REFERENCE ARCHITECTURES FOR PRIVACY PRESERVATION IN CLOUD-BASED IOT APPLICATIONS
(EXTENDED VERSION OF 7398 AT MS 2014)

Ivor D. Addo, Sheikh I. Ahamed
Marquette University
Milwaukee WI, USA
{ivor.addo, sheikh.ahamed}@marquette.edu

Stephen S. Yau, Arun Buduru
Arizona State University
Tempe AZ, USA
{yau, arunbalaji.buduru}@asu.edu

Abstract
As the promise of the Internet of Things (IoT) materializes in our everyday lives, we are often challenged with a number of concerns regarding the efficacy of the current data privacy solutions that support the pervasive components at play in IoT. The privacy and security concerns surrounding IoT applications often manifests themselves as a threat to end-user adoption and negatively impacts trust among end-users. In this paper, we present a reference software architectures for building cloud-enabled IoT applications in support of collaborative pervasive systems aimed at achieving trustworthiness among end-users in IoT scenarios. We describe a case study that leverages this reference architecture to protect sensitive user data in IoT application implementation. We then evaluate the response data from our end-user survey. In addition we present a Secure, Private and Trustworthy protocol (named SPTP) that was prototyped for addressing critical security, privacy and trust concerns surrounding mobile, pervasive and cloud services in Collective Intelligence (CI) scenarios. We present our evaluation criteria for the proposed protocol, our results and future work.

Keywords: Software Reference Architecture, Cloud-Enabled Service Privacy and Security, Internet of Things, Collective Intelligence

1. INTRODUCTION

Trends pertaining to the use of the Internet of Things (IoT) to collaboratively solve complex problems in healthcare monitoring, online web site advertising, and smart home implementation scenarios, among others, are expected to continue to grow rapidly. Nonetheless, one of the most critical deterrents to mainstream user adoption of IoT systems is a looming distaste for how data privacy is enforced among the various collaborative systems at play in IoT applications. Beyond the privacy and security concerns encircling IoT systems, it is becoming more and more inevitable for pervasive collaborative devices to leverage web services for data sharing and communication to backend storage systems. With the advent of cloud computing, it is not uncommon for the mobile services that these pervasive devices communicate with, to be hosted in the cloud. Consequently, with the imminent domain-specific privacy and security concerns for cloud computing, IoT, pervasive systems and web services, it is important to establish a reference architecture that provides a holistic solution for implementing cloud-enabled applications and service interactions in IoT scenarios in a fashion that improves the overarching goal of attaining end-user trust and, in turn, improve user adoption of IoT applications (Apps).

We consider some of the key spheres of significance in arriving at a reference architecture that is aimed at achieving trustworthiness among end-users in IoT applications, as being reminiscent of the implementation of security and privacy in:
- The IoT application, holistically
- Ubiquitous computing systems in the solution
- Participating Cloud computing systems
- In the Service-Oriented Architecture (SOA) layer

As the adoption race for the aforementioned innovative computing paradigms continue to mount, researchers have uncovered some of the critical concerns and proposed solutions to various facets of the all-inclusive problem that we seek to address.

In the face of recent attempts at establishing security and privacy frameworks to support trust management in pervasive systems, a comprehensive model that fosters trust among the target users of these emerging technologies is yet to achieve mainstream adoption [21]. Among others, Itani et al. [1] described a set of security protocols for safeguarding privacy and compliance of end-user data in cloud computing scenarios. Yau et al. [2] looked at performance and security tradeoffs in SOA, while Ponemon Institute [3] shared an insightful research report detailing proactive steps to protect sensitive information in the cloud.

A number of previous studies have proposed privacy and security frameworks for protecting data in specific domains ranging from mobile health monitoring [30], self-improving smart spaces [19], location privacy in mobile computing [31], privacy protection in web services [32], privacy enhancement in platform-as-a-service cloud computing scenarios [10], and

http://www.hipore.com/ijsc
more. We challenge the trend by proposing a holistic view to the problem with a focus on protecting the security and privacy of end-user data while fostering trust in new and old technology solutions that are willing to subscribe to these standards.

To throw some light on how various facets of security and privacy implementations can be considered in a holistic reference architecture for realizing end-user trust in IoT applications, we consider a case study where a cloud-hosted Movie Recommendation Service (achieved by leveraging both YouTube and Facebook Services) draws end-user media content viewing behavior and preferences in a multi-member family household from a TV-mounted Microsoft Kinect sensor device, a Smart TV and an Apple iPad tablet device collaboratively. The Microsoft Kinect Sensor is used to collect information about individual user preferences for movies in a multi-member family household. The movie recommendations service determines recommendations for movies that each household member or a combination of household members might enjoy based on the previous viewing history of each individual household member (captured by the Kinect Sensor and the iPad tablet device) in conjunction with the content viewing preferences of a given household member’s influential Facebook friends. The ubiquitous Kinect Sensor device is used to identify specific users assembled in front of the family TV. Information gleaned by the Kinect sensor is transmitted through a mobile service to the cloud storage location. The Smart TV records the time of day that a movie was watched by a given household and saves it to the cloud storage through a cloud-hosted mobile service.

**Our Contributions**

Our contributions take the form of a conceptual Reference Architecture for building a security, privacy, and trust management protocol (SPTP) that is capable of protecting private data at the time of disclosure or collection, in-transit, at-rest and for the life of a private data element even when it crosses the boundaries of the original system to be consumed by another system. In addition, we propose a logical Reference Architecture for building cloud-enabled IoT applications.

We also propose a Secure, Private and Trustworthy Protocol (SPTP) with an associated seal that will be readily recognizable by end-users in various online and ubiquitous computing settings. The standard seal is to be used in all systems (including cloud services, mobile devices and applications, sensors, gadgets, web sites, and more) that wish to identify themselves as being secure, private and trustworthy to end-users and other entities.

We describe our motivation for this study in section 2 and showcase a number of relevant application scenarios in section 3. Our resolute contributions are clarified in section 4 through the:

- Explanation of some of the quintessential characteristics of a reference architecture for cloud-enabled IoT Apps that seek to support privacy and security at all major layers of the IoT solution.
- Discussion of the implementation details for our proposed SPTP protocol.
- Depiction of our proposed reference architecture for supporting privacy and security in IoT systems. We consider these design artifacts as one of our key contributions.

Implementation details for two case studies are also described in section 5. A comparison of our approach with that of previous research work is presented in section 6. In section 7, we describe our evaluation and findings regarding the perception of trust among end-users in our IoT system prototype which seeks to implement our proposed reference architecture in the case study. In the light of our findings, we share our conclusions in section 8.

**2. MOTIVATION**

This study advances our current investigations concerning the application of cloud services and collaborative ubiquitous devices in mobile health (mHealth) intervention scenarios. In most instances, sensitive health-related data is collected and stored in a cloud-hosted solution. The reference architecture presented in this paper provides a framework for ensuring that privacy and security take center-stage throughout the application development lifecycle in the pursuit of maximizing the promise of IoT, Ubiquitous computing and Cloud computing archetypes.

In addition, we seek to share a blueprint for developing software architecture that supports privacy and security in IoT solution designs. We envision that our template solution for the IoT domain can be adopted, refined and extended by software designers, engineers, and architects who seek to preserve trust across IoT implementations. By promoting the adoption of this reference architecture, we hope to institute a foundation for ensuring consistency in addressing privacy and security concerns among current and future IoT implementations. Previous studies [4] suggest that establishing a reference software architecture promotes re-use, reduces maintenance costs, and serves as a benchmark for software governance. We expect this reference architecture to serve IoT-related solution designers in the same capacity.

**3. SCENARIO ANALYSIS AND PROBLEMS**

We strongly believe that the scenarios presented in this literature constitute examples of how SPTP can be used to drive technology adoption in several scenarios only limited to the imagination of solution providers and end-users. The two scenarios considered for the SPTP prototype include geographical location monitoring to support online content recommendations, and a ubiquitous health application showcasing elderly care monitoring in a smart environment.

**A. Movie Recommendations Engine**

We consider a scenario where an Online Social Networking (OSN) solution provider (in this case, Facebook.com) allows end-users to disclose personal information on a user profile page where the end-user’s movie preferences are captured and

http://www.hipore.com/ijsc
shared with friends on the OSN web site. We then establish a third-party online video streaming and recommendations solution provider that only exposes its Mobile Application (App) and web site to end-users who have a valid Facebook credential. Facebook authentication is achieved through OAuth over HTTPS. This movie recommendations App is capable of tapping into a logged-in user’s social graph through the Facebook Graph API [5]. Imagine the movie recommendations solution provider (named Zoei) is a start-up company facing pressures to generate revenue to sustain its services.

The simulated movie recommendations App, in turn, surfaces and ranks movie recommendations based on the end-user’s current geographical location – gleaned from the end-user’s mobile device GPS sensor. The recommendations engine also pervasively retrieves additional user profile data from a logged-in Facebook user which has nothing to do with the perceived “good intent” for retrieving movie title “likes” and recent location data from the end-user’s Facebook friends in support of the movie recommendation ranking feature. In this case, the rationale for this “questionable” pervasively mined data is to sell the retrieved data to other advertising affiliates who have an interest in using some of the end-user profile data to enhance their online Ad targeting and general market segmentation efforts. In addition, this App communicates with a cloud-hosted web service to store the mined data in a public Cloud.

Key Privacy Challenges:

- **False Sense of Trust by Affiliation:** The end-user might wrongfully perceive the entire solution to be secure and trustworthy because authentication is supplied by a trusted party (Facebook).
- **Access to Private Data Storage:** Without access to the innards of Zoei, the end-user is blind-sided by Zoei’s clandestine collection, storage and transmission of personal identifiable information (PII) and other private data elements.
- **Ongoing Certification and Reputation Status:** The end-user has no way of determining Zoei’s current reputation for privacy and security when he/she accesses the App on the tablet device.
- **Data Privacy Access Control:** Once the profile data crosses the system boundaries of the OSN, there’s no guarantee of access control protection.
- **Privacy in Public Cloud Storage:** There’s no guarantee that PII or private data stored on Zoei cannot be leaked to other solution providers sharing the public cloud’s resources.
- **Web Cookies:** Control over data that is made accessible to third-party web sites is desired.

**B. Multimodal Health Monitoring in Elderly Care**

Another application scenario that we considered include a futuristic setting in which an elderly person is able to interact with a multimodal health monitoring system that is capable of tracking the participant’s physical activities, habits and private health information.

The user behavior data collected about the elderly person is posted through a web service hosted on a PaaS cloud. The scope of activity monitoring facilitated by the Kinect sensor includes the participant’s time spent walking around the house, indoor localization, screen capture and timestamps for medicine consumption, time spent watching TV, interactions with the Humanoid companion, etc. [12].

**Key Privacy Challenges:**

Some unique concerns in this scenario include:

- **Informed Consent:** Participants will prefer to be notified when both sensitive and non-sensitive data is collected about them in the smart environment [24].
- **Ongoing Reputation Access:** After the participant reviews and consents to the program, ongoing access to the privacy reputation of the solution at any point in time and opt-out options is desirable.
- **Data Access:** In some cases, participants will be interested in having control over the data that is collected and how the data is used.
- **Hardware Vendor issues:** A standard that is adhered to by all sensors in the multimodal environment will be ideal.
- **Compliance:** In a ubiquitous health (uHealth) environment, HIPAA compliance becomes a standard of interest, particularly in the US.

**4. PROPOSED MODELS**

In the ensuing section, we describe the characteristics of our proposed conceptual reference model, a security, privacy and trust protocol and also share a number of illustrations of the reference architecture model.

**4.1 Key Characteristics of the Conceptual Reference Architecture**

The reference software architecture for a given domain seeks to define the underlying components of the domain and their associated relationships [4]. The software architecture of a given implementation in the domain then becomes an instance of the domain reference architecture.

The Internet of Things can be described as an amalgamation of multiple heterogeneous digital devices, people, and services working collaboratively to solve a problem across technology boundaries, with the ability to seamlessly interact and share data about themselves and their environment [6]. In deriving our reference architecture, we outline the major components of modern IoT systems that can benefit from preserving security and data privacy by considering some of the fundamental components of IoT systems in the following applicable scenarios:

- **SCENARIO 1:** A home automation monitoring service that is capable of observing the usage of electricity in a given household and seamlessly

http://www.hipore.com/ijsc
regulates the home’s consumption of electricity by learning the preferences of the household in comparison with optimal power consumption best practices of other neighboring households of similar size

- **SCENARIO 2**: An Online Social Networking (OSN) service that is integrated with a pervasive eyewear device, like Google Glass, for capturing pictures and recording videos of interesting moments. The service is assumed to be useful for storing the recorded photos and videos in cloud storage while enabling the end-user to share the stored media with other friends in the OSN as well as public access

- **SCENARIO 3**: A movie recommendation service that leverages previous media content viewing patterns and the preferences of influential people in a particular household user’s circle of OSN friends to recommend future movies that will be of interest to the user. This scenario is employed in our case study implementation. A contextual view of the IoT-based movie recommendations scenario is illustrated below in Figure 1.

Fig. 1. Logical View of Interactions in the IoT system

In line with the scenario presented above, some of the major components that have their own facets for privacy and security concerns include:

- **End-User Preferences** for Security, Privacy and Trust
- **Cloud Computing**: in the form of a cloud-hosted web or mobile service and cloud-based data storage
- **Ubiquitous Computing**: represented by the Kinect Sensor, Tablet device and a Smart TV
- **Service Oriented Architecture** (SOA): in the form of the Facebook Graph API (web service) used for inferring the preferences of influential friends in a given household member’s OSN circle as well as the YouTube API (web service) for streaming a movie
- **Network communication** across wireless networks for transmitting and receiving data between the ubiquitous devices in the Smart Environment and the external cloud service environment

Conceptually, most of the major facets of a generalized IoT implementation are likely to include the fundamental components captured in Figure 2.

End-users have preferences for security, privacy and trust that must be collected and adhered to at all facets of the solution. There is typically an optional user interface and a physical sensor or ubiquitous device for data collection. These physical data communication components communicate to external systems through a network communication layer using a communication protocol to a web or mobile service of some nature. These web services, in turn, persist streams of data to a backend storage device. Typically, the backend service engine and storage is hosted in the cloud.

### 4.2 The Sptp Protocol

In arriving at a solution to user privacy standardization gaps in uHealth and online advertising scenarios, we propose a protocol that is capable of tagging private data with an access control list (ACL) that can be defined and managed by end-users across multiple platforms. In addition, we propose that the protocol is applied to data in-transit and at-rest. The protocol should be able to retrieve and validate the privacy policy of a given web page or ubiquitous system against the privacy ACL defined by the owner of the private data. The data owner should also be able to gain access to his or her data and make a decision to opt-out when need be. The end-user should also be able to observe the current privacy reputation score of the subscribers to the protocol.

In addition, the protocol is designed to be administered and enforced by a third-party regulating body to create an unbiased regulation of privacy standards and policies aimed at protecting the end-user. Most importantly, the protocol implementation must ensure ease of implementation to avoid the previous plight of P3P. We prefer to look at a holistic standard protocol that can be used to regulate user data privacy and security across ubiquitous and traditional web solutions to ensure consistencies in expectations across various mediums, domains and scenarios. The conceptual architecture of the SPTP protocol is described in the context of a case study in section VII.
4.3 The Reference Architecture

In creating a generalized reference architecture for improving security and privacy concerns in IoT systems we illustrate the various layers and characteristics discussed in section III along with some of the best practices employed in security and privacy implementations in Figure 4.

In most cases, end-users are likely to accept an IoT solution that is managed or hosted on a trusted cloud provider system. We propose the use of a governance body for ongoing certification and regulation of standards pertaining to the all-encompassing extent of a typical IoT implementation.

The ensuing literature describes some of the key concerns inherent in each layer of the IoT reference architecture.

4.3.1 Privacy in the Ubiquitous Sensors and Devices in the Smart Environment

In considering the security and privacy concerns of IoT applications, it is important to hone in on some of the security and privacy challenges pertaining to pervasive devices and sensors that are often working ubiquitously to collect and exchange data in the environment. From a security and privacy perspective, some of the key requirements that can be addressed at this layer of the IoT application include [6]:

- **User identification and validation** to control access and enforce permissions and authorization levels for various components of the system
- **Tamper resistance** of the physical and logical device. Because IoT devices are typically unattended, physical attack vulnerabilities are critical.
- **Content security** - through digital rights management (DRM) of content used in the system
- **Data privacy** to protect sensitive user data.
- **Data communications and storage security** through protective measures for both data in-transit and data at-rest
- **Secure network communication** to ensure that network communications between ubiquitous devices and external services are only authorized through secure connection channels (for example, the wireless communication in the smart home environment of our case study can only be transmitted through the user’s designated “home” wireless router, by default. Eavesdropping vulnerabilities in the wireless network must be curbed.
- **Privacy in ubiquitous computing** comes to play because the way in which the device or sensor collects data about the end-users might conflict with the user’s privacy preferences for a particular scenario. For example, while a user might be open to having the Kinect sensor perform user identification to support the IoT system, he or she might not be open to having the Kinect record certain conversations in the smart home living room. These privacy barriers and preferences must be preserved in order to instill end-user trust in the system
That notwithstanding, some of the key security features that can be incorporated in pervasive device architecture (that is considering both hardware and software requirements) include [6]:

- Lightweight cryptography approaches to support the low power, memory and processing power constraints in most pervasive sensors and actuators
- Security measures to protect the physical device
- An interface for determining and controlling the privacy preferences of the end-user. This might include a visual cue (for example, a green light) when the device is in recording mode. The ability to stop or pause the recording mode easily becomes critical as well
- Standard security protocols for direct device-to-device communication and device-to-service communication. For example, the Smart TV in our case study might need to send the user data securely to the cloud service in our case study through a secure socket layer (SSL) protocol over HTTPS communication.
- Secure on-device storage including RAM, Flash or ROM storage
- Secure operating system to protect data during runtime execution

In everyday human interactions, trust is often demonstrated when a user is able to confined in a close friend by sharing private or confidential information with the friend knowing that the friend will respect the display of trust by protecting the information from leaking to other unauthorized parties. Consequently, privacy goes hand-in-hand with trust. Privacy is sometimes defined as a critical human right “to be left alone” or an elementary need for an end-user to establish and maintain a private barrier to protect his or her information [7]. In devising a privacy solution at this level, Solove’s [8] taxonomy for addressing privacy might be considered during information collection, information processing, information dissemination, and in curbing invasion.

In smart pervasive environments, the information collection process is often invisible to the end-user by virtue of the built-in ubiquity of the solution. This often raises concerns among user privacy experts. In most cases, the end-user does not have access to the information that has been collected about his or her activities. Equally, the end-user often has minimal visibility and control over the processing and dissemination of the data collected in the smart environment. However, IoT promotes a lot of data sharing among multiple devices. It is
more critical for devices in an IoT setting to conform to standard privacy protocols that provide end-users with a level of comfort and trustworthiness that their private data will be protected. These issues have to be considered in deriving an effective architecture for hardware and software privacy.

4.3.2 Privacy in the Cloud Computing Layer

Cloud computing can be defined as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” [9]. In a typical cloud system model, there is a [1] Cloud provider – who exposes cloud services, and a Cloud consumer – who consumes these services. In our reference architecture, the IoT App Provider is also considered as a Cloud consumer.

Vulnerabilities in cloud systems can be categorized as [13] being related to Cloud Multi-tenancy, Elasticity, Availability of information (SLA), Information Integrity and Privacy, Secure Information Management, and Cloud Secure Federation. It is important the IoT provider considers these vulnerabilities in arriving at a secure solution.

Nonetheless, vulnerabilities in cloud solutions can differ for a given cloud deployment model. Some of the cloud deployment models in use today include [14] [15]:

- Private Cloud
- Community Cloud
- Public Cloud
- Hybrid Cloud
- Virtual Private Cloud

Beyond the considerations for each cloud deployment model, there are unique security and privacy issues in each delivery model. We consider the following layers in an IoT solution that makes use of a public cloud deployment solution:

- Services Layer - which includes:
  - Software Applications
  - Data management systems
  - Operating Systems
- Server Virtualization layer
- Physical Hardware layer - which includes:
  - Physical hardware
  - Network communication infrastructure

Some of the popular cloud delivery models [13] [14] include:

- Infrastructure-as-a-Service (IaaS): Where the cloud provider offers storage and computing services on-demand. The cloud customer manages the virtual machines (VMs) and other associated infrastructure components hosted in the cloud – including data storage, operating system and applications hosted on the VMs. Resultantly, security and privacy concerns at the application and operating system level are managed by the cloud customer. The cloud provider will handle security and privacy concerns at the datacenter hosting level including the virtualization and physical hardware layers.

4.3.3 Privacy in the IoT Apps and Service Layer

Security issues in integrating mobile agents and devices with services can be categorized as [18]: Confidentiality, Authentication, Authorization, Integrity, Nonrepudiation, Privacy, and Availability. In most typical IoT App scenarios multiple service endpoints were employed in the solution.
The IoT system interacts with its own cloud-hosted service layer as well as external services. The IoT application user interface itself might have its own privacy and security concerns. In addition, the third party external services used in the solution might need to be governed to ensure that they protect the end-user’s privacy and security preferences. For example, if the IoT application interacts with the Facebook Graph API, the end-user might have specific privacy settings set on Facebook (an OSN) that needs to be protected in the IoT system.

A. Cross-Cutting Governance Layer

In investigating an overarching solution that can protect end-users from the security and privacy vulnerabilities inherent in pervasive and cloud systems, we believe that it might be useful to introduce a trusted third-party security and privacy governance organization and/or a standard protocol for monitoring and developing ongoing compliance requirements that can be used to certify and regulate cloud and ubiquitous monitoring device providers in a bid to garner the kind of trust that is needed in such a big sphere of concerns.

From a cloud provider perspective, Ponemon Institute [3] recommends a number of proactive steps to be taken to protect sensitive information in the cloud environment including:

- Employ policies and procedures that stress the importance of protecting sensitive data in the cloud
- Assess the security status of third party vendors prior to sharing sensitive information through a thorough audit or review of the vendors’ security qualifications
- Establish a functional role dedicated to information governance oversight to ensure better security practices are employed
- Provide transparency into the security infrastructure to help instill confidence in cloud consumers that information stored in the cloud is secure

We believe that a third-party governance institution that can address the need for third-party assessment, regulations at all layers of IoT systems, transparency, policies, standards and ongoing status certification will be greatly beneficial to improving the trustworthiness of IoT applications.

B. Health Information Security and Privacy Compliance

In spite of the adoption and improvement of health information privacy protection in the US through the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule [28], there are ongoing concerns about data privacy associated with electronic health solutions.

While it might seem important that ubiquitous and cloud technology providers comply with HIPAA and PCI compliance requirements, these organizations only regulate healthcare and Ecommerce applications. This leaves gaps for non-compliant vendors to remain susceptible to other vulnerabilities that can cost end-users notable security and privacy breaches.

To present an overarching solution that will protect end-users from the security and privacy vulnerabilities inherent in pervasive and cloud systems, we strongly believe that third-party organizations may need to step in and develop compliance requirements that can be used to certify and regulate cloud providers and cater to the various cloud service delivery and deployment models discussed above. SPTP can then be employed to communicate and verify compliance to the standard security and privacy policies.

5. CASE STUDIES

We share two case studies that we used to validate the feasibility and validity of the proposed models described earlier.

5.1 Case Study for The Reference Architecture: A Movie Suggestions IoT Application

We implemented a prototype solution for a personalized movie recommendation IoT Application that takes into account our proposed reference architecture in order to derive the IoT Application’s solution architecture for governing security and privacy concerns at various layers of the solution.

Personas or Actors identified in the reference model include:

- End-users of the IoT solution
- Device providers or vendors who build pervasive sensors and devices that are used in IoT systems. For the Kinect sensor, the device vendor is Microsoft.
- IoT Application Provider and Cloud Consumer
- Cloud Provider who exposes cloud services that are used by IoT Providers. For our case study, the Cloud Provider was Microsoft’s Azure Cloud. The third-party OSN provider in our case study was Facebook’s Graph API while movie trailers surfaced in the App were served through Google’s YouTube API.
- Our pseudo third-party Security and Privacy governance provider is expected to take on the regulation and certification of various components in

Fig. 6. External OSN service (Facebook) API interactions between an end-user and the IoT movie recommendations application.
the IoT context including the cloud service and storage, external services like the Facebook API, and the IoT application itself. The provider also ensures adherence to standard protocols like OAUTH, SSL, etc. across the communication channels.

The external services employed include the Facebook Graph API and the YouTube API. To access the household member’s Facebook friend information the privacy of the user’s data must be considered in the external system. Access to the end-user’s Facebook information is controlled by Facebook’s implementation of a secure OAUTH 2.0 over HTTPS protocol for user authentication. In addition, Facebook allows the household user to authorized specific access to the IoT system, after the user’s credentials have been successfully verified. An access token is required by both the YouTube API and the Facebook API for the IoT endpoint to exchange data with the third party services.

For our case study, the IoT application’s user interface takes the form of a movie recommendations engine accessible through both an iPad device and a Smart TV as a web-based application. The user interface for our movie recommendations IoT App is represented in Figure 6 below.

The network communications component in the smart environment, in our case study, represents a wireless router for secure communications between the smart devices and cloud-hosted IoT web service. The ubiquitous computing device in our case study is represented by the Kinect for Windows sensor connected to the Smart TV. The movie suggestions that are provided in the application are ranked based on the social influence of a particular household user’s OSN friends as well as the previous movie preferences of the OSN friends (captured as Facebook “Likes”). In addition, movies that are similar to media content that was previously identified by the Kinect sensor as part of the authenticated user’s viewing history are factored into ranking the recommended movies for that particular user. While the benefit of this scenario seems to outweigh the need for the Kinect sensor to monitor the user’s viewing behavior, there can be a number of privacy and security concerns that might deter end-user adoption.

The cloud system model used in our case study analysis is synonymous with that of a public cloud [1] where the cloud provider manages and exposes storage and computing services through a geographically dispersed and on-demand scalable cloud infrastructure. We (as the cloud consumer) then utilize cloud storage to host data gleaned from the IoT device sensors. The web services employed in the IoT scenario also operate as cloud services hosted on the PaaS cloud infrastructure.

**Improving Privacy Concerns in this Case Study:**

Some of the concerns considered in enforcing privacy and security best practices at various layers of the reference architecture include:

- **Informed Consent:** We learned that end-users preferred to be notified when the Kinect sensor is collecting both sensitive and non-sensitive data in the smart environment. A visual cue by the form of a blinking green light indicator on the device while it is in recording mode proves to be useful.

- **Control over Privacy Settings:** The parent’s in the household may not want their children to have access to uncensored content, so the parent might want control over media content suggestions that are surfaced to the children in the household. Also, the parent might want to limit how much data is stored by the IoT App (for example, exclude geo-location information from data collection).

- **Vendor Regulation:** A third-party regulation body could be employed to monitor and expose gaps in the system based on the end-user’s pre-defined security and privacy preferences. Ongoing risk assessments on behalf of the end-users could prove to be useful.

- **Access to User Data and Opt-Out:** In some cases, participants prefer control over the data that is collected about them. End-users are also interested in how their data is used and seek to reserve the ability to opt-out and delete their data at will.

- **Ongoing Reputation Access:** Beyond the participant’s initial consent to allowing the IoT App access to his or her Facebook (OSN) data, it will be useful if the participant can access the privacy of the IoT solution itself at any point in time and opt-out without any loom of lock-in.

- **User Identification and Authentication:** If the identity management system throughout the IoT implementation is not accurate, uncensored content that might be appropriate for the parent but
inappropriate for the child might be surfaced mistakenly to the child.

- **Physical Security and Wireless Networks:** Prevention of eavesdropping in the wireless network as well as measures to enforce security of the physical objects in the environment proves to be critical.

### 5.2 Case Study For The Sptp Protocol: Elderly Care Monitoring

To test the efficacy of our proposed protocol, our simulation introduced a futuristic smart-environment where an elderly person’s physical activity will be monitored by a Microsoft Kinect for Windows Sensor. The Kinect sensor is mounted on a television in the elderly person’s living room. In addition, the subject is able to periodically interact with a NAO Humanoid robot as a personal companion. Private data collected by both the Kinect Sensor and the Humanoid Robot is transmitted and persisted in an SPTP tagged form through a Windows Azure Cloud Service (PaaS) to a storage account. The simulation seeks to demonstrate the use of several heterogeneous systems in a collective intelligence-inspired solution for activity monitoring [11]. The Kinect sensor is able to transmit data to the cloud storage service through a wireless (WiFi) connection as depicted in Figure 2. It also displays a consistent visual cue when in recording mode.

In this case, the user’s privacy preference ACL is applied to each recorded data segment in the form of a tag that can only be decrypted using the user’s privacy identifier. An informed consent form is presented to the elderly person describing the scope of monitoring and his rights to the data. The elderly person is also able to review information collected in the smart environment (through a web portal) to ensure that it conforms to his or her predetermined privacy preferences.

When the user decides to revoke a portion or all of the data that was previously collected about him or her, there is an option available through the web site to facilitate this. The user’s preference is then subsequently honored in all third-party systems that have previously consumed the private tagged data within a period of time – assuming those services also subscribe to the SPTP protocol.

![Fig. 8. Solution Architecture – Elderly care Monitoring](http://www.hipore.com/ijsc)

### 6. RELATED WORKS

While several security and privacy frameworks and reference architectures exist for various domains, we are not aware of a generic reference architecture that caters to modern IoT App scenarios. NIST [22] proposed a reference architecture for Cloud Computing and Itani et al. [1] have explored a reference framework for privacy in cloud computing scenarios. Several studies have focused on legal compliance and the technical implementation of trust models, frameworks and protocols. Additionally, Langheinrich [23] addressed key privacy concerns in ubiquitous systems.

Recent studies in this area can be categorized as either high-level frameworks (with a focus on legal compliance and risk assessments) or low-level frameworks (with a focus on technical implementation of access controls to data). Neither of these approaches offers a panacea.

### 6.1 P3p – Privacy Preferences Platform

Arguably, the most popular privacy protocol that is synonymous with our approach is the Platform for Privacy Preferences (P3P) project [25] [26]. P3P turned out to be difficult to implement and further work on the protocol has been suspended. We propose SPTP as a generic security, privacy and trust protocol that will transcend web and other ubiquitous computing scenarios, whereas the domain of focus for P3P was web-based solutions.

However, the mission of SPTP is consistent with the goals of P3P in enabling web sites to express their privacy practices in a standard form that can be verified by user agents [26] and make it easier for end-users to recognize the level of privacy compliance of a given solution without having to read the full privacy policy [25]. One of the limitations of P3P is that, while it facilitates better communication about privacy policies it does not act as an enforcement mechanism for privacy.
6.2 Other Privacy Frameworks

Alpcan et al. proposed the use of a “novel probabilistic diffusion scheme for detecting anomalies possibly indicating malware which is based on device usage patterns” [27]. Behl and Behl [26] recommend solutions to protect end-users from the potential privacy and security vulnerabilities of cloud systems. From a best practices perspective, Yale University [14] proposed some useful security and privacy approaches to support HIPAA compliance.

7. DATA ANALYSIS

We describe our evaluation of the two reference architectures as follows.

7.1 Reference Architecture Evaluation

To test the hypothesis that our reference architecture is feasible for most modern IoT implementations, we reviewed the implementation of security and privacy solutions aimed at achieving trust in the three scenarios (among others) described in section III and compared the inherent layers in the scenario to that of our proposed conceptual reference architecture.

In addition, we built a prototype of the case study described in this paper and shared the way in which various security and privacy concerns are addressed in our work-in-progress solution with a few technologically savvy end-users. We collected feedback from these end-users through a survey to gauge their comfort level with the implementation of security and privacy solutions at various layers of the conceptual model.

Of the 18 distributed surveys, we received 14 usable responses with questions centered on evaluating the importance of the various facets in the reference architecture and how it affects their overall level of trust in the IoT system:

- Trust in the underlying Cloud data storage system
- Trust in the ubiquitous devices and user interface

Participants (end users) were asked to indicate their rating with a scale of 1 through 3 (where 3 means the characteristic is Important, 2 represents Indifferent, and 1 denotes Not Important). Our analysis of the survey response indicates that most savvy respondents (92.8%) were most comfortable with the IoT system when the immediately visible device or sensor exhibited security and privacy best practices.

7.2 SPTP Evaluation

To evaluate the SPTP protocol, we plan on employing a number of approaches including:

- User survey on the perceived benefits of SPTP
- Performance measurement access control
- Analysis of the SPTP protocol and its impact on Ubiquitous system adoption and trust management.

http://www.hipore.com/ijsc
7.2.1 User Survey on the perceived benefits of SPTP

To test the hypothesis that SPTP is likely to inspire trust in the adoption of ubiquitous systems among adults, we conducted a preliminary survey to qualify users for our long-term study after demonstrating the proposed use of the protocol in a simulated smart environment for elderly care monitoring and interaction with a humanoid robot.

Of the 20 distributed surveys, we received 14 usable responses. The questions asked in the survey were categorized as Consent, Cues, Access, and Reputation. The survey respondents were also categorized as technologically savvy (9 participants) and non-savvy end-users (5 participants). The age range of the respondents fell between 25 and 53 years old. Participants were asked to indicate their rating with a scale of 1 through 3 (where 3 means the characteristic is Important, 2 represents Indifferent, and 1 denotes Not Important). The results of the user study are illustrated in Figures 3 and 4.

Our analysis of the survey response indicates that most savvy respondents (66.7%) are concerned with having some form of verbal or visual cue present when information that they perceive to be private is recorded and transmitted.

In general, users concluded that having a dedicated third-party service that regulates and certifies security and privacy in these environments could contribute to their level of trust in the system. Most of the non-savvy users expressed strong interests in having the robot instill a sense of connectedness and show unconditional care as a key driver for trustworthiness of adopting the simulated smart-environment.

7.2.2 Performance measurement of access control lists

We plan on evaluating the performance impact of adding the proposed ACL tags to data transmission and storage. Accordingly, we hope to minimize any additional overhead that might be caused by pursuing this approach.

7.2.3 Analysis of SPTP's Impact on Trust

Once the prototype is fully developed, we plan on conducting a survey with a wider audience to fully expound the promise of SPTP in ubiquitous and online systems. Considering the extent of the project, there is still a significant amount of work to be done to fully test our hypothesis regarding the impact of SPTP on trust management.

8. CONCLUSIONS

With the outburst of cloud services and the advent of pervasive and context-aware services, it is increasingly necessary to ensure that sensitive data is not compromised.

8.1 Sptp Protocol

As the results of our survey indicates, the savvy users of these technologies will have more trust and confidence in cloud-enabled ubiquitous solutions if they can garner some form of assurance that a third-party privacy protocol that enforces compliance standards has certified the application.

Similar to the Data Security Standards (DSS) compliance requirements that often governs the Payment Card Industry (PCI) we envision that it will be useful for third-party entities to adopt our proposed protocol or a variant of it, for managing the expectations for trustworthiness among cloud-enabled ubiquitous systems and web sites.

8.2 Reference Architecture

Based on the findings of our user study, even though addressing key security and privacy concerns holistically helps to minimize end-user adoption barriers, perceptions related to the trustworthiness of an IoT application hangs significantly on the implementation of security and privacy best practices in the immediately visible IoT device or application user interface. Nevertheless, with growing concerns of security and privacy in

http://www.hipore.com/ijsc
IoT Application scenarios, we believe that the proposed reference architecture can be adopted by researchers and IoT solution architects, at large, as a yardstick for governing the implementation of security and privacy concerns at all facets of an overarching IoT solutions architecture.

9. REFERENCES


http://www.hipore.com/ijsc


Authors

Ivor D. Addo is an IT Instructor and a PhD student at Marquette University, USA. He is also a member of ACM and IEEE. Ivor’s research interests are focused on privacy and security issues in IoT and Sociable Robotic applications. Ivor has a number of published peer-reviewed conference papers.

Sheikh Iqbal Ahamed is a professor and director of Ubicomp Lab in the department of Math., Stat., and Computer Science at Marquette University, USA. He is also a faculty member of Medical college of Wisconsin, USA. He is a senior member of the IEEE Computer Society and ACM. He completed his Ph.D. in Computer Science from Arizona State University, USA in 2003. His research interests include mHealth, security and privacy in pervasive computing and middleware for ubiquitous/pervasive computing. He has published 100+ peer reviewed journal, conference and workshop papers including nine best paper/posters. Dr. Ahamed serves regularly on international conference program committees in software engineering and pervasive computing such as COMPSAC 13, COMPSAC 12, PERCOM 08, and SAC 08. He is the Guest Editor of Computer Communications Journal, Elsevier.

http://www.hipore.com/ijsc