A Method and Framework for IoT Network Security

A Technical Paper prepared for SCTE•ISBE by

Umamaheswar Achari Kakinada
Principal Engineer, Wireless R&D
Charter Communications, Inc
6360 Fiddlers Green, Greenwood Village, CO 80111
847-544-6560
Achari.Kakinada@Charter.com

Dr. Hossam H. Hmimy
Sr. Director – Wireless R&D
Charter Communications, Inc.
6360 Fiddlers Green, Greenwood Village, CO 80111
720-536-9396
Hossam.Hmimy@Charter.com

Manish Jindal
GVP – Wireless R&D
Charter Communications Inc.
6360 Fiddlers Green, Greenwood Village, CO 80111
303-793-4486
Manish.Jindal@Charter.com

Table of Contents

Title **Page Number**

List of Figures

Title **Page Number**

1. Introduction

The Internet of Things (IoT) is connecting any device or “thing” to the Internet. These devices include sensors, actuators, machines and wearables that are capable of collecting and transmitting data about location, activity, situational awareness, environmental activity, etc., to allow autonomous or real-time changes that can enhance or optimize everyday activities.

The number of “things” connected to the Internet is growing at nearly an exponential rate and delivering data about everything from the temperature of an industrial refrigeration unit, to household water consumption, to your heart rate. Each one of these “things” is a doorway into a larger network. Together, these generate colossal amounts of data and can add enormous value to many spheres of society. To realize this value, these things and the systems they are connected to and the data that is generated must be reliable and trustworthy. Thus, it is of paramount importance to secure the things, associated systems and the data generated.

More and more connected devices are being deployed, and a threat or security breach in one area or in one device can have a domino effect on other devices connected to that same network. Potential damage can extend past the network and the data. Finances, reputation, brand and disruption of city services are just some of the areas to be considered in a security assessment to mitigate potential risk. We’ll discuss how devices and networks can—and should be—protected as part of an overall strategy of sensor deployment, data collection and analysis.

The Industrial Control Systems (ICSs), which preceded today’s IoT systems, existed in silos and used proprietary protocols, networks and technology. Conventional network and system security were provided by establishing a perimeter around the entities which needed to be safeguarded. Once established, firewalls, intrusion detection and prevention systems served as the foundation for security and virtual private networks provided a tunnel into the network. But IoT is drastically reshaping how applications and ICSs operate and are secured.

Current IoT devices have ubiquitous connectivity to the network using open standards, which no doubt is beneficial in providing rich functionality, but enhances threat surface significantly. The network, the things, the associated systems and applications need to be secured. IoT induced reshaping is based on the differentiators in an IoT network versus conventional ones. The differentiators individually impact security, but, when combined, portend exponential security threats and subsequent impacts. Key IoT differences include:

(1) The network topology is ever expanding, pushing the boundaries of the network with the constant addition of functionalities, applications, devices and equipment.
(2) With the constant network expansion, more functionality gets incorporated in to the edge of the network. While edge computing has many advantages, including improved response time and localized services and processing, it exposes the network as a whole to significant vulnerabilities.
(3) Diverse functionalities/applications require different levels of authorization and access to data and systems in the network, edge and backend systems. Improper use of authorization and access or providing blanket permissions to a large number of systems may make the entire network vulnerable.

(4) There is shared multi-tenant cloud usage for compute and storage. Vulnerability of any service or user in any part of the network can impact the entire network.
(5) Critical infrastructure in factories, utilities, cities, etc., can be managed and operated from mobile consoles and personal devices, which brings additional security challenges.
(6) Due to perpetual addition of new applications and functionalities, the network is in a continuous state of flux.
(7) State, federal and international data privacy and security regulatory compliance requirements, under the Federal Trade Commission's (FTC) privacy framework and Federal Trade Commission Act ("FTC Act"), the California Consumer Privacy Act (CCPA), the European Union's (EU) General Data Protection Regulation (GDPR), city/state specific regulations etc., mandate operators/utilities to ensure data security and privacy over a broad range of personal information and/or data.

Ultimately, the highest level of security is paramount, and the network is only as secure as the weakest connected device, with the quantity of devices expanding and changing daily (theoretically). Furthermore, conventionally used perimeter-based security measures (e.g., firewalls, De-Militarized Zones (DMZs), etc.) are not sufficient for IoT networks as one has to consider both fixed IoT devices (e.g., water meters) and mobile IoT devices (fleet management) that extend the edge and make it dynamic. For example, government employees leveraging mobile IoT devices frequently access critical infrastructure networks in cities and utilities. Malicious access through one of these IoT devices could cause catastrophic network effects.

Compounding security problem are data flows (from sensors through networks to public clouds and third-party devices and services) outside of service provider or network operator control. This adds additional dimensions for IoT data security. For instance, data exchanged with water meters by a utility over an operator's network needs to be secured and protected for privacy across all the segments during transit and storage. It requires clear delineation of responsibilities and adherence to protocols for secure operation and management of the devices in transit and data generated from these devices. Not only is the IoT infrastructure itself exposed, but citizens' personal information (PI) could also be exposed, which could be out of compliance with data security and privacy regulations such as California Consumer Privacy Act (CCPA) and General Data Protection and Regulation (GDPR).

According to some industry studies, IoT security still comes up as the number one deterrent to IoT adoption year after year.1] Having mentioned different vulnerabilities of an IoT network and its impact on network security, we'll now discuss the approaches that may be adapted to mitigate some of these concerns.

IoT devices are relatively inexpensive, have ubiquitous connectivity to the critical network infrastructure, possess enough compute and storage, but probably are not ruggedized enough from a security perspective. This makes them attractive for rogue players with malicious intent to potentially harm the network systems, applications and critical infrastructure. A case in point— in 2016, in one of the infamous IoT DDoS attacks, a botnet infected nearly 65,000 devices in its first 20 hours, doubling in size every 76 minutes. [2] Before eradicated, it infected thousands of devices globally and halted the Internet for a portion of the U.S. for some time.

Cloud computing has become pervasive with many domains, including IoT, rapidly adapting to it. Cloud computing is attractive in providing flexibility in deployment, providing scalability and is cost effective. Also, the multitenancy aspects of cloud are especially attractive as it is an enabler for scaling different applications or verticals of the IoT network independently. However, as some recent incidents[3] across many organizations, including the US Navy, major corporations and more than a dozen cloud providers globally have shown, vulnerability in one segment can be exploited to impact other parts of the network. Even if one maintains one's own network diligently from a security perspective, it may still become a victim of vulnerability of a different entity in the shared cloud. The sensitivity level of the data may trigger regulatory compliance requirements or create enhanced risk if not properly secured under the FTC's privacy framework or GDPR. Private and hybrid clouds are also not immune from this problem by virtue of their accessibility needs over a public network.

Having mentioned different vulnerabilities of an IoT network and the impact on network security, now let us discuss the approaches that may be adapted to mitigate some of these concerns.

2. Proposed IoT Security Framework

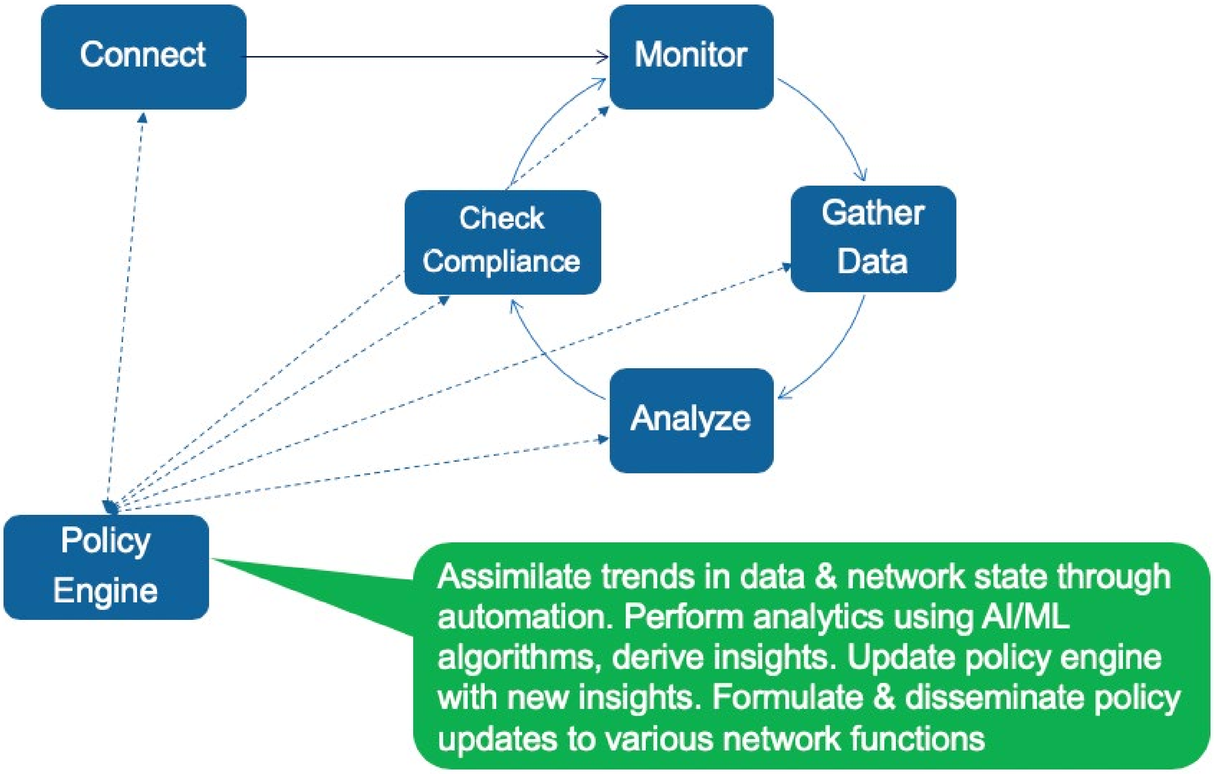

Connect
Monitor
Check Compliance
Gather Data
Analyze
Policy Engine
Assimilate trends in data & network state through automation. Perform analytics using AI/ML algorithms, derive insights. Update policy engine with new insights. Formulate & disseminate policy updates to various network functions

Figure 1 - IoT Security Life Cycle

As depicted above, each entity in the IoT network should be provided with *minimum viable access* (to connectivity, bandwidth, amount of data transmitted and frequency of transmissions, authorization to connect to systems and access to data). All this should be continuously monitored through an automated process to gather the data, analyze to discern insights and identify anomalies. The policies need to be updated based on gathered insights, observed trends in data and operator input. This minimal viable access and compliance with policies for each entity, including devices, edge compute nodes or more complex core/access network functions, forms the foundation of IoT network security.

To illustrate the importance of this point, it may be noted that in 2017 a casino lost its high roller database through the network connectivity provided for a fish tank. [4] The fish tank had sensors connected to a PC that regulated the temperature, food delivery and cleanliness of the tank. This vector was used to steal the high roller database. Needless to say, a temperature control system for a fish tank does not need, and should not have had, any possible connectivity to critical data, and it is a failure of formulating and enforcing effective security policies (e.g. minimal viable access to connectivity, data and authorization).

It is important to recognize that, network security is ***not*** an isolated standalone function, rather it is an overarching, all-encompassing characteristic of a system. As the saying goes, a given system is only as secure as its weakest constituent component. It is imperative that the security of the entire system be looked into as a whole, not as individual isolated components.

2.1. Connect:

The diversity and volume of IoT use cases are numerous. Equally large are associated devices, network components and diversity of their connectivity needs. This diversity certainly increases the threat surface area, variety of threat vectors and vulnerabilities. To mitigate this risk, a strong connectivity policy needs to be created and enforced. The policy should be customizable and consider the characteristics of each device, the evolving trends in the network, the availability of the network resources, the relative priority and criticality of various functions and their connectivity needs. This can be arrived at after a thorough analysis of various components in the network and building a subsequent enforcement framework.

2.2. Monitor:

The diversity of devices and network functions in an IoT network have different capabilities and provide different metrics to gauge and monitor these capabilities. The monitoring function needs to consider a profile for each entity (devices, edge/core/access network functions) and create a set of characteristics to be monitored and adapt these characteristics to evolving conditions in the network. Some of these may be conditional on meeting certain thresholds in different areas.

Continuous monitoring of the different aspects of the network, such as traffic patterns, directions of data flow, any norm breaking trends in data or traffic, and evolution in the network are key to highlighting the existence of potential security threats and identifying them. Today’s network technologies also offer greater visibility into application and device activity. Software designed to detect anomalous behavior at the network level, revealing Distributed Denial of Service

(DDoS) and other attacks, can now leverage artificial intelligence (AI) and machine learning (ML) to respond. Changes in behavior at the application and device level can raise alerts.

2.3. Analyze:

The IoT network is diverse in topology and in its constituent network elements. The security issues often cannot be detected or identified by looking at the snapshot of the network at any given time in isolation. It requires a thorough analysis of data gathered from the above mentioned continuous monitoring of the different aspects of the network. The analysis needs to examine not only individual snapshots of the network, but also needs to correlate data points from different parts of the network and across different points in time to identify any emerging trends and discern insights. The insights derived may lead to the addition of new policies or updating existing policies.

2.4. Compliance:

This is a gating function, which ensures all entities in the network adhere to respective policies and rules that need to be enforced strictly without exception. Any updates needed to these enforcement rules should come through the policy engine after careful analysis of the impact of the proposed changes across the entire network based on available data and/or operator input. Automation of policy adoption and enforcement is critical for ensuring continued compliance and building resiliency into the process. Automation also helps recognize and address shifting trends in the network.

2.5. Improvement cycle:

The IoT Security Life Cycle is a continuous improvement cycle. The accumulation of data and analytics previously mentioned and the correlation of different data points across time and different parts of network provide insights about the network and applications in their current state, as well as for emerging trends in the future. These insights can be used to mitigate current threats and plan for, and address, any emerging threats in the future even before these are materialized.

The improvement cycle comprises identifying potential threats and fine-tuning security policies to adapt to the perceived and emerging threat vectors, based on the insights gathered from analysis and correlation of various data points. This process of keeping the security policies in sync with current and emerging needs of the network allows for continuously updating the policy engine based on the insights. This can also make the network more efficient by eliminating any redundancies, in addition to enhancing the robustness of the network. In summary, this continuous improvement process helps to mitigate security threats of the IoT network, constituent devices, supported applications and enables realization of value of five Vs *(volume, velocity, variety, veracity and value)* of IoT data generated and processed.

3. IoT Data : Security, Inegrity and Ownership

People now often say that data is the new oil. However, it doesn't fully characterize the value of IoT data. To quote Adam Schlosser of the World Economic Forum, "unlike oil, the value of data doesn't grow by merely accumulating more. It is the insights generated through analytics and combinations of different data sets that generate the real value." [5]

IoT data promises to convey more useful information than ever before, and the volume and velocity could improve the speed and accuracy of all sorts of business and strategic decisions significantly. Reliability and security of data is essential to make the available information actionable. IoT data security, integrity and ownership are the building blocks of this trust and are of paramount importance.

3.1. Security and Integrity:

As described previously, IoT networks comprise a diverse collection of devices, and applications on the network are evolving and generating enormous amount of data. The security solution for this dynamic, ever-evolving network cannot be static. The security policies, framework and measures need to adapt to this diversity in devices and applications. We propose the following framework for securing IoT data and ensuring its integrity:

- The data shall be secured while it traverses through the network across different network elements, including end to end.
- A chain of custody shall be established for the data generated from the point of origin until it is processed/transmitted/stored.
- There may be different stakeholders for each segment of the network, such as device-users, access network providers, core network providers, application server providers, etc.
- There are clearly delineated responsibilities and expectations for each of the stakeholders regarding how to handle the data as it enters the entity and how the data gets processed and leaves the entity.
- Any two entities exchanging data shall have a *security association (SA), minimum viable connectivity, access and authorization driven by the security policy,* which may differ in each direction of data transfer.
- The overhead associated with above mentioned security association and chain of custody is not cumulative and additive for each piece of data transferred across this interface.
- All data is secured in transit and storage. The data security shall include both ciphering and integrity protection as dictated by the security policy.
- Each entity in the network shall have no more visibility and authorization than absolutely necessary to perform its function. This applies to data as well as other network resources.
- AI/ML based algorithms shall be used to correlate different metrics in the network to detect and mitigate any suspicious activity.
- A process is established to isolate and quarantine the impacted applications, devices and segments of the network through a rapid response system.
- A security model shall be adopted to create micro-segments and enable granular enforcement of security policies. This model shall be used to manage data and devices, and migration of data across different components, both external and internal

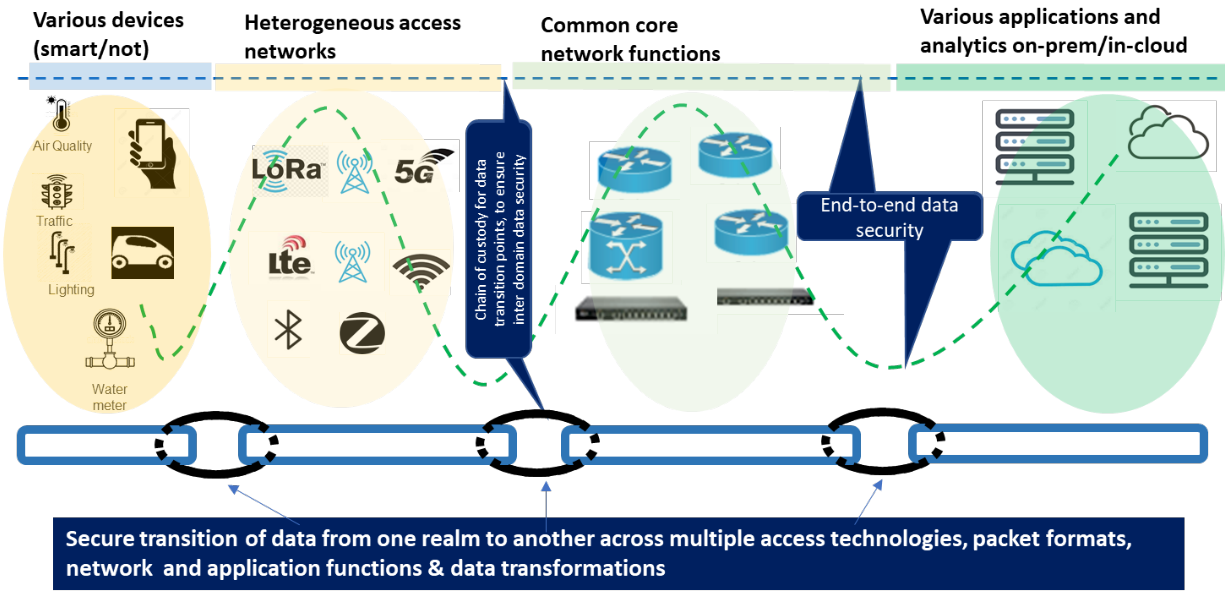
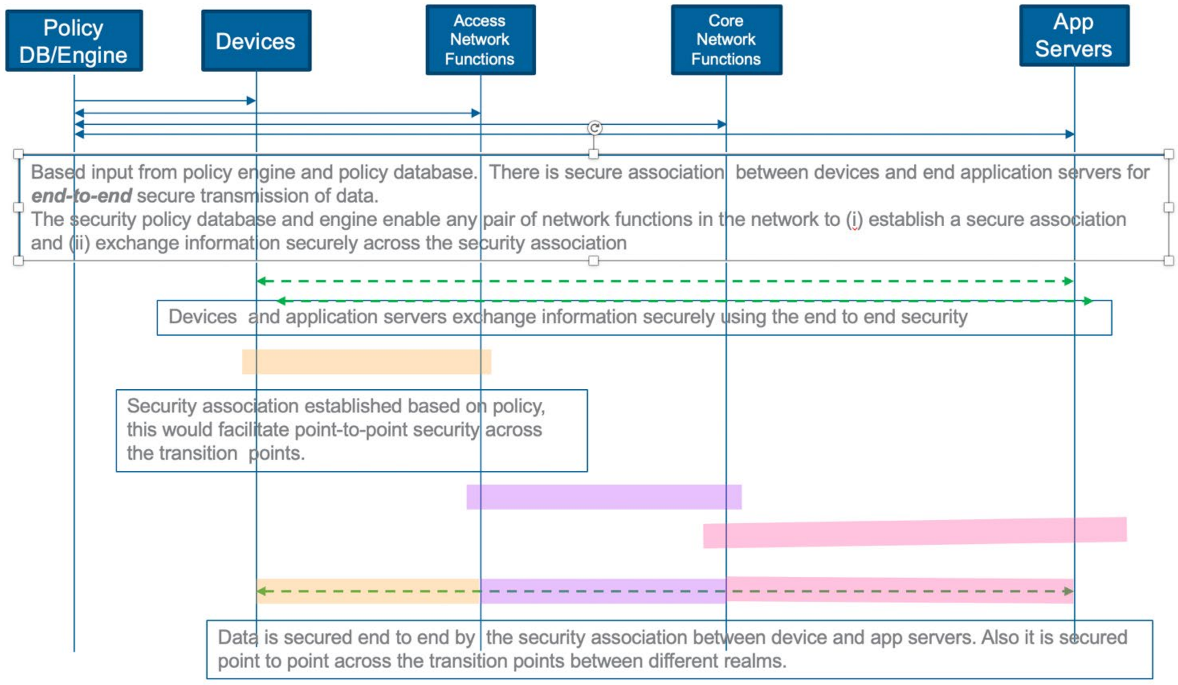

Various devices (smart/not)
Heterogeneous access networks
Common core network functions
Various applications and analytics on-prem/in-cloud
Air Quality
Traffic
Lighting
Water meter
LoRa
5G
Lte
Chain of custody for data transition points, to ensure inter domain data security
End-to-end data security
Secure transition of data from one realm to another across multiple access technologies, packet formats, network and application functions & data transformations

Figure 2 - Chain of Custody for IoT Data Security

To establish this chain of custody (CoC) for the data as it traverses through the network across different network elements, access/segment specific methods shall be used. For resource constrained (i.e. low bandwidth, smaller payloads, high latency) segments of the network, access segment specific methods are needed. Any two entities exchanging data shall have a *secure association, minimum viable connectivity, access and authorization driven by the security policy.* For the segments of the network, based on the sensitivity of the data and availability of bandwidth, a blockchain-based method may be adapted. It may be noted that the distributed ledger/blockchain based methods are suitable for IP networks and have cumulative overhead for securing the data. Our proposed method is adaptable to different access technologies and transport methods and does not incur cumulative overheads. However, the proposed chain of custody is complementary to blockchain-based technologies. To secure data in any given segment of the network, blockchain-based methods may be adapted within this framework.
A robust set of security policies shall be formulated taking the above into account. The more granular these policies are, the more fine-grained control it provides on different aspects of data, applications and network. Automation is key to ensuring persistent compliance with established security policies with aforementioned characteristics.

Below is an illustration of messages and information exchanged between different entities in the network to establish a policy driven chain of custody for secure exchange of data without incurring cumulative overhead.



Based input from policy engine and policy database. There is secure association between devices and end application servers for ***end-to-end*** secure transmission of data.
The security policy database and engine enable any pair of network functions in the network to (i) establish a secure association and (ii) exchange information securely across the security association

Devices and application servers exchange information securely using the end to end security

Security association established based on policy, this would facilitate point-to-point security across the transition points.

Data is secured end to end by the security association between device and app servers. Also it is secured point to point across the transition points between different realms.

Figure 3 - Message Flow for Chain of Custody for IoT Data Security

3.2. Ownership:

Data is an asset. With IoT, data is collected and acted upon at different points within the larger IoT framework. The stakeholders for different parts of the framework may be different. For this reason, it is essential that ownership of different aspects of the data and its visibility among the stakeholders is clearly defined upfront.

As an illustration, consider autonomous/connected vehicle data. Vehicle manufacturers, the companies that produce the individual components, telecommunications providers and possibly insurance companies may all want the data produced during an operation. Meanwhile, the vehicle owner might have qualms about sharing personal data. In any event, there's value in that data, and, naturally, each stakeholder desires to capitalize on it.

With Smart Cities, data ownership is further complicated. In addition to different stakeholders like utilities, consumers, etc., city projects may have regulatory compliance requirements, as well as implications associated with public funding of city projects. Unlike the enterprise data, public funding of various city projects often triggers various concerns of the public's right to information aspects for the city's IoT data. Usage, disclosure and monetization of this data may have additional constraints. To avoid any confusion about the ownership of data and insights derived from it, it is imperative to establish upfront roles, responsibilities and rights as to the ownership of data among all stakeholders at the beginning of the project.

4. Standards support

Technologies like IoT evolve faster than related standards. What makes IoT unique is that standards are required for multiple enablers such as communications, semiconductors, devices, privacy and security to name a few. Standards are also the foundation for interoperability. The faster they can be defined and adopted, the faster IoT systems will deliver potential advantages. The IoT standards for access networks, security and core functions are at various stages of evolution.

In a report titled *Hype Cycle for IoT Standards and Protocols, 2020,* [6] Gartner states "we still see many standards overlapping, or competing directly, especially in areas with large commercial potential. There are also areas of the IoT in which standards are incomplete or lack full stack support. Consequently, new standards will continue to emerge in the coming years." Currently available security standards from various standards bodies such as LoRa Alliance, 3GPP, IETF, NIST, GSM-A, etc., can be leveraged, adapted and enhanced to secure an IoT network. These standards, originating from diverse standards bodies, were originally intended to address different needs. Adaptation of these for securing an IoT network requires a thorough analysis of the network being secured, configuring, customization and integrating these protocols together to address the specific needs of the IoT network under consideration.

5. Conclusion

There are many challenges in the rapidly evolving IoT applications, network and devices with huge amounts of data generated. Security is of paramount importance among all of these. To realize the promise and potential of the IoT network, it is clear that the data generated and needed to be acted upon must be secured and trusted. Ownership is an imperative and requires clear and upfront delineation of roles and responsibilities of all stakeholders.

6. Acknowledgements

The Authors would like to express sincere gratitude to Mr. Satya Parimi and Ms. Patricia Zullo for their time and effort for many cycles of reviews, industry insights and valuable suggestions for improvement.

Abbreviations

3GPP	3rd Generation Partnership Project
AI	Artificial Intelligence
CCPA	California Consumer Privacy Act
CoC	Chain of Custody
DoS	Denial of Service
DDoS	Distributed Denial of Service
GDPR	General Data Protection and Regulation
GSM-A	Groupe Speciale Mobile(GSM) Association
IETF	Internet Engineering Task Force
IoT	Internet of Things
LoRa	Long Range
ML	Machine Learning
NIST	National Institute of Standards and Technology
PI	Personal Information
SA	Security Association

Bibliography & References

1. "*IoT Security is Still a Major Barrier to Adoption*," Kathryn Weldon, Global Data, https://itcblogs.currentanalysis.com/, March 21, 2019
2. "*Inside the infamous Mirai IoT Botnet: A Retrospective Analysis."* Elie Bursztein. Cloudflare.com, December 14, 2017. https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/
3. *"Ghosts in the Clouds: Inside China's Major Corporate Hack"*, Rob Barry and Dustin Volz. Wall Street Journal, December 30, 2019: https://www.wsj.com/articles/ghosts-in-the-clouds-inside-chinas-major-corporate-hack-11577729061
4. "*How a fish tank helped hack a casino*," Alex Schiffer, Washington Post, July 21, 2017**:** https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/
5. "*You may have heard data is the new oil. It's not*," Adam Schlosser, World Economic Forum, Jan 10, 2018, www.weforum.org/agenda/2018/01/data-is-not-the-new-oil/
6. Gartner, Inc. "Hype Cycle for IoT Standards and Protocols, 2020," Bill Ray, June 30, 2020