World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:10, No:6, 2016

The Internet of Things Ecosystem: Survey of the Current Landscape, Identity Relationship Management, Multifactor Authentication Mechanisms, and Underlying Protocols

Nazli W. Hardy

***Abstract*—**A critical component in the Internet of Things (IoT) ecosystem is the need for secure and appropriate transmission, processing, and storage of the data. Our current forms of authentication, and identity and access management do not suffice because they are not designed to service cohesive, integrated, interconnected devices, and service applications. The seemingly endless opportunities of IoT are in fact circumscribed on multiple levels by concerns such as trust, privacy, security, loss of control, and related issues. This paper considers multi-factor authentication (MFA) mechanisms and cohesive identity relationship management (IRM) standards. It also surveys messaging protocols that are appropriate for the IoT ecosystem.

***Keywords*—**Survey of internet of things ecosystem, protocols, identity relation management, multifactor authentication.

I. Introduction

IOT is a digital ecosystem that will have pervasive technological, social, and economic, impact on the human population. Its success and development revolves around the connection of everyday objects, to the Internet [1]. It was at the Consumer Electronics Show (CES) in 2014, that the reality of IoT became accessible in tangible, everyday forms. Industry professionals, the media, and consumers, were treated to a realm of practical possibilities presented by IoT. While IoT may have initially been met with skepticism, many consumers found that they had already, unwittingly and easily, slid into the world of IoT with the use of wearable devices such as the Fitbit. Over the last two years, the acceptance of IoT and its potential benefits have begun to fall into place. The success of IoT in the last years can possibly be attributed to a firm shift on a service and aesthetic oriented approach by the IoT industry, and also a focus on practical convenience. Conceptually grand, but cost-prohibitive IoT devices have now given way to convenient, practical and affordable IoT devices. "Wearables" that are functional and offer useful services, and are also fashionable (or can be discreet), like the FitBit, smart watches, Google Glass, iPod shuffle, and smart headsets, have become popular with consumers. And thus, in many ways, wearable technologies that are compact, value-added, and can be integrated with mobile devices, have led the momentum for IoT. In addition, convenience, integrated service, and a luxury factor play a role in the adoption of IoT. Certain products like Whirlpool "smart", for example, can be connected to a smartphone app that will text or email the user when the clothes are ready. It can also be connected with other IoT appliances like Nest to save energy with longer and more efficient dryer cycle. There are coffee machines that can coordinate with home monitoring systems and will turn on when the user comes home [3].

Nazli W. Hardy, MBA, Ph.D. Associate Professor of Computer Science Millersville University of Pennsylvania, PO Box 1002, Millersville, 17551-0302, USA (email: Nazli.Hardy@Millersville.edu).

II. Privacy Concerns for Data Collection by Interconnected Devices

It is estimated that by 2020, with billions of people connected to the Internet, the number of connected devices will exceed 50 billion, [2] and thus IoT represents a paradigm shift for authentication and access management. What has been, and continues to be a challenge, is privacy, security, and data ownership. By nature, in order to provide a cohesive and integrated service, connected devices need to collect, aggregate, store, analyze, mine, and process personal and personalized data on individuals and corporations in a variety of contexts and environments. Internet applications (e.g. Web, email, file transfer) are primary sources of data collection, both voluntarily and involuntarily. In the European Union (EU), the Data Protective Directive and the e-Privacy Directive regulate the data protection of consumers. However, the United States does not have a single and united overarching privacy law. Instead, on a federal level, it has disparate and industry-specific legislation, for example the Health Insurance portability and Accountability Act (HIPPA), the Fair and Accurate Credit Transaction Act (FACTA), the Children's Online Privacy Protections Act (COPPA) [9]. The Organization for Economic Co-operation and Development (OECD), with 34 member countries including many European countries and the United States, has taken steps to building a consumer-protective society. However, it is important to note that countries with large Internet-using populations like China, India, and Brazil are not yet member countries of the OECD. Countries like the United States, operate on an opt-out model. The opt-out model is deceptive since the consumer is not aware that there is an 'opt-out" policy, what data is collected, and what it is used for. In this landscape, IoT increases data access and collection, and decreases any transparency about

who and what are collecting data and how and when and why this data is used, transmitted, or stored.

At CES 2016, Edith Ramirez, chairperson of the Federal Trade Commission's words alluded to the continued concerns of gathering of sensitive and private consumer information: "… the industry needs to address these concerns and be more transparent about how they handle personal data …how that data is being used, or shared, and the potential for unintended uses, is a concern." Concern is perhaps an understatement given, for example, the digital toymaker, V-Tech Holdings which was hacked in 2015, exposing the data of 6.4 million children, along with that of 4.9 million adults. Laws like COPPA do nothing to protect against cyber-attacks and exposure and theft of personal data of children [9]. Research shows that 54% of digital customers are cautious about the information they share due to the lack of confidence in the online security that protects their personal data [7]. Edith Ramirez's actions are more telling than her words since she chooses to use a simple and unconnected pedometer to track her steps, over using an actual Internet-connected devise like the Fitbit.

III. Some Driving Forces of IoT

Despite the credible security and privacy concerns, IoT is a flourishing ecosystem that is spanning the world. For example, India is planning to invest approximately US$11 billion for developing 100 "smart" cities [2]. Some of the driving forces for IoT are:

- Wearable devices like the FitBit and smart headsets, which are either fashionable and cool or discreet and understated. They are seen as compact devices that can be connected to other mobile devices and offer value-added application services to the savvy user.
- Organizations and corporations see the advantage of using IoT-driven data to gain a better understanding of their customers' habits/ needs. Based on that knowledge, companies can improve supply chain/inventory coordination, investments.
- For the IoT ecosystem be able to function effectively, it needs to be scalable and adaptable, especially with metropolitan cities that are looking to transform themselves into "smart cities." The shift of population inflow from rural to urban areas deplete non-renewable energy sources, however "smart" interconnected infrastructure could force the implementation of solutions like smart grid, smart waste management, smart traffic control, smart utilities and sustainable city [2].

With so much riding on this burgeoning IoT ecosystem, a strong identity and authorization protocol is not sufficient, it is necessary. The login-password ordered pair is simply not enough as the identity and authorization piece for the management of a network of interconnected devices. Logins are easy to deduce logically, and passwords are easily cracked with readily available tools. In fact the login-password 2-tuple is altogether, unreliable for the IoT ecosystem.

IV. Identity and Access Management

The Internet has been evolving since the 1960's, when it was a simple network of 4 nodes, consisting of Stanford Research Institute, University of California Santa Barbara, University of Utah and University of California Los Angeles. The evolution now has catapulted to a multidimensional level with respect to identity management, networking performance, and overall security. The paradigm shift is from single connected devices, to the interconnection of humans, devices, applications, services, and the implications of those connections – in terms of identity and access management. So far identity and access management have focused on employees, and more generally on a static human interface. It is now necessary to:

a) address the introduction of devices from various locations, the service applications that each of the devices provide, and the users of these various devices.
b) facilitate the cohesive, secure and, reliable interconnection amongst people, devices, and the application services.
c) take into account the access mechanism of each device; the access mechanism must be easy to use for the legitimate user, but hard to access by an interloper
d) ensure that administration/employees/customers/clients are trained to understand and accept the need for the new set of protocols.

There is no clear and strategy for a cohesive, secure and reliable communication. A 2015 Hewlett-Packard/ Garner study [5] on the top 10 smartwatches found some concerning trends that show how these devices are susceptible to various attacks. Data collected on the smartwatches was transmitted to several backend sites. Watches that interface with the cloud use a simple and inadequate login-password 2-tuple, 70% of the watch firmware is transmitted without encryption, and many of the watches that included a mobile authentication allow for unrestricted account enumeration. And since the data being collected is sent to multiple sites, unencrypted, the security concerns go beyond the device. This study on smartwatches is relevant for a number of reasons. These wearable devices are one of the driving forces in the acceptance and implementation of the IoT ecosystem, and will conceivably be used as much as smartphones in the near future. It is also likely that smartwatches may replace smartphones as the control point for communication with other personal and professional devices in the IoT ecosystem (Fig. 1). So, it is clear that to address the paradigm shift created by the IoT ecosystem, the primary task is to be able to authenticate the:

a) user access to each of the multiple, connected, everyday devices,
b) service provider gateway via which the devices transmit data that is being access,
c) transmission of this data over the Internet,
d) people/ consumers/ employees/ clients accessing the data,
e) service applications being provided by each of the devices.

Additionally, there is the critical component of secure storage of this interconnected personal and personalized data

that creates a clear blueprint of a person's / family's daily habits, preferences, lifestyles. In cases like medical and health information, there are legal considerations bound by HIPPA, and in the case of underage children, COPPA laws must be abided. IoT is a complex ecosystem and the authentication of interconnected entities, their interoperability, and the management of access and storage will continue to pose a significant area of investigation, research, buy-in, and investment of several groups from around the world.

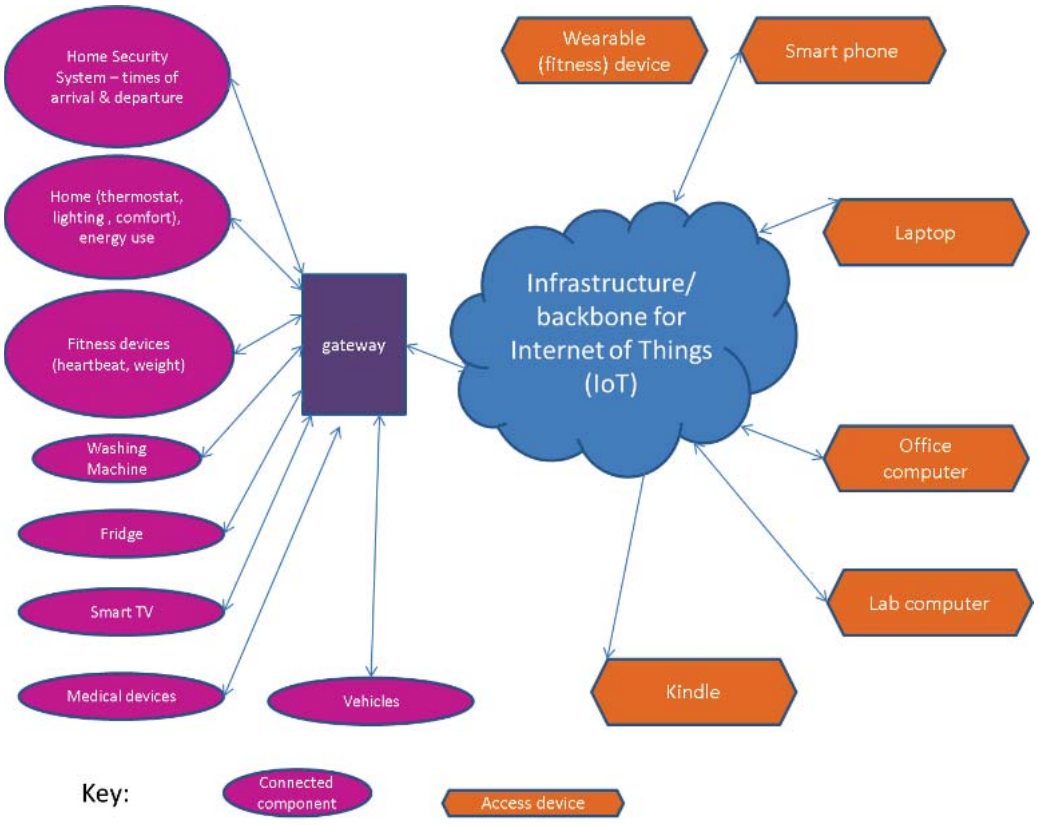

Fig. 1 A sample of multiple, everyday devices interconnected into the IoT ecosystem

V. IRM AND MFA

In the last two years, several organizations and working groups have been investigating and defining IoT identity management standards. Strong, appropriate, revised, and even redefined identity and access management (IAM) is now critical to the function of IoT due to the necessary transition from people-centric to device-centric authentication. According to Gartner's Ant Allan, "the Identity of Things requires a new taxonomy for the participants in IAM systems. People, software that makes up systems, applications and services, and devices will all be defined as entities and all entities will have the same requirements to interact" [4]. Thus IoT and the extension of identity management, Identity of Things (IDoT), must go hand in hand. IDoT must necessarily map the relation between entity-entity, entity-human, entity-application services, human-application services, and do so in a cohesive and meaningful way. In the safest of scenarios, a login-password authentication using a screen interface is a lightweight and optimistic measure of privacy or security. In addition, devices and the service applications that they provide, will not always have a screen interface to provide users with the login-password authentication. The subject of authentication not only needs to be urgently addressed, it needs to be redefined.

A group consisting of Experian, Salesforce, ForgeRock, and The Kantara Initiative defines an evolution from IAM to IRM and advocates this by defining "pillars of IRM" for business and for technology [8].

The business pillars include the following;

a) consumer and things over employees – identity management that must manage access privilege across several interconnected devices which may be in different physical locations.
b) adaptable over predictable – IRM must be adaptable to contextual circumstances.
c) top line revenue over operating cost – a secure and efficient IRM solution should be seen as a revenue item, as opposed to an operating cost.
d) velocity over process – it is necessary to base IRM decisions, not on cost of deployment only, but primarily on speed, accessibility, ease of use, and scalability for customer and employee needs.
e) Internet scale over enterprise scale – as the numbers and types of users (employees, partners, customers, devices)

are accessing networks from anywhere, IRM systems must be scalable and adaptable enough to accommodate thousands or even millions of identities, instantaneously, simultaneously.

f) dynamic intelligence over static intelligence – depending on where, when, and what device a user is logging in from, it may be necessary to dynamically restrict, expand, adjust access, and ask for additional authentication beyond the login-password ordered-pair.

g) borderless over perimeter – isolated secure perimeters are not secure in an environment where employees, partners, and customers, need access from any number and type of devises, anytime, from anywhere, including vehicles and the cloud.

h) modular over monolithic – given the multitudes of users, access points, circumstances, and privileges that represent IoT, an IRM solution needs to be well-thought out, visionary, integrated, cogent, cohesive stack that is purpose-built to handle complexity.

It is clear that for the broad, context-based, and pervasive nature of IoT, single factor authentication will not suffice. The European Commission's Expert Group on IoT, advocates a MFA: "the issues of providing non-colliding unique addresses in a global scheme requires an infrastructure in place that supports highly dynamic devices that appear and disappear from the network at any time, move between different local and/or private networks and have the flexibility to either identify their user uniquely or hide his/her identity, thus preserving privacy as needed." [1]

Accenture [7] reports that in a survey taken in 2015, 60% of people find the use of login-password to be cumbersome, 77% of the people are interested in alternative means to protect their security on the Internet.

The Cloud Security Alliance's IoT Working Group has made a list of recommendations with respect to identity and access management in the IoT ecosystem [6], some of which include:

- defining a common namespace for IoT devices,
- defining a clear registration process for IoT devices that is in line with the degree of sensitivity of the data being handles by the particular device,
- determining the level of security protections (confidentiality, authentication, authorization) to be applied to unique data flows from sensors and other IoT components
- determining and documenting whether outside organizations have access to certain categories of data
- defining how to perform authentication and authorization for IoT devices that are only intermittently connected to the network
- identifying access control requirements that apply to IoT according to an organization's access control policies.
- integrating next generation smartphones for authentication, since they are likely to be able to incorporate a combination of biometric (facial, voice recognition, finger printing) authentication.
- plan for the IoT ecosystem with devices that are designed to use IPv6
- establishing an explicit relationship diagramming between people and devices that includes specific authorization of specific data sets on specific devices. These must be enforced with MFA
- creating a well-documented plan for response to failures and breaches of security and privacy within the IoT ecosystem.

VI. Some Underlying Protocols for the IoT Ecosystem

The following protocols, their derivatives or combinations are viable contenders as protocols for the IoT ecosystem (Table I). Some are pre-existing and adaptable, and some implemented with IoT in mind.

TABLE I
Assessment of Protocols Implemented in the IoT ecosystem

Underlying Protocol	
Atmel/ MXCHIP	Atmel and MXCHIP, a Chinese IoT start-up have announced that the 2 companies will develop an ultra-low power (IoT) platform with secure Wi-Fi access to the cloud, enabling designers to quickly bring their connected devices to market [10].
Sigfox	Already deployed in major cities across Europe, offering a robust, power-efficient and scalable network that can communicate with millions of battery-operated devices across areas of several square kilometers, making it suitable for various M2M applications that are expected to include smart meters, patient monitors, security devices, street lighting and environmental sensors.
OAuth 2.0	A technology that offers such a design pattern with the use of access tokens, which are requested by clients, and subsequently presented to resource servers when demanding access to protected resources managed by those resource servers [12]
Constrained Application Protocol (CoAP)	An open standard, and is commercially supported and growing rapidly among IoT providers. It is a client/server protocol and provides a one-to-one "request/report" interaction model with accommodations for multi-cast, although multi-cast is still in the early stages of IETF standardization. CoAP is specified from the outset to support IoT with lightweight messaging for constrained devices operating in a constrained environment.
Message Queue Telemetry Transport (MQTT)	A machine-to-machine (M2M)/ IoT connectivity protocol designed as a lightweight publish/subscribe messaging transport, that is useful for connections with remote locations. TCP/IP port 8883 is also registered, for using MQTT over SSL. It is an existing protocols that has been adapted to IoT needs [11].
eXtensible Messaging and Presence Protocol (XMPP)	A TCP communications protocol based on XML that enables near-real-time exchange of structured data between two or more connected entities. XMPP is decentralized; XMPP works similar to email, operating across a distributed network of transfer agents rather than relying on a single, central server or broker (as CoAP and MQTT do) [15].
DDS	A protocol that enables network interoperability for connected machines, enterprise systems, and mobile devices. It provides scalability, performance to support IoT applications. DDS provides a global data space for analytics and enables flexible real-time system integration [12].
Bluetooth Smart	A short-range communications technology especially important for wearable products, often connecting through a smartphone. Tt has been designed to offer significantly reduced power consumption.
ZigBee	The only open, global wireless standard to provide the foundation for IoT by enabling simple and smart objects to work together, improving comfort and efficiency [13], [14].

VII. Conclusion

There have been early adopters of IoT from both industry and the consumer base who are eager to take advantage of the value-added conveniences of interconnected smart devices. For this adoption to extend itself effectively and efficiently on a global scale, and to gain widespread momentum, consumers need confidence in the service of device, experience and brand [7]. Security is a continuing source of concern, with respect to traditional networks, and this apprehension is manifold with respect to IoT Some specific factors include the adaptation of appropriate and MFA that can encompass authenticating a) various devices (that are interconnected, at different locations, providing different levels of services, accessing data that is personal and personalized), b) people accessing the devices from different locations and from different contexts, and c) service applications. Another factor of concern is the security and protection of data; their transmission, storage, mining, and access. In recognition of the need to cater to the paradigm shift of networked devices, several groups have been working diligently and in conjunction with other research groups. Even so, the current body of research is disparate, and in time will need to be consolidated. What is clear is that the navigation of this expanding and intricate IoT ecosystem, is a complicated proposition, and as of yet, there are no widely accepted standards or protocol sets that are broadly used in industry. The Internet has technically been in existence since the 1960s, and its expansion to its current form was not foreseen. Likewise, it is anticipated that in the next few years the expansion and the landscape reshaped by IoT will also be unrecognizable. What we can presume is that, its rate of success will be dependent on the appropriate and rigorous multifaceted authentication and protection of data; consumer and business.

References

[1] Report on the Public Consultation on IOT Governance, European Commission January 2013
[2] Insights on Governance, Risk and Compliance: Cybersecurity and the Internet of Things, Ernst and Young, March 2015
[3] The Internet of Things: prepare for a Connected Life, Lancaster Online, January 2015 http://lancasteronline.com/features/the-internet-of-things-prepare-for-a-connected-life/article_27a9c5ec-980d-11e4-9944-1fefbe6e1564.html *retrieved on 3/5/16*
[4] The Identity of Things for the Internet, Gartner, February 2015
[5] The Internet of Things Security Study: Smartwatches, HP, 2015
[6] Identity and Access Management for the Internet of Things – Summary Guidance, Cloud Security Alliance IOT Working Group, 2015
[7] Accenture Digital Consumer Survey for Communications, Media, and Technology (CMT), 2015
[8] https://kantarainitiative.org/irmpillars/ *retrieved on 3/5/16*
[9] Differences between the privacy laws in the EU and the US, Infosec Institute, January 2013
[10] http://blog.atmel.com/2015/05/05/atmel-and-mxchip-develop-wi-fi-platform-with-secure-cloud-access-for-iot-apps/ *retrieved on 3/5/16*
[11] http://electronicdesign.com/iot/mqtt-and-coap-underlying-protocols-iot *retrieved on 3/5/16*
[12] http://portals.omg.org/dds/ *retrieved on 3/5/16*
[13] http://www.zigbee.org/ *retrieved on 3/5/16*
[14] http://www.rs-online.com/designspark/electronics/knowledge-item/eleven-internet-of-things-iot-protocols-you-need-to-know-about *retrieved on 3/5/16*
[15] http://www.infoworld.com/article/2972143/internet-of-things/real-time-protocols-for-iot-apps.html *retrieved on 3/5/16*