Al-Sakran, H. O., 2015. Intelligent traffic information system based on integration of Internet of Things and agent technology. In *International Journal of Advanced Computer Science and Applications (IJACSA),* 6(2), 37–43.

Bradley, J., Reberger, C., Dixit, A., Gupta, V., 2013. Internet of everything: A 4.6 trillion public sector opportunity. In *Cisco White Paper*. CISCO Corp.

Babu, S. M., Lakshmi, A. J., Rao, B. T., 2015. A study on cloud based Internet of Things: Cloud IoT. In *Global Conference in Communication Technologies (GCCT)*, pp. 60–65. IEEE.

Henze, M., Hermerschmidt, L., Kerpen, D., Häußling, R., Rumpe, B., Wehrle, K., 2014. User driven privacy enforcement for cloud based services in the internet of things. In *International Conference on Future Internet of Things and Cloud (FiCloud),* pp. 191–196. IEEE.

Perera, C., Ranjan, R., Wang, L., Khan, S. U., Zomaya, A. Y., 2015. Big data privacy in the internet of things era. In *IT Professional*, 17(3), pp. 32–39.

Alpár, G., Batina, L., Batten, L., Moonsamy, V., Krasnova, A., Guellier, A., Natgunanathan, I., 2016. New directions in IoT privacy using attribute based authentication. In *Proceedings of the ACM International Conference on Computing Frontiers,* pp. 461–466. ACM.

Williams, J., 2014. Internet of Things: Science Fiction or Business Fact?. In *Harvard Business Review Analytic Services Report.*

Aazam, M., Khan, I., Alsaffar, A. A., Huh, E. N., 2014. Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved. In *Proceedings of 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan,* 14th-18th January, pp. 414–419. IEEE.

Kozlov, D., Veijalainen, J., Ali, Y., 2012. Security and privacy threats in IoT architectures. In *Proceedings of the 7th International Conference on Body Area Networks*, pp. 256–262. Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering (ICST).

Weber, R. H., 2010. Internet of Things–New security and privacy challenges. In *Computer Law & Security Review,* 26(1), 23–30.

Mattern, F., Floerkemeier, C., 2010. From the Internet of Computers to the Internet of Things. In *From active data management to event based systems and more,* pp. 242–259. Springer Berlin Heidelberg.

Friess, P., 2013. *Internet of things: converging technologies for smart environments and integrated ecosystems*. River Publishers.

Babar, S., Mahalle, P., Stango, A., Prasad, N., Prasad, R., 2010. Proposed security model and threat taxonomy for the Internet of Things (IoT). In *International Conference on Network Security and Applications*, pp. 420–429. Springer Berlin Heidelberg.

Santucci, G., 2010. The Internet of Things: Between the Revolution of the Internet and the Metamorphosis of Objects. In *Harald Sundmaeker, Patrick Guillemin, Peter Friess, Sylvie Woelfflé Vision and Challenges for Realising the Internet of Things,* Cluster of European Research Projects on the Internet of Things (CERP- IoT).

Medaglia, C. M., Serbanati, A., 2010. An overview of privacy and security issues in the internet of things. In *The Internet of Things*, pp. 389–395. Springer New York.

Ziegeldorf, J. H., Morchon, O. G., Wehrle, K., 2014. Privacy in the Internet of Things: threats and challenges. In *Security and Communication Networks,* 7(12), 2728–2742.

Cranor, L. F., 1999. Internet Privacy. In *Communications of the ACM*, 42(2), pp 29–31.

Rubin, A. D., Daniel E. Geer Jr., 1998. A Survey of Web Security. In *IEEE Computer,* pp 34–40.

Grandison, T., Sloman, M., 2001. A Survey of Trust in Internet Applications. In *IEEE Communications Surveys and Tutorials,* 3(4), pp 2–16.

Glen, L., Urban, F. S., William, J. Q., 2000. Placing Trust at the center of your internet strategy. In *Sloan Management Review*, 42 (1), pp 39–48.

Sicari, S., Rizzardi, A., Grieco, L. A., Coen-Porisini. A., 2015. Survey Paper Security, privacy and trust in Internet of Things: The road ahead. In *Computer Networks,* 76, 146–164.