A PARTICIPANT-DRIVEN FRAMEWORK FOR INTERNET OF THINGS (IOTs) SECURITY POLICY

ADAMU Aishatu [1], SANUSI Muhammed [2], BISALLAH Hashim I [3], EBELOGU Christopher U [4]

Research Scholar[1], Lecturer[2-3], Research Scholar[4]

[1-4]Department of Computer Science,

University of Abuja, Abuja,

Nigeria

Abstract

The ability to connect, communicate with, and remotely manage an incalculable number of automated devices via the Internet is becoming pervasive, from the factory floor to the hospital operating room to the residential basement. Internet of Things (IoT) can also be described as the use of intelligently connected devices and systems to leverage data gathered by embedded sensors and actuators in machines and other physical objects. In other words, it is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. In line with this development, the majority of the governments in Europe, in Asia, and in the Americas consider now the Internet of Things as an area of innovation and growth. Although larger players in some application areas still do not recognize the potential, many of them pay high attention or even accelerate the pace by coining new terms for the IoT and adding additional components to it. Moreover, end-users in the private and business domain have nowadays acquired a significant competence in dealing with smart devices and networked applications. The purpose of the research work is to develop a participant-driven framework for IoT security. The researcher is of opinion that the basis for all security is policy which is a major component of security governance. The significant of the research is to contribution to knowledge and the industry. The first part is achieved through developing of theoretical and conceptual frameworks for security policy of IoT. The method used in carrying out this research work is a research survey of existing models, framework or policies that are currently applicable to mitigate security threats of related technology.

Keywords: *Internet of Things (IoTs), IoT Ecosystem, Data Analytic, Security Framework, Data Sensor, Communication, Wireless Network, Unique Identifier (UIDs), Generic Protocol.*

1. Introduction

[4] used the term Internet of Things (IoT) to refer to the connection of systems and devices that are of physical purposes (e.g. sensing, heating/cooling, lighting, motor actuation, transportation) to information networks (including the Internet) via interoperable protocols. The growth of network-connected devices, systems, and services creates immense opportunities and benefits for our society. The ability to connect, communicate with, and remotely manage an incalculable number of automated devices via the Internet is becoming pervasive, from the factory floor to the hospital operating room to the residential basement [4]. Internet of Things (IoT) can also be described, according to GSM Association [5] as the use of intelligently connected devices and systems to leverage data gathered by embedded sensors and actuators in machines and other physical objects.

[12] highlight some of the potential Internet of Things application areas such as Smart Cities (and regions), Smart Car and mobility, Smart Home and assisted living, Smart Industries, Public safety, Energy & environmental protection, Agriculture and Tourism as part of a future IoT Ecosystem have acquired high attention.

IoT has the potential to make our highways safer by enabling connected vehicles to interact with each other to prevent accidents, to make quality health care more accessible through remote monitoring devices and telehealth practices for those who cannot easily travel, and to reduce waste and improve efficiency both in factory supply chains and in the running of cities. It has the potential to create new industries and consumer goods that have yet to be imagined [3]. Utilities are starting to be connected, with the electricity sector increasingly adopting the SmartGrid technology. Smart water is next, with the benefits of sensing technology to pinpoint leaks in the water delivery system [1].

2. Research Objectives

The research work is aimed at developing a policy framework that considers the roles of key players in IoT ecosystem namely developer, service providers, end users, securers and exploiters and how these participants' concerns relate to each other.

- Develop a framework that specifies the interactions among the participants in the IoT ecosystem.
- To develop the policy that ensures the safety of the IoT ecosystem.

For specificity, the researcher considers the application of smart metering, the IoT device that collects information about power usage and billing from household and send to the power company for administration. The proposed framework would be evaluated by adapting it to the protection of privacy of customer information to ensure that the information is only accessed with customer's permission.

3. Motivation Of The Study

The research work is motivated by a work by [7] for Internet Society. In the work, it is pointed out that, as a matter of principle, developers and users of IoT devices and systems have a collective obligation to ensure they do not expose users and the Internet itself to potential harm. Accordingly, a collaborative approach to security will be needed to develop effective and appropriate solutions to IoT security challenges that are well suited to the scale and complexity of the issues. It is obvious the number of things (devices) that will be connected to the internet will continue to increase; therefore, insecurity is not an option. Some challenges are still left open to be discussed and alleviate on the IoT elements. The challenges include IoT privacy, participatory sensing, data analytics, GIS based visualization and Cloud computing, architecture, energy efficiency, security, protocols, and Quality of Service. The research work is therefore motivated by these challenges.

4. Literature Review

Currently, there is no single, universal definition for IoT. However, [6] describe IoT as an interconnection of sensing and actuating devices that provides the ability to share information across platforms through a unified framework of developing a common operation for enabling innovative applications. This is achieved by seamless ubiquitous sensing, data analytics and information representation using Cloud computing as the unifying framework.

The concept of combining computers, sensors, and networks to monitor and control devices has existed for decades. The recent confluence of several technology market trends, however, is bringing the Internet of Things closer to widespread reality. These include ubiquitous connectivity, widespread adoption of IP-based networking, computing economics, miniaturization, advances in data analytics, and the rise of cloud computing.

Furthermore, in order to explain the applications of IoT in industrial control system, [14] describe Industrial Internet of Things (IIoT) as a system that connects and integrates industrial control systems with enterprise systems, business processes and analytics. An IIoT system enables significant advances in optimizing decision-making, operations and collaborations among a large number of increasingly autonomous control systems.

IoT has come to stay. This is no longer hype – the reality is evident in cool new applications being announced every single day – smart watches, fitness bands and trackers, smart glasses to name just a few. The IoT is manifesting itself in technologies beyond consumer electronics in other markets and applications too. The rapid advances being demonstrated through self-driving cars and drones provide endless possibilities that a network of smart connected devices can bring to improving human productivity, safety, and overall quality of life. Today, we can confidently assert that the promise of the IoT is already being realized.

[9] in introduction to IoT proposed three Cs of IoT; Communication - IoT communicates information to people and systems, such as state and health of equipment and data from sensors that can monitor a person's vital signs. For example, an IoT-enabled HVAC system can report if its air filter is clean and functioning properly.

4.1. Internet of Things Communications Models

Figure 4.1 shows a generic Internet of Things topology proposed by [16]: A typical IoT deployment will consist of sensor-equipped edge devices on a wired or wireless network sending data via a gateway to a public or private cloud. This topology will vary broadly from application to application; for example, in some cases the gateway may be on the device. Devices based on such topologies may be built from the ground up to leverage IoT (greenfield) or may be legacy devices that will have IoT capabilities added post-deployment (brownfield).

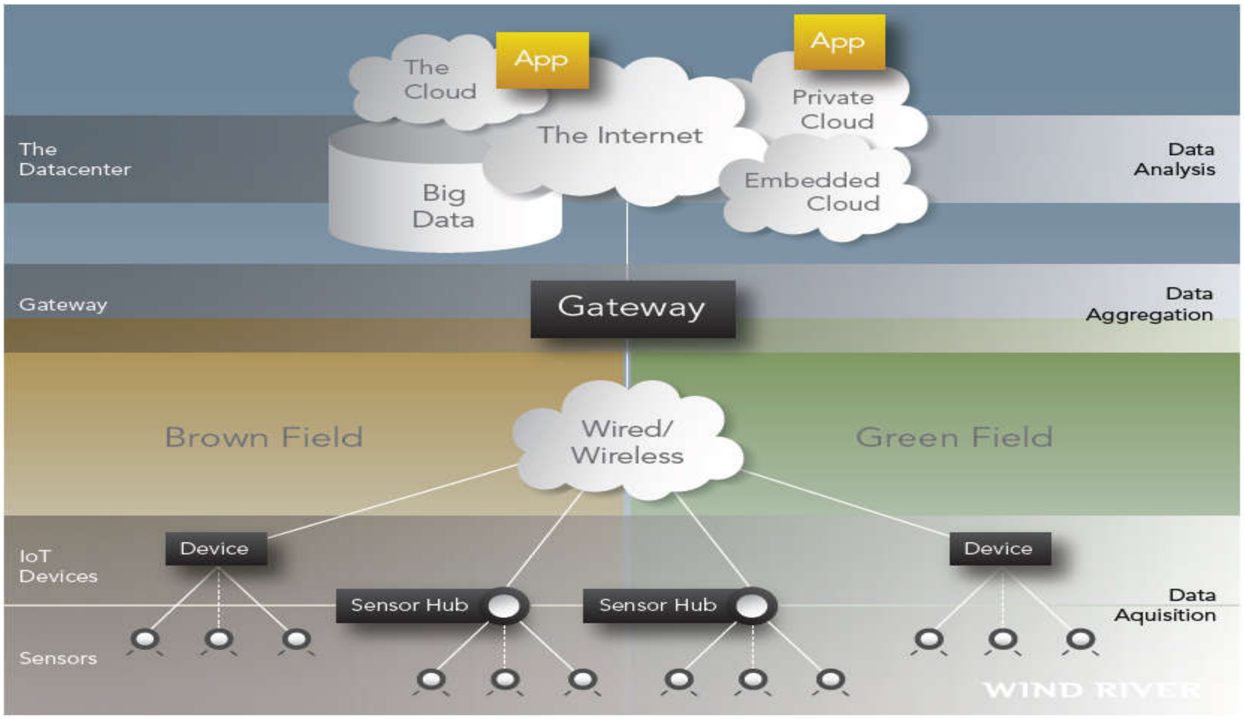

Figure 4. 1: A generic Internet of Things topology

A model shown in Figure 4.2, for IoT ecosystem proposed by [12] has acquired much attention. The model depicts three factors namely users/stakeholders who desire IoT applications, IoT enabling technology, and IoT viable marketplace. While this model is good to explain the generic topology and architecture of IoT, the interacting factors of IoT ecosystem and the participants that drive these interactions are not stated. Therefore, it cannot be used as a template for the model for a participants-driven approach for IoT security, which we sought.

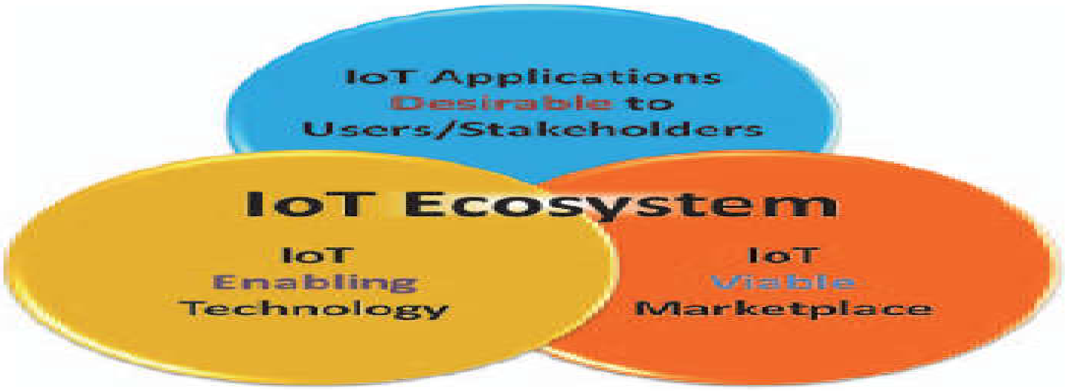

Figure 4. 2: IoT ecosystem

4.2. Challenges of Securing the IoT

The protection of system from unintended or unauthorized access, change or destruction is referred to as system security [14]. No IoT system can behave securely in every context. Therefore, the specific contexts deemed relevant must be explicitly stated along with the secure behavior that the stakeholders expect from the system. Assurance of security on information assets is often assessed in terms of risks on its components. Elements of security risk include a threat (someone or something that is attempting to do harm), the targeted asset (that has a value), a potential vulnerability or weakness of the asset that the threat will exploit, and connecting more things in more places creates new security challenges. Mitigating risk requires a combination of cybersecurity and physical security. The IoT is expected to grow to 50 billion users by 2020 [11]. Each device is a potential entry point for a network attack by insiders, hackers, or criminals.

Traditionally, security has been considered in terms of confidentiality, availability, and integrity, with a number of practices established to ensure these qualities. Applying these same practices or variants of them in the IoT world requires substantial reengineering to address device constraints [16]. Many small devices have limited CPU power not sufficient for security [8]. There is need for new encryption schemes with less CPU power. Blacklisting, for example, requires too much disk space to be practical for IoT applications. Embedded devices are designed for low power consumption, with a small silicon form factor, and often have limited connectivity. They typically have only as much processing capacity and memory as needed for their tasks. There is not a human being operating them who can input authentication credentials or decide whether an application should be trusted; they must make their own judgments and decisions about whether to accept a command or execute a task.

The endless variety of IoT applications poses an equally wide variety of security challenges [16]. In factory floor automation, deeply embedded programmable logic controllers (PLCs) that operate robotic systems are typically integrated with the enterprise IT infrastructure. The challenge is how best to shield those PLCs from human interference while at the same time protecting the investment in the IT infrastructure and leveraging the security controls available. Similarly, control systems for nuclear reactors are attached to infrastructure.

Also, there is need to develop a technique that enables the software to receive updates or security patches in a timely manner without impairing functional safety or incurring significant recertification costs every time a patch is rolled out. Many IoT devices are intentionally designed without any ability to be upgraded, or the upgrade process is cumbersome or impractical [7]. For example, consider the 2015 Fiat Chrysler recall of 1.4 million vehicles to fix a vulnerability that allowed an attacker to wirelessly hack into the vehicle [8]. These cars must be taken to a Fiat Chrysler dealer for a manual upgrade, or the owner must perform the upgrade themselves with a USB key. The reality is that a high percentage of these autos probably will not be upgraded because the upgrade process presents an inconvenience for owners, leaving them perpetually vulnerable to cybersecurity threats, especially when the automobile appears to be performing well otherwise.

5. Research Method

The method used in carrying out this research work is a research survey of existing models, framework or policies that are currently applicable to mitigate security threats of related technology.

5.1. Research Scenario

We consider the installation of a smart meter - one which is able to send energy usage data to the utility operator for dynamic billing or real-time power grid optimization. Smart meters enable two-way communication between the meter and the central system. The architecture consists of resident or industrial customer, smart meter with communication interface/protocol, gateway with communication interface/protocol, and database [15]. Communications from the meter to the network can be done via fixed wired connections (such as power line communications) or via wireless. In using wireless, one can opt for cellular communications (which can be expensive), Wi-Fi (readily available), wireless ad hoc networks over Wi-FI, wireless mesh networks, low power long range wireless (LORA), ZigBee (low power low data rate wireless), Wi-SUN (Smart Utility Networks), etc [15].

Regardless of the type or quantity of their measurement, smart meters should have six basic functionalities as outlined by [13], which include quantitative measurement of the medium by using various topologies, control and calibration to compensate the small variations according to each system type, security communication of operational commands and stored data as well as upgrades for its firmware trustworthily, power management to help the system to exactly maintain its functionality when the primary source of energy is lost, display information usage of electricity energy to customers for real time billing and efficiently management of their demand, synchronization of data between the customers and the collector systems or central hubs for billing and data analysis.

Serious vulnerabilities in smart electricity meters continue to expose both consumers and electric utilities to cyberattacks [2]. According to [2], experts have analyzed the methods that can be used to hack smart meters using remote software hacking which is much easier than physical attacks. In the case of attacks aimed at consumer home networks, hackers can abuse ZigBee because Smart meters don’t ensure that a new device should be allowed to join the network before they share the network key with it. This key can allow an attacker to impersonate any device and take control of other devices on the network, said the expert. If they hijack the meter itself, attackers could find and exploit vulnerabilities – the lack of CPU and memory resources in a smart meter often results in minimized ZigBee code, which does not include security checks. While memory corruption issues, such as buffer overflows, might not be easy to exploit, the researcher believes it's enough for an attacker to find a segmentation fault and crash the meter, which can lead to a power outage [2].

The coexistence of power systems and IT systems also create vulnerability in smart metering system [3]. Since power systems coexist with the relatively short lived IT systems, it is inevitable that outdated equipments are still in service. This equipment might act as weak security points and might very well be incompatible with the current power system devices.

The theft of data and energy [11] breathes availability of power which definitely threatens revenue.

There is a threat to consumer's privacy [16]. i.e. unauthorized access to information or disclosure. For instance information that power usage has dropped could indicate that a home is empty, making it an ideal target for a burglary or worse. Similarly, attackers could analyze data from meter to achieve "consumer profiling" with an alarmingly high accuracy [15], for example, the data could show the estimate of how many people live in the house, type of devices, duration of occupancy, ability of security and alarming systems. [10] have shown that they can identify the use of major devices in a house of customer by analyzing cumulative energy consumption data from the smart meter with a 15 min interval.

5.2. The Building Blocks for Proposed IoT Security Framework

The proposed IoT security framework with its functional viewpoint comprises six interacting building blocks. They are organized into three layers. The top layer comprises the four core security functions: endpoint protection, communications and connectivity protection, security monitoring and analysis, and security configuration management. These four functions are supported by a data protection layer and a system-wide security model and policy layer. These three layers comprise the functional viewpoint of the industrial internet security framework.

The elements that need be upheld to provide the security of information and system assets are confidentiality, integrity and availability, often referred to by the acronym CIA.

Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities or processes. Breaches of confidentiality can occur by word of mouth, printing, copying, emailing, or through software vulnerabilities that allow attackers to read or exfiltration data. Data exfiltration is the unauthorized transfer of data read through exploits at another location under the control of the attacker. This data may be used for blackmailing or other purposes. Confidentiality controls include access control and encryption technologies.

Integrity ensures that improper information modification or destruction is guarded against. Integrity controls include hashes, checksums, anti-virus functionality, whitelisting and code signing that ensures there have been no changes to the system, code and elements controlling the physical processes of the system. Data integrity, a subset of integrity, ensures that unauthorized parties cannot alter data and take control of the system without detection.

Availability is the property of on-demand, timely and reliable access to and use of information by an authorized user. The systems responsible for controlling the physical process should provide continuous control and oversight by human operators of the physical process. A human may need to intervene in the case of an attack, for example to shut the system down. Availability controls generally involve redundancy and engineering change control. Sometimes they include security activities that find and mitigate software vulnerabilities that create unreliable execution, visualization or resource consumption that negatively affect the systems.

6. System Implementation

6.1. IoT Security Framework for Participants Equities and Relationships

The first phase of the work is the developing of framework that identifies the players and their equities. The framework identifies five general groups of actors representing the principal players in this ecosystem: users, developers, service provides, exploiters, and securers.

As in all ecosystems, actors in the IoT ecosystem seek to maximize their own interests or equity. The equity is actors' interests based on their desire to maximize the benefit they derive from the ecosystem. For users, their equity involves maximizing the value they get from the cyber ecosystem, whether it allows them to engage in activities they could not do before or to operate better, cheaper, easier, or faster. Developer and service provider seek to maximize their competitiveness within the cyber market, such as by providing better capabilities, increasing profits, gaining wide user acceptance, or being acknowledged for uniqueness or quality. Exploiters seek to extract value from the ecosystem, principally at the expense of users. The value they seek can be economic, or it can be to manipulate and gain influence over users. State-based exploiters might have political or military motivations. Securers' equity derives from thwarting the actions of exploiters. Securers find value in making some aspect of the cyber ecosystem more secure from exploiters than it would be otherwise. These equities are illustrated in Figure 6.1.

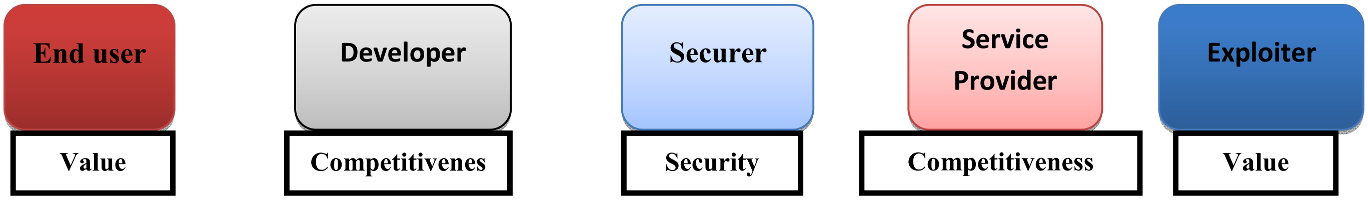

Figure 6. 1: IoT Participants equity framework

Likewise, Figure 6.2 shows the relationships that co-exist among the players in IoT ecosystem. To secure the ecosystem, the relationship between securers, and service provider, users and developers need to be mature and adequate. Although users clearly want security, they want increased capability more. They should be willing to pay for security in the form of increased costs or forgone capabilities. Likewise, developers should see security as a determinative competitive advantage. There is an inherent tension observed between actors and their equities, or priorities and interests. These equities - value for users, competitiveness for developers and service providers, and security for securers - have something of a zero-sum relationship. The competitiveness that developers and service provider seek benefits their own interests while also benefiting exploiters by dissuading investment in security. As a result, for users and securers, competitiveness works against security interests. The security that the securer seeks works to the user's advantage but raises the bar for the exploiter and raises costs for the developer. Similarly, the value that users seek prioritizes performance, capability, and cost over security, which works to the advantage of the exploiter. These dynamics fail to properly incentivize the developer and service provider to provide robust security or to adequately reward the securer.

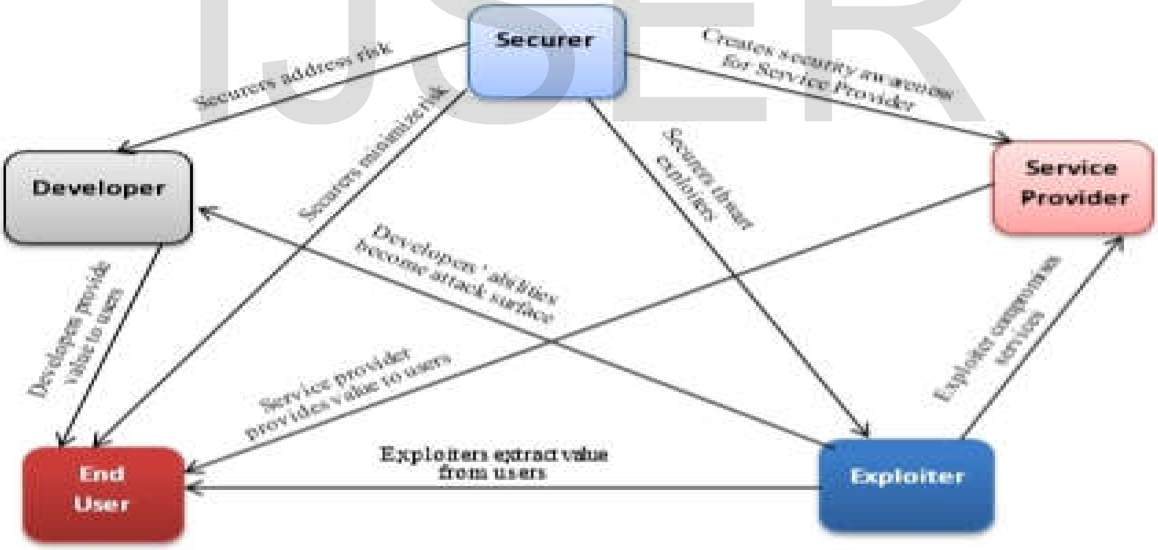
Securer
Securers address risk
Creates security awareness for Service Provider
Developer
Securers minimize risk
Securers thwart exploiters
Service Provider
Developers ' abilities become attack surface
Developers provide value to users
Service provider provides value to users
Exploiter compromises services
End User
Exploiters extract value from users
Exploiter

Figure 6. 2: IoT Participants relationship framework

6.2. IoT Security Framework Functional Building Blocks

The functional viewpoint of the security framework comprises five interacting building blocks, as shown in Figure 6.3. They are organized into three layers. The top layer comprises the three participants (end user, service provider and developer) with core security functions: endpoint protection, communications and connectivity protection, security monitoring and analysis, and security configuration management. These functions are supported by a system-wide security model and policy layer which also shows the direction at which these functions are implemented.

The security of the IoT ecosystem is centered on end user, as shown in Figure 6.3. The model shows that the roles of both service provider and IoT developer are all about making life easy for the end user, securing the end user's data and the IoT itself. By so doing, both participants achieve their interests such as competitiveness. The securer as briefly defined in Section 4.2 played its role which is targeted towards the developer, service providers and end user by making research, developing policy and creating awareness of threats to IoT ecosystem.

Security model and policy governs how security is implemented and the policies that ensure confidentiality, integrity and availability and other security parameters of the system throughout its lifecycle. It orchestrates how all the functional elements work together to deliver cohesive end-to-end security.

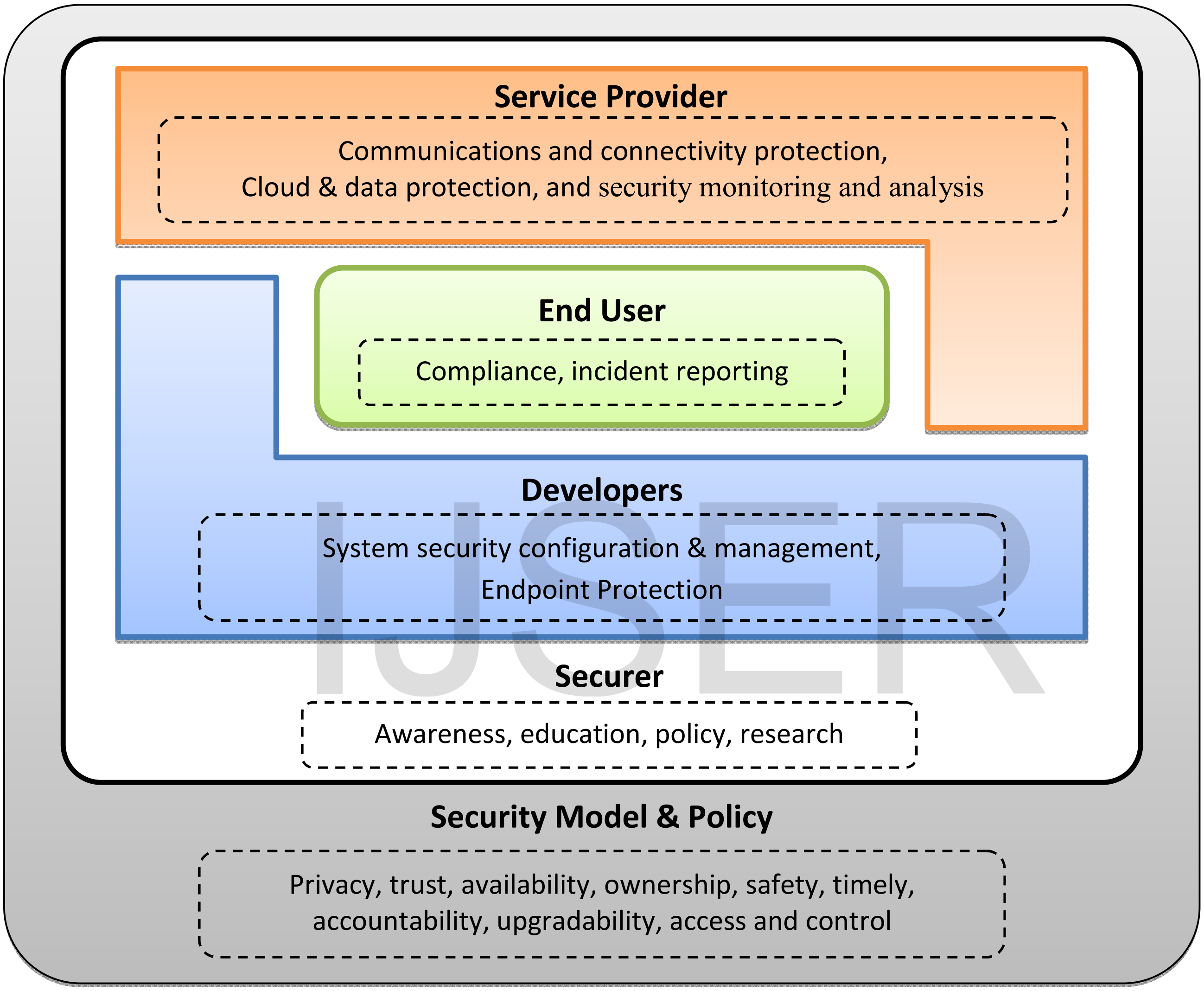
Service Provider
Communications and connectivity protection,
Cloud & data protection, and security monitoring and analysis
End User
Compliance, incident reporting
Developers
System security configuration & management,
Endpoint Protection
Securer
Awareness, education, policy, research
Security Model & Policy
Privacy, trust, availability, ownership, safety, timely,
accountability, upgradability, access and control

Figure 6. 3: IoT Security Framework Functional Building Blocks

7. Summary

The Internet of Things (IoT) promises to deliver a step change in individuals' quality of life and enterprises' productivity. Through a widely distributed, locally intelligent network of smart devices, the IoT has the potential to enable extensions and enhancements to fundamental services in transportation, logistics, security, utilities, education, healthcare and other areas, while providing a new ecosystem for application development. The transition from closed networks to enterprise IT networks to the public Internet is accelerating at an alarming pace—and justly raising alarms about security. As we become increasingly reliant on intelligent, interconnected devices in every aspect of our lives, how do we protect potentially billions of them from intrusions and interference that could compromise personal privacy or threaten public safety?

As every player with a stake in IoT is well aware, security is paramount for the safe and reliable operation of IoT connected devices. It is, in fact, the foundational enabler of IoT. Where there is less consensus is how best to implement security in IoT at the device, network, and system levels. Network firewalls and protocols can manage the high-level traffic coursing through the Internet, but how do we protect user' privacy, this is paramount.

We consider smart metering in our scenario, many players are involved; the power supplier, the maker of the meter, the cloud system manager and the customer. IoT comes with a lot of security challenges. However, we attempt to seek security approach that ensures user's privacy. The user' information such power usage and the analysis of appliances used in a household should not be exposed to the third party without the permission of the customer.

8. Conclusion

IoT security requires the support of all participants in the ecosystem except the attacker. Having surveyed some existing solution, model or framework, they all lack the quality of privacy assurance as our orientation is towards protection of user's privacy. However, it is obvious new system is borne out of the existing one. We can therefore use them as motivated background for our upcoming work.

9. Recommendation

We recommend a relevant research line in IoT security that directed, through participant-driven approach, towards user's privacy assurance. Similarly, the existing IoT security policy should be enhanced to consider privacy enhancement through techniques such as the use of pseudonyms, anonymous assertions or permission control through acknowledgement technique. Also, we recommend new protocol for acknowledgement of permission for critical information disclosure.

Reference

[1]. Australia, I. A. (2017). Internet of Things Security Guideline *Workstream 5 Security and Network Resilience of the IoT Alliance Australia (IoTAA), V1.0.*

[2] Eduard, K. (2017). Smart Meters Pose Security Risks to Consumers. *Utilities: Researcher. Security Week, Internet and Enterprise Security News, Insights and Analysis*.

[3] Engineering-and-Technology-Publishing, E. (2012). Smart Grid Security: Threats, Vulnerabilities and Solutions. *International Journal of Renewable Energy and Smart Grid (IJRESG), Vol. 1*(No. 1).

[4] Gloria, D. (2016). Strategic Principles For Securing The Internet of Things (IoT). *U.S. Department of Homeland Security - US-CERT IRT Concept of Operations, Version 1.0*.

[5] GSM-Association. (2014). Understanding the Internet of Things (IoT).

[6] Jayavardhana, G., Rajkumar, B., Slaven, M., & Marimuthu, P. (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. *Article on Internet of Things (IoT).*

[7] Karen, R., Scott, E., & Lyman, C. (2015). The Internet of Things: An Overview - Understanding the Issues and Challenges of a More Connected World. *Internet Society*.

[8] Liwei, R. (2015). *IoT security: Problems, Challenges and Solutions.* Paper presented at the SNIA Data Storage Security Summit.

[9] Maribel, L. (2013). An Introduction to the Internet of Things (IoT) - Part 1 of *The IoT Series. Lopez Research.*

[10] Murrill, B. J., Liu, E. C., & II, R. M. T. (2012). Smart Meter Data: Privacy and Cyber security. . *Congressional Research Service; USA. 2012; 1–45*.

[11] Nenad, A. (2016). Security in Smart Grid. *IoT - Comtrade Solutions Engineering*.

[12] Ovidiu, V., & Peter, F. (2013). *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*. River Publishers Series In Communications.

[13] Silicon-Laboratories-Inc. (2013). Smart Metering Brings Intelligence and Connectivity to Utilities. *Green Energy and Natural Resource Management*.

[14] Sven, S., Hamed, S., Jesus, M., C Jeff, David, M., Frederick, H., Jean, P. L., & Marcellus, B. (2016). Industrial Internet of Things Volume G4: Security Framework I. *IC:PUB:G4:V1.0:PB:20160919*.

[15] Trong, N. L., Wen-Long, C., Dang, K. T., & Tran, H. N. (2016). Advanced Metering Infrastructure Based on Smart Meters in Smart Grid. *Intech - Open science, open mind*.

[16] Wind-River-Systems-Inc, W. (2015). Security in the Internet of Things - Lessons from the Past for the Connected Future. [Retrieved from Wind River at www.windriver.com.]. *White Paper*.