ISSN 2047-3338

Use of 5G Network and Standardization of Frameworks to Enhance Security of IoT Systems

Ajwang, Stephen Oloo

Department of Informatics and Information Science, School of Information Communication and Media Studies, Rongo University, P.O. Box 103-40404, Rongo

oloohs@gmail.com

***Abstract*– Internet of Things (IoT) has advanced over the years as a result of convergence of various technologies brought about by the increasing availability of embedded systems, pervasive computing and big data. IoT uses sensor technology and data analytics capabilities to transform data to actionable intelligence for business, transport, manufacturing, automotive and smart cities. Despite its widespread adoption, IoT devices have increasingly become a target for cyberattack because of the huge amount of valuable data they carry, lack of standard development framework, closed loop functioning ability, open and concurrent access of the system by data consumers and data controllers, and the inherent memory constraints. This paper therefore evaluates the strength of the available security protocols provided by AWS, Azure and Arm Mbed IoT frameworks and recommends enhancement of the security of the IoT devices through standardization of frameworks at technology and regulatory level to manage common security goals of confidentiality, integrity and availability. The paper also recommends the use of 5G 3GPP standards to secure IoT devices by leveraging its network capabilities such as ultra-low latency, reliability, reusability modularity and self-containment of network functions for consumer protection and network resilience.**

***Index Terms*– Internet of Things, Security, Frameworks, 5G Networks and Convergence**

I. INTRODUCTION

A) Internet of Things (IoT)

According to CISCO [1] about 50 billion IOT devices will be connected through machine to machine (M2M) [2], Machine to Human communication (M2HC), Radio Frequency Identification (RFID), Location-Based Services (LBS), Lab-on-a-Chip (LOC) sensors, Augmented Reality (AR), robotics and vehicle telematics by 2020. This is a substantial increase up from the projected 8.4 billion devices in 2017 [1]. The growth has been facilitated by the increasing availability of handheld devices, personal computers, ubiquitous computing and low storage. It has also been enabled by the availability of homogenous and big data that reside in the new technologies of social, mobile, analytics and clouds platforms. IoT are characterised by mobile, scalable, interoperable and resource constraint devices [3].

IoT devices integrates data from various sources and applies analytics tools to provide highly specialized data driven decision [4]. IoT comprises many different components each performing critical role in the IoT ecosystem. The components are: the devices (which provide the "things") connected to sensors and other components; the field gateway which act as the connection point between cloud and other devices for communication and protocol translation; cloud gateways for cloud hosting of the IoT systems; and services such as REST APIs and databases. IoT devices are implemented through the internet protocols which are easy to install, scalable and interoperable thereby becoming increasingly applicable in sharing data [5]. Also the Universal Plug and Play (UPnP) [6] feature of IoT allows networked devices to automatically find, communicate and share data.

IoT components are embedded intuitively to build an interactive system capable of autonomous sensing and responding to stimuli from the real world without human intervention [7]. This provides an aura of convenience, efficiency and real time data analytics but also create platform for shared risk due to multiple, open and concurrent access by data consumers and controllers. IoT devices have increasingly become a target for cyberattack due to the amount of valuable data it holds and its closed loop functioning ability [8]. The typical small sizes of IoT devices also limits hardening of security compute capabilities and onboard encryption algorithm to the devices. IoT systems are built on different frameworks [9], [10] further compromising enforcement of security standards in protecting the devices. Therefore, there is need for a secure standard framework over which IoT solutions are built.

B) Security requirement for IoT

The interconnectivity of devices, UPnP and the unlimited flow of large volumes of data within IoT system result into several technical and operational challenges such as integration, scalability, security, privacy and interoperability [11]. However, typical IoT systems should guarantee

confidentiality, integrity, availability access controls mong other critical concepts of security as discussed below:

Privacy

Confidentiality

IoT devices may contain sensitive data held in confidence within IoT environment. Confidentiality can be achieved through symmetric and asymmetric encryption schemes depending on the application and device capability

Integrity

The value and usability of data is synchronous to its applicability across various devices, networks and analytical framework. The loss of data integrity in some IoT system can be life threatening e.g., data failure in industrial IoT or healthcare can prove fatal. Therefore, data in IoT system must be error free and consistent either on transit, at storage or in use.

Availability

IoT system consist of hosted services such as data, device and connectivity services which must remain available all the time to provide information continuously. The security protocol implemented by IoT must protect the system from threats such as denial of service (DoS) attack that may impede service availability.

Authentication

IoT system must provide capabilities for verifying user identity through mutual authentication. The service providers and users must remain assured that the services being accessed are offered by an authentic source. Strong authentication helps in preventing spoofing attacks. Typically, IoT systems will register user identities and resources thus creating authentication constraints.

Authorization

This is a means of expressing access policies by assigning permission and privileges to system users. IoT ecosystem should provide fine grained, reusable, dynamic, easy to use policies, defining and updating mechanism and the applicable limitations/constraints.

Access control

This is whereby only authorized users are allowed access to IoT resources. This will protect and secure the information and data available in the system from unauthorized access. For example, a smart transport system may have private data about road users which if accessed by unauthorized users may lead to leakage of personal data on traffic offenses.

Trust worthiness

Application of IoT in sensitive spheres of life such as autonomous vehicles require high sense of trust worthiness.

Auditing

A secure system should keep track of usage statistics by logging user activities. This will help in error detection and correction. This can be achieved by ensuring that the system logs details of users who have accessed the system, the resources accessed, time and date of access.

C) Security challenges in IoT

Secure and reliable IoT infrastructure is an integral part of security enhancement in IoT systems as compared to other IT devices. However, the security aspect of IoT is challenged by several factors including complexity of distributed systems, multi-programming languages, varied communication protocols and lack of standardization of IoT frameworks [12]. According to Symantec [13], about 600% increase in cyber-attack and over 24,000 malicious application have been blocked in mobile environment daily. Other factors include:

Constrained memory: the limited capability of devices hampers implementation of complex security algorithms and logical operations which require higher processing power ultimately reducing the CPU cycles.

Back up: IoT systems are built to operate in autonomous environment without alternative back-up systems, therefore, whenever primary connection is lost, then the accessibility of the system will be compromised.

Management of IoT systems: IoT ecosystem comprises billions of interconnected devices whose management can pose challenges.

Internet Protocol: IP devices have default settings and configurations which can be easily ignored by users during system installation thus becoming a target for cybercrimes such as TheMoon which was discovered in 2014 and Persirai discovered in 2016 [14].

The automated protocols of UPnP can bypass firewall and introduce malware to the router thus creating a gateway for malicious programs such as Mirai and EternalSilence botnets discovered in 2016 and 2017 respectively to attack the IoT system [14].

To cope with some of these security challenges in IoT, devices should provide authentication, authorization, confidentiality, privacy and integrity of information. According to Internet of Things Cybersecurity Improvement Act, 2017 [15], the United States directed that vendors of IoT systems must provide list of all system security vulnerabilities, capability of the system to accept properly authenticated updates, and uses only non-deprecated standards protocols and functions to communicate, encrypt and interconnect with other devices. The Act also provides that there is need for clear documentation of how the device receives security updates and timelines for receiving vendor security support.

To enhance security of IoT systems, its required that the systems are free from fixed or hard-coded credentials for remote access and updates. During the design of the system, security protocols [16] should be embedded in the system which may be updated and activated by users before initialization of the IoT system. Some of the security protocols that can be embedded in the systems include: the public key infrastructure (PKI) to encrypt, secure data exchanges and verify identity; Application Performance Indicator (API) to protect integrity of data over networks; unique identification of each devices; end-to-end hardening of devices; protection of networks; provision of inventory of IoT devices as network access control (NAC) procedure; and continuous patch management and software updates [17].

The emergence of consumer protection has necessitated the need for enhanced security of IoT. According to FTC [18], protection of privacy data has become invaluable due to the availability of large volumes of data. OECD [19] found out that protection of privacy is built on the principles of collection limitation, data quality, purpose of data collected, authorization of the use of data, security against unauthorized access, data destruction, uses of data, modification or disclosure of data availability and openness about personal data and dissemination of required data.

II. REVIEW OF IOT FRAMEWORKS

IoT framework is the structural representation of IoT systems showing the coordination and control of functions and processes of IoT elements. The framework presents the relationship and the flow of data between various components (user, database, devices) of IoT system. This paper has reviewed three popular IoT frameworks as shown below:

A) AWS IoT

This is a cloud platform for IoT released by Amazon [20] to enable interconnected devices to securely interact with the amazon web services (AWS) cloud and other connected devices. The framework integrates artificial intelligence to provide functionalities and solutions to build any IoT device. The framework is scalable to allow expansion of requirements and can be used without the need for internet connectivity. It also allows creation of security features that can be defined within the system to respond to future security requirements [20].

The services provided by various components of AWS IoT include:

Data services which are provided by AWS IoT Analytics that provides big data analytics capability; Events which facilitates detection and response to events from IoT sensors and applications; SiteWise which helps in data capture, analysis storage and retrieval [20]

Control services provided by AWS IoT CORE which allows connected devices to securely interact with cloud applications and other devices; Defender which monitor and audit IoT configuration in accordance with security standards and protocols; Management which coordinates and control functionalities of devices within a network, Things Graph which provides platform for building IoT applications [20].

Device software such as AWS IoT greengrass and FreeRTOS that provides device connection and operation at the edge [20].

Security Feature in AWS IoT

AWS IoT provide a secure system for access and sharing of data. This has been achieved through:

a) Authentication identities principals of X.509 certificates, AWS IAM users, groups, and roles, AWS Cognito identities, and AWS federated identities [20].
b) Authorization and access controls based on authentication protocols and policies which controls the operations an identity can perform [21].
c) Secure communication through encryption of all messages over SSL/TLS protocols. TLS guarantees confidentiality of the application protocols (Message Queuing Telemetry Transport (MQTT), hypertext transfer protocol (HTTP)) supported by AWS IoT. [21]
d) Cross Account Access which allows cross subscription of functionally independent topics defined in AWS account and not owned by the principal.

Security limitations in AWS IoT

By limiting: the number of policies that can be attached to a certificate/amazon cognito identity; policy document size characters; policy versions; and the number of device certificate that can be registered per second, the system security can easily be breached.

B) ARM Mbed/Pelion IoT

This is scalable, connected and secure platform for developing IoT devices by integrating Mbed Tools and services. The platform is based on ARM microcontrollers which provides all requirements through its ecosystem to build either an IoT standalone applications or networked ones [22].

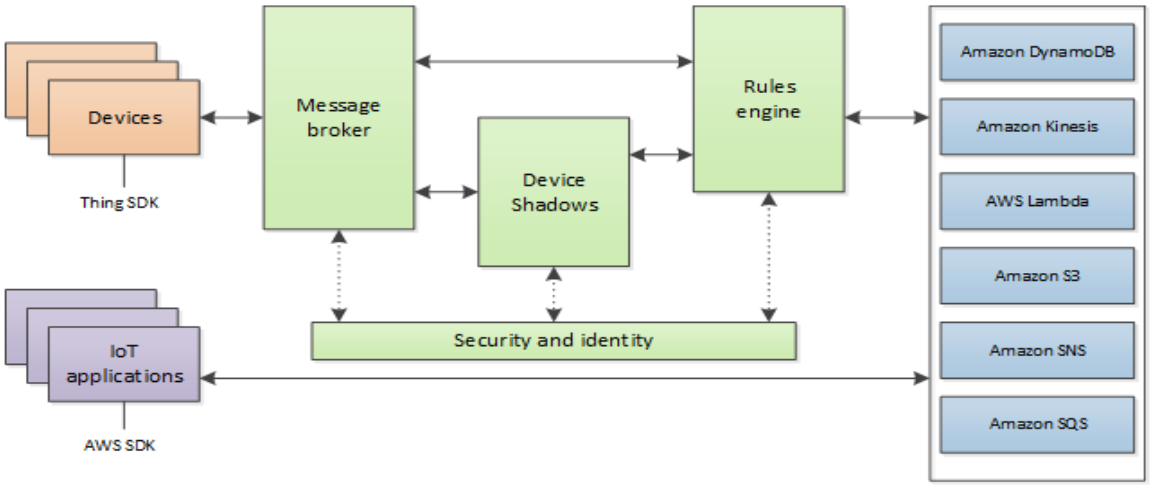

Fig. 1. AWS IoT Components/Services (AWS Inc. 2019)

Fig. 2. AWS IoT Security Framework (AWS Inc. 2019)

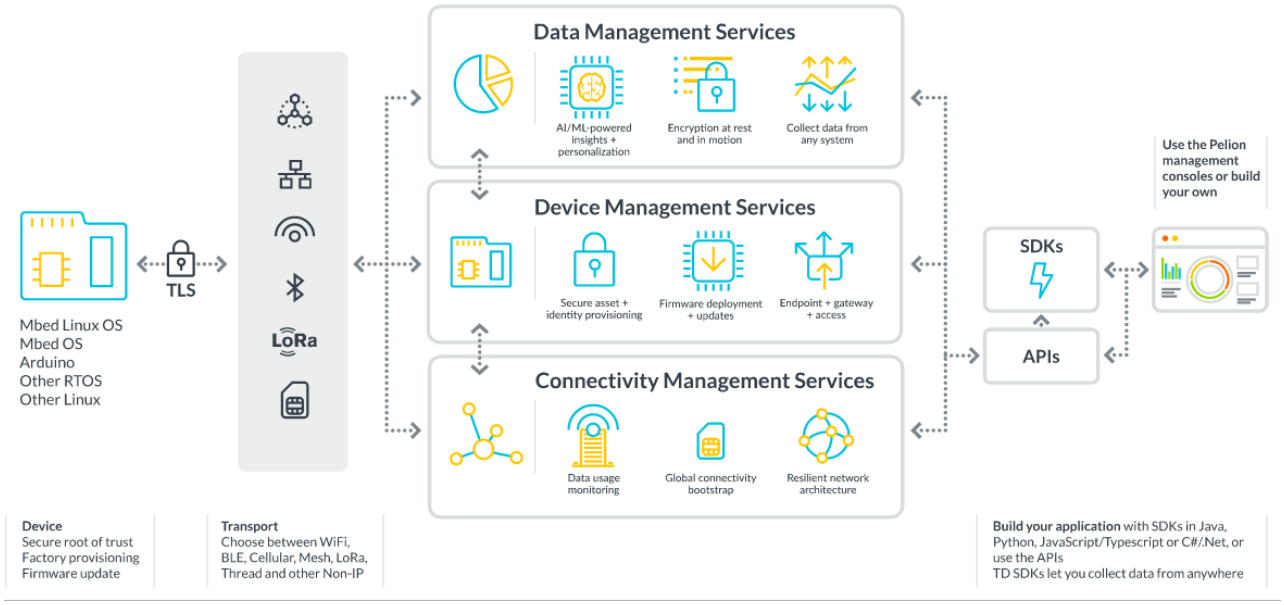

Fig. 3. Arm Mbed/Pelion Component/Services (Arm Mbed. 2019)

Components of Arm Mbed IoT

The platform consists of three core IoT services that can either be combined or applied separately depending on the product to be developed. The services are:

Data management services: big data has increasingly become available as a result of the growth of IoT device data. The platform utilizes Arm Treasure enterprise customer data platform (CDP) to flexibly and securely ingest any IoT data from any connected device, correlate it and leverage AI/ML-powered insights to act on the data [22]. This strategy enables organizations to handle large and complex data sets to improve services and seamlessly grow the business.

Device management services: Pelion device management ease and accelerates IoT projects through embedded and web services which can be integrated into new or deployed devices. It can also allow developers to efficiently transit from prototype to production with adequate tools and resources. The device communication is made equivalent to interacting with APIs while device management services integrates into existing stack. Device management supports variety of hardware including Arm Cortex-M microcontrollers and Cortex-A systems. It also supports protocols like REST model such as HTTP, transport layer security (TLS) and internet protocol (IP) for web apps; datagram TLS (DTLS), constraint application protocol (CoAP), user datagram protocol (UDP) and IP for IoT backhaul and Low-Power Wireless Personal Area Networks (6LoWPAN) for IoT nodes. It also uses IP for internet connectivity and non-IP devices such as Bluetooth low energy (BLE). It also has REST API which gives full

control over devices. It has software development kit (SDK) to create language-specific abstraction in JavaScript, Python, .net and Java [23].

Connectivity management services: the platform provides global cellular connectivity services (4G LTE, 3G and 2G) and communication protocols for all trusted devices to automatically plug and play (PnP) in any IoT system. The connectivity can either be peer to peer in-country, sponsored roaming and global roaming. Some of the PnP devices are the wearables, mobile and smart buildings.

Other components of ARM Mbed IoT include

Mbed Device interface which supports a variety of IP and Non-IP communication protocols such as BLE, WiFi Ethernet, ZigBee IP and 6LowPAN. The TLS module available in Mbed provides end-to-end security encryption across the communication channels. It also supports application protocols such as CoAP, HTTP and MQTT [22].

Mbed OS which creates a platform operating system for IoT. It contains all the features required to develop connected products based on Arm Cortex-M microcontroller [24], including security (uVisor, TLS and SSL), connectivity, modularity, drivers for sensors and I/O devices.

Mbed Client Library provides a channel to communicate between the upper and lower layer of the architecture. It implements the secure (TLS) communication stack with low power consumption based on CoAP. It is portable to various OS such as RTOS and Linux and supports open mobile alliance (OMA) Lightweight machine to machine (LwM2M) compliance.

Mbed Device Connector allows connection of IoT devices to cloud without physical infrastructure while guaranteeing secure (end-to-end encryption), simple and capable IoT application at scale. It makes messaging, provisioning and updates in IoT devices available to enterprise software, web applications and cloud stacks through REST APIs. Using standard protocols such as CoAPP, HTTPS, TLS, DTLS and OMA, the IoT devices can be managed efficiently and data communication will also be efficient. It also offers full integration of the developed console and web tools with Mbed.com (API keys, authenticator and developer console).

Mbed Cloud which provides Software-as-a-Service (SaaS) solution for managing IoT devices by allowing secure update, provision and connection of devices.

Security Features of Mbed IoT

Mbed provides security through the following features:

1) Mutually authenticated (D)TLS connections between your device and Pelion using Mbed TLS

Mbed TLS/DTLS allows developers to include cryptographic and SSL/TLS capabilities in the embedded products facilitating its functionality with minimal code footprint. This feature can be hardened into the system development or can be manually selected and configured. The Mbed TLS has a functional library comprising the SSL/TLS protocol implementation, cryptographic library and X.509 Certificate handling library. Mbed TLS uses continuous integration system to enhance code quality [22].

2) A first time-use LwM2M bootstrapping mechanism

Device management provides onboarding through bootstrapping and using direct Pelion LwM2M server credentials [24]. Bootstrapping allows devices to connect to the bootstrap service to provide LwM2M service account credential for registration. This will allow the system to restore bootstrapping when LwM2M credentials is renewed. In direct Pelion LwM2M server credential, the device onboard straight to the LwM2M thus it cannot fall back to bootstrap.

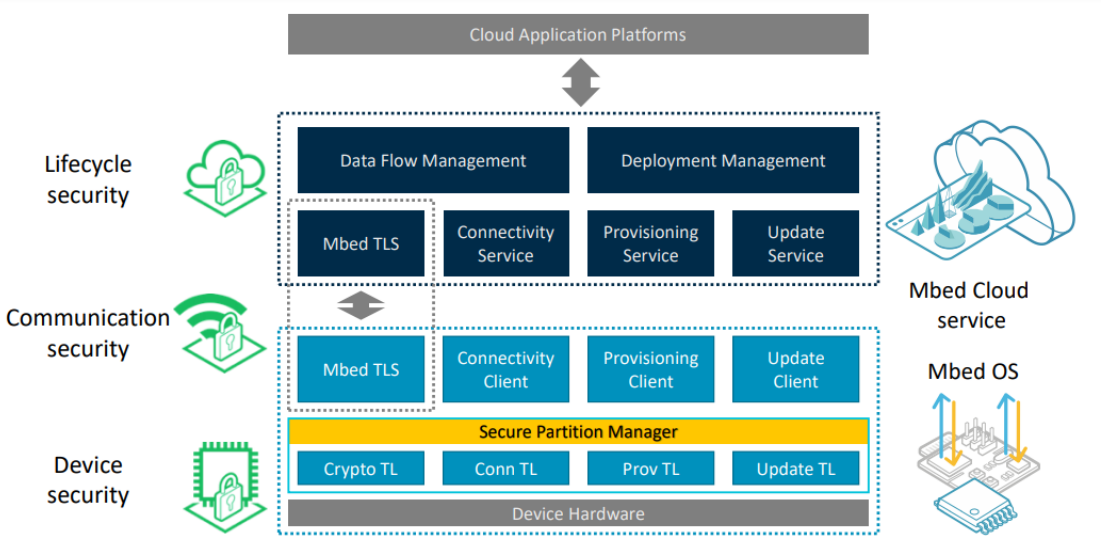

Fig. 4. Arm Mbed/Pelion Security Framework (Arm Mbed. 2019)

Both methods rely on provisioning of device credentials during manufacturing.

3) A firmware update mechanism

This is the extension of the device life through regular upgrades and critical fixes such as security patches. The device management update service sends new firmware to deployed devices client. The update client verifies, installs and report the progress of firmware update to the update service. The device management update uses certificates to ensure end-to-end security and validates the source and genuineness before accepting the firmware update

The following security properties are provided by the aforementioned features:

1) Authentication

This is provided by Mbed TLS software blocks which allows end-to-end encryption through public/private key, symmetric and key exchange encryption. For example, it can use X.509 Certificate to authenticate server and client activities.

2) Authorization and access control

Authorization through Arm Mbed IoT is done by use of uVisor [24] which provides hardware-enforced compartments for individual code blocks by limiting access to memories and peripherals using the existing hardware security features of the Cortex-M microcontrollers. It segments data into either private or public. It creates isolated security domains on Arm Cortex-M3, M4 and M7 microcontrollers with a Memory Protection Unit (MPU).

Mbed IoT also uses Secure Partition Management (SPM) to separate firmware into partitions so that each have their own memory and storage space. The communication between the partitions is handled through standardized APIs. The APIs abstract the fact that partitions could be living inside a virtualized environment (v8M, TEE on Cortex-A), or another chip (Twin-V7M) [23].

3) Secure communication

Mbed TLS enables cryptographic and SSL/TLS communication security for use in cloud and connected device applications. Mbed TLS forms part of the current Mbed Cloud, Mbed OS and platform abstraction layer (PAL) implementations. It is also used in production systems by a wide variety of 3rd parties in cloud and device software implementations. Mbed Cloud Provisioning is used to inject unique cryptographic identity and Mbed Cloud connection parameters into devices during manufacturing [25].

Security challenges in Arm Mbed IoT

The compartmentalization of hardware and segmentation of data in Mbed IoT may slow the performance of functions in the devices due to the potential exchange bottlenecks between the compartments.

C) Microsoft's Azure IoT Suite

This platform consists of a set of services that enables users to interact with and receive data from IoT devices as well as perform various operations over data, such as multidimensional analysis, transformation and aggregation, and visualize those operations in a way that's suitable for business [26].

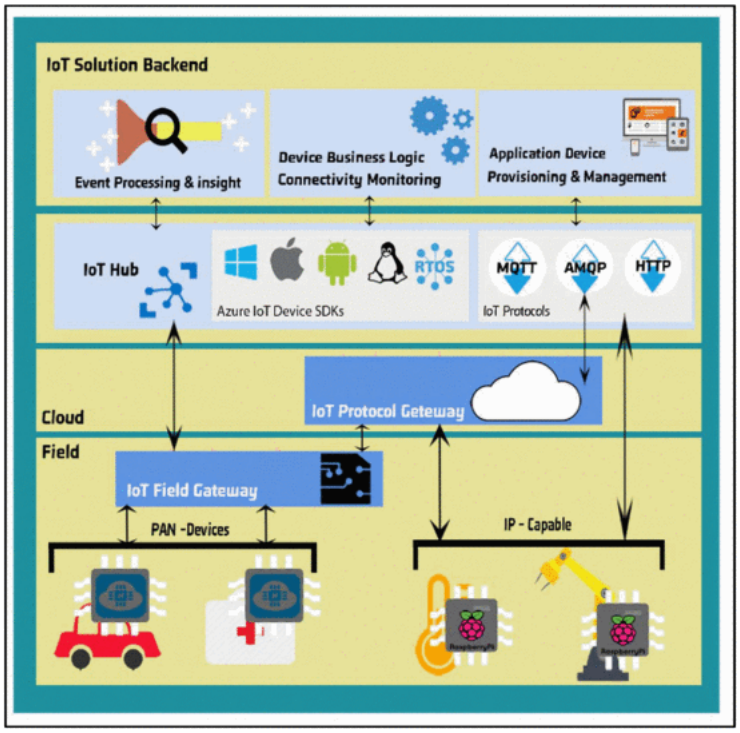

Fig. 5. Microsoft Azure IoT Components/services (Microsoft Inc. 2019)

Components of Azure IoT

The *IoT Hub [26]* provides the cloud gateways for device interconnection allowing several devices to connect and process and communicate large volumes of data. It is composed of multiple protocols including HTTP and AMPQ, MQTT. The IoT Hub also secures the IoT system by providing per-device authentication support.

Stream Analytics [26] is a real-time analytics service that enables detection of anomalies and archival of data from IoT devices. It utilizes data coming from devices into IoT Hub and enables writing stream processing logic with temporal semantics in a simple SQL like language.

Blob Storage [26] provides a cost-effective way to store data from the devices to the cloud.

DocumentDB [26] is used to manage the metadata about devices being provisioned, such as configuration, state and security properties of the devices. Its semi-structured model allows combination of different types of devices with different data schemas.

A Web App [26] is deployed to host the web application used to inspect the device data dashboard, configure and send commands to devices, create and update business logic, and

manage event-driven actions such as sending text messages when certain thresholds are met.

A Logic App [26] helps to integrate IoT solution to existing infrastructure and automate workflow process. Logic Apps allow developers to design workflows that start from a trigger and then execute a series of steps—rules and actions that use powerful connectors to integrate business processes.

Security Features in Azure IoT

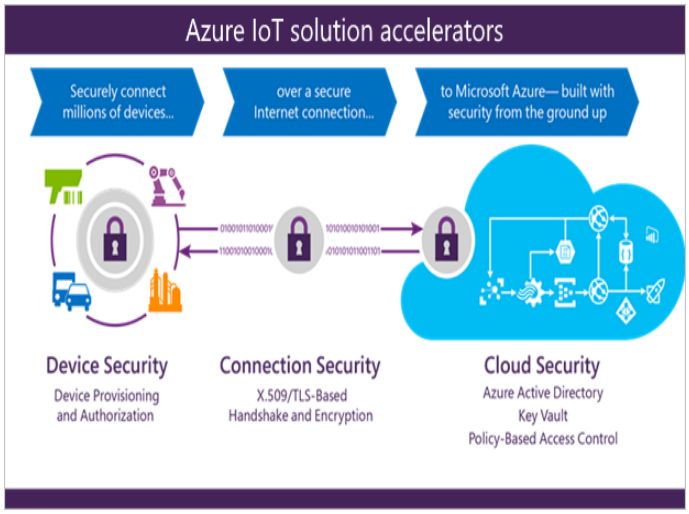

Fig. 6. Microsoft Azure IoT Security Framework (Microsoft Inc. 2019)

1) Authentication

Through device provisioning a unique identity key such as end-to-end encryption, X.509 Certificate, TLS-based handshake, each device can be used to communicate with the other device while it is operating. The key forms the basis of a token used in all communication by the interconnected devices. This key cannot be easily changed since it is associated with the devices during manufacturing. Through authorization, Azure IoT Hub Identity registry, securely store device identities and security keys which will allow or block accessibility thus enabling complete control over device access. Further, in Azure IoT, devices accept only solicited network connections by iteratively checking for pending commands to process before receiving a command from the backend. The devices also establish connection to only well-known services peered to it. Azure IoT also uses per-device identities making access credentials and permissions near-instantly revocable [27].

The X.509 Certificate Authority (CA) feature enables device authentication to IoT Hub using a CA [28]. It greatly simplifies initial device enrollment process, and supply chain logistics during device manufacturing.

2) Authorization and access control

Using Azure Active Directory (AAD), Azure IoT solution accelerators can provide a policy-based authorization model for data in the cloud, enabling easy access management that can be audited and reviewed [28]. This model also enables near-instant revocation of access to data in the cloud, and of devices connected to the Azure IoT solution accelerators. The data in the cloud can be processed and stored in any user-defined workflow. Access to each part of the data is controlled with Azure Active Directory, depending on the storage service used.

3) Secure communication

Azure IoT Hub through cloud security enables secure and reliable bi-directional communication between IoT devices. Each device is hardened with security key to enable it to connect to IoT and store the identities and keys into IoT identity registry. The Hub supports HTTP and AMQP protocols to allow IP enabled devices to communicate with the Hub. Data is also stored either in the Axure Cosmos DB or in SQL database thus enhancing the level of privacy [29].

Security Limitations of Azure IoT

In some cases, the SDKs cannot support all the protocols or all the authentication methods. Also, HTTP/l is inefficient for both the devices and IoT Hub where it does not have efficient way to implement server push and devices poll. Further, AMQP and MQTT are more compact than HTTP/l which are binary protocols.

III. PROPOSED FRAMEWORK

This paper proposes the need to enhance the security of existing IoT framework through standardization and use of 5G security protocol for consumer protection and network resilience.

A) Standardization of frameworks

As discussed in section II, each IoT framework had distinctive layer each implementing varied security protocols to protect data and the devices. Further, the devices have localized intrinsic security mechanisms embedded within the hardware, and software which are inadequate in securing the devices. Furthermore, the traffic generated by interconnected devices could be vastly different to what conventional user equipment in legacy systems generate [30]. However, with standardization of frameworks, development of secure application will be made easier. The standardization should be enhanced at technology (wireless communication, network protocols and data integration) and at regulatory level (security and privacy of data); see Fig. 7. Standardization will enhance management of common security goals of confidentiality, integrity and availability.

B) Security in the era of 5G

The fifth generation (5G) networks is becoming more readily available as a major driver of the growth of IoT applications [31]. 5G network is exponentially increasing the interconnection between people and devices and among devices [32]. The Third Generation Partnership Project (3GPP) is defining 5G standards to secure the network core, radio and user equipment, which include procedures for user privacy assurance and identity management. Understanding these relationships is essential to build new devices which can operate safely, fully qualifying and understanding the risks across the entire IoT eco-system [33]. Privacy assurance and

identity management procedures also need to be linked to user consent and data handling mechanisms. The 5G 3GPP standard allow different types of physical and virtual overlap between the radio access network (RAN) and core network [31]. Also, services are provided via a common framework to network functions that are permitted to make use of these services, see Fig 7. Modularity, reusability and self-containment of network functions have also been included in 5G network.

5G networks leverages devices connection to the mobile infrastructure via different access technologies. Therefore, with machine type communication, 5G networks empowers IoT with network capabilities such as ultra-low latency.

To achieve the necessary level of targeted security in mobile networks, the trustworthiness [34] of connected IoT devices must be considered while assuring the IoT device's identity and access control (access privileges and confidentiality) of associated data generated by the IoT device, Fig. 7.

Also, security designs provided by 3GPP, enables light-weight approaches to conventional security problems [35], whilst not undermining security operations and not leaving backdoors that could impede system security. The proposed framework includes a critical communication application that involve low power wide access (LPWA) technologies requiring stringent latency and reliability levels [36]. The resultant IoT devices will strike the balance between energy efficiency, battery life, and high security assurance which is provided by 3GPP [36].

C) Proposed standard framework based on 5G 3GPP

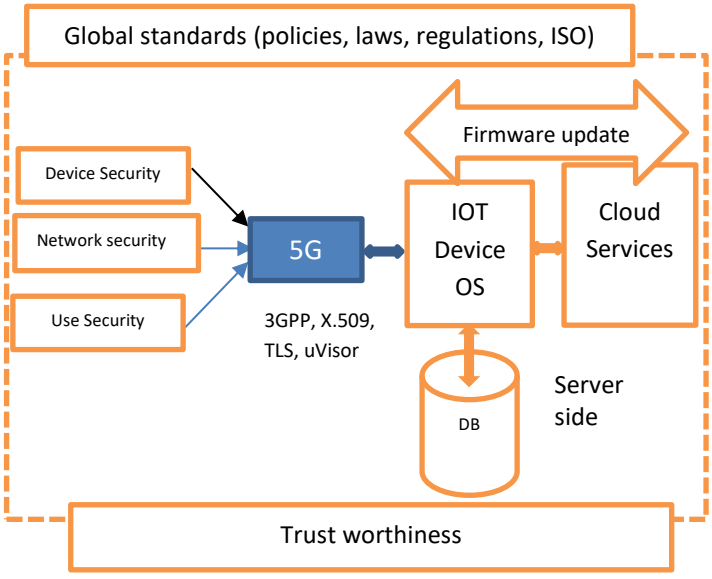

Fig. 7. Proposed framework

In the proposed framework, 5G 3GPP security protocol which provides non-IP data delivery (NIDD) has been introduced to enhance the security of IoT devices as discussed in section III.B together with X.509 Certificate, TLS and uVisor. There will also be an overarching standard on the salient features and system organization that must be considered when developing IoT systems. Regular firmware update and security patches will also be provided for as a standard in the framework. Absolute trust in the data generated by IoT devices and the interconnection between IoT devices and cloud services has also been established and maintained through mutual authentication of both the devices and servers.

The proposed framework will standardize IoT development and service provision by key stakeholders such as cloud providers, original equipment manufacturers and chipset makers, service providers and mobile network operators [32] thus enhancing the security of IoT devices

IV. CONCLUSIONS

From the above analysis it is noted that the available IoT framework provided by AWS, Azure and Arm Mbed provide security based on different protocols which is strong to some extent. However, there is need to standardize the frameworks and implementation of 5G networks to enhance the security of devices, data and connectivity within IoT ecosystems.

REFERENCES

[1]. CISCO, (2016). Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015—2020 White Paper. Cisco Public Information

[2]. Chen, S. et al., (2017). Machine-to-Machine Communications in Ultra-Dense Networks-A Survey. IEEE Communications Surveys & Tutorials.

[3]. Mannilthodi, N. & Kannimoola, J. M., (2017). Secure IoT: An Improbable Reality. s.l., SciTePress, pp. 338-343.

[4]. Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami, (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. Future Generation Computer Systems, 1645-1660.

[5]. V. Karagiannis, P. Chatzimisios, F. Vazquez-Gallego, and J. Alonso-Zarate, (2015). "A survey on application layer protocols for the internet of things," Transaction on IoT and Cloud Computing, vol. 3, no. 1, pp. 11-17.

[6]. Pal, D. Funilkul, S. Charoenkitkarn, N. Kanthamanon, P. (2018). Internet-of-Things and Smart Homes for Elderly Healthcare: An End User Perspective. IEEE Access,6, 10483–10496

[7]. M. A. Ezechina, K. K. Okwara, C. A. U. Ugboaja (2015). The Internet of Things (Iot): A Scalable Approach to Connecting Everything. The International Journal of Engineering and Science 4(1), 09-12.

[8]. Yaqoob, I. et al., (2017). Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges. IEEE Wireless Communications, 24(3), pp. 10-16.

[9]. Rahman L. F., Ozcelebi T., and. Lukkien J. J, (2016). Choosing Your IoT Programming Framework: Architectural Aspects. 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud).

[10]. Krishnamurthy J. and Maheswaran M., (2016). Programming frameworks for Internet of Things. Internet of Things, pp. 79–102, 2016.

[11]. Tweneboah-Koduah, S., Skouby, K. E., & Tadayoni, R. (2017). Cyber security threats to IoT appliations and service domains. Wireless Personal Communications, 95(1), 169-185.

[12]. Liu, X., Zhao, M., Li, S., Zhang, F., & Trappe, W. (2017). A security framework for the Internet of Things in the future Internet architecture. Future Internet, 9(3), 27.

[13]. Huansheng Ning, Hong Liu, (2012). Cyber-Physical-Social Based Security Architecture for Future Internet of Things. Advances in Internet of Things, 1-7.

[14]. Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security, 4(1), 65-88.

[15]. Internet of Things (IoT) Cybersecurity Improvement Act of 2017. United States 115 Congress

[16]. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, (2017). A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications", IEEE Internet of Things Journal, pp. 1-1.

[17]. Uviase, O., & Kotonya, G. (2018). IoT Architectural Framework: Connection and Integration Framework for IoT Systems. arXiv preprint arXiv:1803.04780.

[18]. Federal Trade Commission, FTC. (Jan 2015). Staff Report: Internet of Things: Privacy & Security in A Connected World, 7-10. [Hereinafter FTC IoT Report],

[19]. OECD (2015), (2015). Chapter 6 Emerging Issues: The Internet of Things. OECD Digital Economy Outlook 2015", OECD Publishing, DOI: http://dx.doi.org/ 10.1787/9789264232440-en

[20]. AWS Inc. 2019. AWS Developer Guide

[21]. Amazon AWS identity and access management (iam). https://aws.amazon.com/iam/. Online; accessed: October 2019

[22]. Arm Mbed IoT device platform. http://www.arm.com/products/iot-solutions/mbed-iot-device-platform . Online; accessed October 2019.

[23]. Arm Mbed device connector. https://www.mbed.com/en/platform/cloud/mbed-device-connector- service/ . Online; accessed: October 2019.

[24]. Arm Mbed security. https://www.mbed.com/en/technologies/security/. Online; accessed: October 2019.

[25]. Mbed uVisor. https://www.mbed.com/en/technologies/security/uvisor/. Online; accessed: October 2019

[26]. Azure Microsoft IoT reference architecture. https://azure.microsoft.com/en-us/updates/microsoft-azure-iot-reference-architecture-available/. Online; accessed: October 2019.

[27]. Azure Microsoft IoT hub. https://azure.microsoft.com/en-us/services/iot-hub/ . Online; accessed: October 2019.

[28]. Azure Microsoft IoT Communication protocols. https://azure.microsoft.com/en-us/documentation/articles/iot-hub-devguide-messaging/#communication-protocols. Online; accessed: October 2019.

[29]. Azure Microsoft IoT protocol gateway. https://azure.microsoft.com/en-us/documentation/articles/iot-hub-protocol-gateway/. Online; accessed: October 2019.

[30]. Wang J., Zhu R., and Liu S., (2018). A Differentially Private Unscented Kalman Filter for Streaming Data in IoT. IEEE Access, vol. 6, pp. 6487–6495, 2018.

[31]. Gupta S., Parne B. L., and Chaudhari N. S., (2018). Security Vulnerabilities in Handover Authentication Mechanism of 5G Network,"

[32]. GSMA IoT SAFE specifications for eSIM provide scalable IoT security. https://www.gemalto.com/iot/iot-security. Online; accessed: January 2020.

[33]. Sandoval R., (2017). Information systems development (ISD) and the national institute of standards and technology (NIST) risk management framework.

[34]. Menezes A. J., (2019). International Conference on Secure Cyber Computing and Communication (ICSCCC). IEEE, pp. 369–374.

[35]. Eisenbarth T. and Kumar S., (2007). A survey of lightweight-cryptography implementations. IEEE Design Test Computers, vol. 24, pp. 522–533.

[36]. Braeken A., Liyanage M., Kumar P., and Murphy J., (2019). Novel 5G Authentication Protocol to Improve the Resistance against Active Attacks and Malicious Serving Networks. IEEE Access.