IoT Based Smart Systems using Machine Learning (ML) and Artificial Intelligence (AI): Vulnerabilities and Intelligent Solutions

Shaftab AHMED
Software Engineering Department
Bahria University Islamabad, Pakistan

Mohammad ILYAS
College of Engineering and Computer Science
Florida Atlantic University
Boca Raton, Florida, USA

M. Yasin Akhtar RAJA
Center for Optoelectronics & Optical Communications
University of North Carolina
Charlotte, North Carolina, USA

ABSTRACT

Internet of Things (IoT) has assumed great importance in technical and social domains due to desire of smart living and intelligent solutions for industrial operations, home automation and healthcare. The telecommunication networks provide all-time internet connectivity for the devices in physical systems and hand- held devices. The developments have made it easy to remain engaged on all time, anywhere basis, while users interact with one or more applications. Many smart devices may interact in the background resulting in event-driven intelligent activities raising alerts or recording status summary under a policy. The smart solutions are being shaped for the industry, transport, eHealthcare, eEducation and other daily life activities. IoT activities are autonomous and support dynamic Machine-to-Machine (M2M) communication. The challenges of hetrogeneity, dynamic variation in signal quality and large volume of data are being addressed through number of techniques. In this paper, we discuss IoT based smart system technologies, security, vulnerabilities and role of intelligent solutions using Machine Learning (ML) and Artificial Intelligence (AI). A crucial factor hindering the ongoing efforts for widespread IoT-adoption, is security. We propose the requirement of Standard Security Framework (SSF) for platform independent and interoperable hardware/software modules in distributed networks domains. Trends to use Fog- and Edge-computing along with cloud applications has been also reviewed in the context to security and efficiency

Keywords: Internet of Things (IoT), Machine to Machine (M2M) Communication, Machine Learning (ML) and Artificial Intelligence (AI), Distributed Security Framework (DSF).

1. INTRODUCTION

The wide acceptance and use of smart systems through handheld devices, especially hand-held devices/cell phones and Wi-Fi enabled buildings, enterprises and public places have changed the outlook of human society. Social networks have broadened the horizon of all human activities. The smart devices constituting the Internet of Things (IoT) are being rapidly used to collect, share data, and often take suitable actions autonomously. Those devices have embedded electronics, software and sensors use the internet for data collection and exchange. Those are usually self-configuring and designed for smart interaction with neighboring nodes [1]. The enormous data generated needs to be analyzed and archived under a certain policy. The cloud services support storage, processing and sharing of data through all-time anywhere connectivity and availability of desired information. The devices use the wireless and internet services which makes them an easy target for the hackers. Data communication and cyber security developers and engineers have proposed several solutions for data transport, access, and usage [2]. That has enabled safe usage of such services, but still canny hackers exploit any loopholes left. The forensics and other cyber security tools are being used to overcome such challenges.

In situation of smart systems, the human intervention, the wide range of devices and platforms being used increase the scope and challenges for the developers. Hence, the developers are working on proactive collection of network activity intelligence through machine-learning (ML) and embedded-intelligent agents in the software systems to initiate suitable measures to identify and take appropriate actions in case of malicious activity. The solutions require computing and battery resources which are scarce in the widespread smart sensors and mobile devices [2]. To address those challenges, designers are resorting to use Fog and Edge-computing for spreading the activities and reducing power requirement of the terminal nodes.

IoT examples for Smart Systems often include:

a) Home Automation (HA) IoT
b) Healthcare and Assisted Living IoT
c) Smart Buildings and Cities
d) Smart Enterprises
e) Smart Healthcare

In the section II of the paper, we review the IoT related developments in Information & Communication Technologies (ICT) particularly, about the security and the usage of AI/ML for secure and smart systems of future. In section III, we discuss the key features of smart systems that is followed by the section IV on the vulnerabilities. We also propose the need for Smart System Framework (SSF) and inclusion of ML and AI in embedded software paradigms.

ISBN: 978-1-950492-63-3
ISSN: 2771-6368

https://doi.org/10.54808/ICSIT2022.01.56

2. RELATED WORK

The IoT based smart systems offer efficient resource utilization, minimize human efforts/intervention, provide time efficiency in data-collection, classification, and storage for intelligent operations. Proactive knowledge-based analysis is used for operations through the framework of Machine Learning (ML) and Artificial Intelligence (AI). For this purpose, mobile agents are extensively used for performing diagnostics, data-collection, configurations, and signal quality management without human intervention [3].

IoT Architecture:
The architecture of IoT devices include operations such as; Connect, Analyze, and Integrate to handle/maintain the smart systems' activities.

IoT ecosystems have evolved from the 3-layer to a 5-layer implementation as shown in Fig.1. The Application layer provides user interaction through front end applications for end-to-end solutions including smart grids, smart highways, smart homes, and smart health and so on. Networking layer facilitates use of various networking models and protocols. Perception layer is also called the sensing layer of IoT architecture. Perception layer is used to collect real-world data and detect events as well. Sensors are embedded in IoT devices through sensor hub which provide connectivity of IoT device to the network layer.

Table-1: **IoT Architecture (**Ref.: *IoT courseware* Edureka.com**)**

IoT Function	Data Acquisition and Control	Smart Services
Integrate	IoT Application Oriented Platform, User Interface and Data Presentation	Enterprise Level communication using REST API Command and Control of IoT Devices in Home, Hospital, Shopping Mall, Airport, Office etc.
Analyze	Data Collection, Error Handling, Data Rationalization and Selection	Build Business Knowledge, Data Enrichment, Storage and event Generation
Connect	Physical or Wireless Connectivity with Sensor Devices	Data virtualization for Platform Independent usage and Endpoint Management

The five-layer model uses Business and Application layers for front-end applications and adds processing layer for data classification and segregation. The Transport layer connects processing and perception layers:

Three-layer IoT architecture:
Application Layer
Networking Layer
Perception Layer

Five-layer IoT Ecosystem:
Business Layer
Application Layer
Processing Layer
Network / Transport Layer
Perception Layer

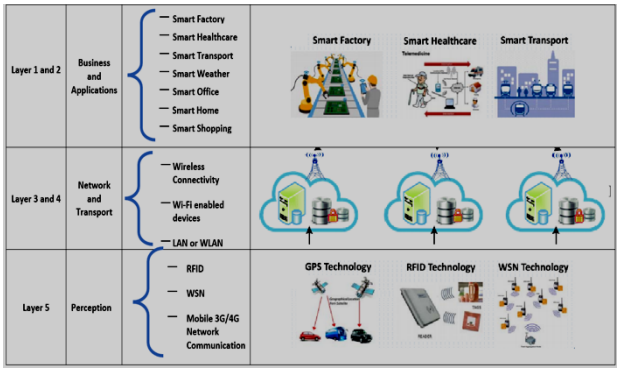

Figure 1. Five layer model of IoT ecosystem [20]

Networks Virtualization:
The use of cloud services is increasing with wider acceptability in the industry and daily life. However, the cloud service face serious limitations of latency, mobility, reliability, and scalability in the context of smart sensor networks which operate in real-time. To overcome these, cloud datacenters have been introduced through smart gateways and smart devices. The designers have introduced new dimensions to the architecture through Fog- and Edge-computing. They allow better management of activities in distributed systems specially for security architectures. Hence, four new layers have been inserted between transport and perception layers i.e.

- Security Layer
- Storage Layer
- Preprocessing Layer
- Monitoring Layer

Machine Learning (ML) and Data Collection for Artificial Intelligence (AI):
The data generated by sensor networks and devices is classified prior to storage. The ML agents capture useful data intelligently hence maintain status of devices regarding type of activities, periodicity, battery-life and so on. The embedded agents gather information proactively for security and operation reliability. The models used for this purpose, utilize Supervised, Unsupervised and Reinforcement learning [4]. AI-based cybersecurity systems are used to maintain knowledge-base of security threats used to make important decisions in critical situations. AI practices are expected to enhance cybersecurity by assisting human system-managers with automated monitoring, analysis, and rapid responses to the cyberattacks.

Autonomous Network Operations:
Central management of Sensor Networks is not possible due to very large number of parameters involved, dynamic changes in topology, scarce visibility of dynamically varying network conditions related to topology, signal quality, mobility, and dynamic application requirements. Hence a distributed management is more suitable to support autonomous decision-making capabilities [5]. Those systems allow status monitoring and re-configuration of itself to fix problems in the network.

Security Requirements of IoT:
Wireless sensor networks and IoT devices have yet to achieve the goal of foolproof security, robustness and resilience required for automation and uninterrupted operations in smart applications. Confidentiality, Integrity and Availability (CIA) triad is required for secure operations and data management [6]. The IoT must provide end-to-end security and privacy to meet the expectations in applications such as healthcare [7][8]. Most of the solutions

implemented today use centralized client server architectures where the devices enjoy unique identity within a domain. They are authenticated and granted access under a policy. The problem is aggravated in case of large number of sensor nodes using cloud services covering large storage capabilities and processing features. Hence, the bottlenecks, downtimes and recovery become service limitation, especially in real-time operations. The terminal devices and sensors are resource constrained and cannot implement comprehensive security features.

Distributed Security Management:
The smart systems span several domains of operations hence distributed security implementation are seen to be the future direction of research for secure IoT based networks e.g., Fig. 2. The Authentication and Authorization are visualized at user and device levels. Before communication starts device, identity and authorization are setup for end-to-end security by exchanging information [9]. Some challenges faced by IoT developers are:

- Light-weight security operations
- High reliability
- Scalability
- Fault tolerance
- Early fault / malicious activity detection

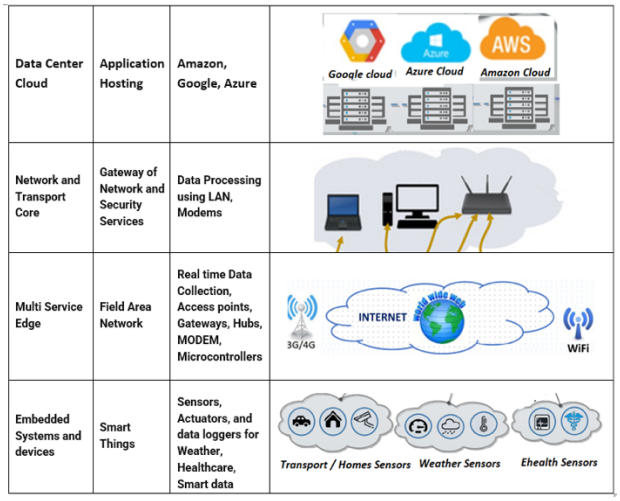

Figure 2. Distributed Security Management Theme [19][22]

The concept of security gateway at each layer of the model helps categorization of security issues related to each layer mapped against several types of attacks [8].

Application Layer	Data stealing, False data injection, Service interruption, Malicious code insertion and sniffing
Data Processing Layer	Signature wrapper, Man in The Middle, Flooding
Communication Layer	DDoS/DoS, sybil, Secure onboarding
Perception Layer	Node capture, Malware injection, Side channel risk, Eavesdropping, Interference and Sleep deprivation

Figure 3. The vulnerability of layered architecture of IoT layers [1] [8]

The vulnerability of layered architecture of IoT are in the following tabulated Fig. 3 that helps categorization of security issues related to each layer.

3. IoT COMPONENTS AND TECHNIQUES FOR SECURITY FRAMEWORKS

IoT devices are often comprised of-the-shelf sensor hardware and microcontrollers, and/or processors driven by custom software design provided by the developers. The integration of such hardware devices and software with cross- platform compatibility and interoperability are important considerations. The evolution of user-friendly IoT frameworks for intelligent component integration and management is yet another important development for long-term applicability of solutions in the ICT industry. Hence it is desirable to develop common middleware with standard interfaces to make the applications more adaptive and easy configurability. Such practices will speed up the development of IoT based smart systems. The IoT based smart systems frameworks are often comprised of the following main features [10][11][12]:

Components:
Sensing, Actuation and Response of IoT Wireless technologies such as Bluetooth, Zigbee, WiFi and so on.

Data Communication Standards of Physical Layer:
RS232, RS485, SPI, I2C, CAN, LIN, MQTT, UDP, MQTT brokers, HTTP, COAP, XMPP and Gateway protocols.

IoT Operating Systems and Management:
FOG- and Edge-computing.

Cloud Services:
Commercial clouds, Dashboards, Big data analytics and Hadoop.

Open Source IoT Platforms:
Interfacing and data logging with cloud etc.

Operation and Security Frameworks:
IoT for home automation, smart eHealthcare and Ambient assisted living.

Middleware for Portable Solutions
The Software Defined Networks (SDN) and Network Frame Virtualization (NFV) are being used. Those provide flexibility for data management and network activity monitoring to support Intrusion Detection systems (IDS) and Data Packet Inspectors (DPI). They offer firewall solutions, authentication / authorization features through ML and AI. Virtual networks are useful to incorporate autoconfiguration and on demand service operation features. They offload extra computing effort from IoTs hence saving energy and improving efficiency.

The rapid growth of sensor technologies and heterogeneity of both hardware and software platforms has led the developers to use middleware to virtualize network domains for flexible management and operations, Fig.4. Middleware is used to address communications challenges by providing [12] [13]:

- Interoperability and program abstraction
- Device discovery management
- Scalability
- Big data analytics
- Security and privacy

- Cloud services
- Context detection

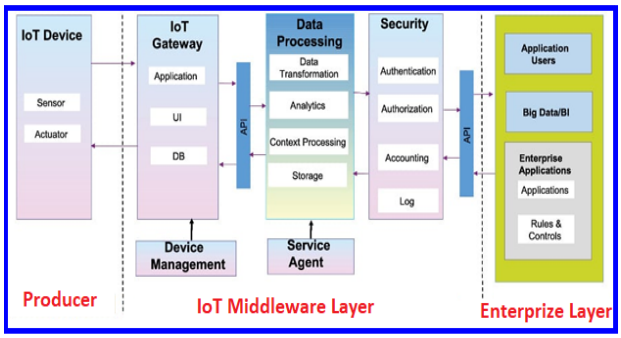

Figure 4. Middleware to address communication challenges [13]

4. STANDARD SECURITY FRAMEWORK (SSF) FOR IOT SOLUTIONSHEADINGS

In this section we present and discuss the requirement of Standard Security Framework (SSF) for platform independent and interoperable hardware and software modules without compromising security management.

The IoT developers are using heterogeneous platforms in hardware and software for field signal detection, aggregation, and presentation. The network models being used vary in implementation of security features, need refinement and standardization to handle the vulnerabilities of IoT systems. The AI/ML tools are being used to monitor user behavior, changing user patterns and other data irregularities to raise alerts. The autonomous learning at the intelligent nodes is useful for intelligent ML/AI solutions but those may also be a source of insecure communications. Serious reservations on
this account has been raised by the researchers and the developers [14]. It is recommended that the data sets involved, should be standardized to make AI/ML based solutions to decipher and analyze them quickly.

Considering the features and technologies being used in smart systems, we feel that standard encryption protocol for IoT devices supporting light weight implementations will help relieve the extra computation requirements and wider introduction of networks. The forensics and data analysis are required for the wider scope and security audit; however, the online malicious activities can be identified using ML and AI features embedded in the implementation of IoT frameworks.

Proposed Standard Security Features and Protocol

The heterogeneous technologies and multiplatform deployment of IoT systems pose serious problems in design of secure interoperable systems. The vulnerabilities of sensor nodes on account of exposure in the physical domain add another dimension of complexity. To overcome such problems, it is necessary to reach a universal acceptance of data handling and security protocols embedded in sensor network architecture for use in IoT systems. We propose to develop a robust security policy through Standard Security Framework (SSF) in implementing IoT solutions.

Distributed system architecture with hub-based security architecture to expand the computation requirements over the implementation layers is useful. The hubs are intelligent loaded with 'plug and play', self-configuration, and diagnostic features.

A dynamic secure key generation protocol using Trusted Platform Module (TPM) [16] features with the help of network-wide certification authority (CA). That will be used for initiating secure communications providing boot level security. The protocol overhead will be reflected on the hubs for each layer, whereas the terminal sensor nodes will use light weight features for secure communications [15][16]. Embedded security mechanisms with light weight algorithms are proposed which is now being called security by design (SD) [17] [18]. That is based on the concept of generating embedded secure keys using hardware device identity e.g., MAC address. Those are shared between sensors and host during plug-and-play engagement of sensors without involvement of the higher level.

We proposed to use token based dynamic exchange of information between participating devices or IoT nodes to generate security keys after plug and play engagement of sensor devices, instead of fixed or embedded identity or secure key distribution methods, shown in Fig.5. Sensor nodes use random parameters, such as temperature, pressure, device ID and time to generate mutually accepted Token containing set of physical keys generated by embedded algorithms. Starting from sensor nodes, the Token plays a key role in generating secondary keys at upper levels like hubs and application servers. Tokens are dynamically regenerated/updated making it extremely difficult for hackers. False data injection is avoided by registration of devices used at the application server level; it is a part of the secure-key generation mechanism.

Similarly, the secure engagement model for edge to transport and application levels can be used. Proceeding from the sensor nodes in IoT architecture, additional security methods such as firewalling, forensic data collection and report generation can be used as the computation resources and battery power are not a problem. The low-level security protocol augments robust security algorithms available at higher levels in network model.

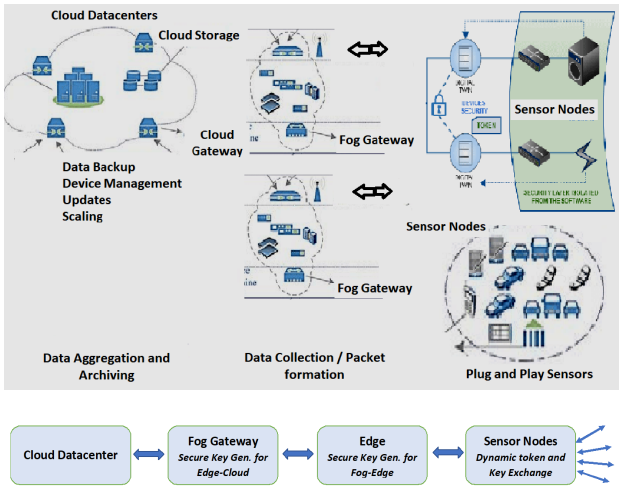

Figure 5. Distributed Security Architecture for IoT Solutions [7][14]

The solution proposed guards the IoT system from malicious activity around exposed sensor nodes, while using less battery power and computation overhead. It provides a token-based mechanism to propagate and integrate with the existing secure mechanisms used in hierarchical levels of IoT architecture.

5. CONCLUDING REMARKS AND FUTURE WORKFIGURES AND TABLES

Autonomous large-scale wireless networks are expected to rapidly increase soon. The proposed and developed frameworks will support aggregation of data and intelligence with the help of middleware and intelligent nodes. The features required include [17]:

- International acceptance of standard security service protocol
- Use of Service Oriented Architecture (SOA) to handle plug and play hardware software modules, allowing use of protocols i.e., SOAP, MQTT, XMMP & HTTP and so on.
- Energy-Harvesting to overcome the battery life problem
- Self-repairing and configuring features for robustness
- Network scaling, aggregation, and management
- Machine learning and AI tools for proactive operations

The data traffic from numerous IoT devices affects speed and efficiency of backbone network services. The use of IoT gateways at Sensor-nodes, Edge, Fog and Application layers play an important role in bridging the WSN traffic between sensors and backbone communication network [22]. Gateways collect information from sensors and pass it to the server layers. Distributed security management may take advantage of the gateway hierarchy to meet the challenges of wireless communications [19]. End-to-end security could be provided by light weight security at terminal sensor nodes along with higher level of security algorithms at hub and server nodes. The proposed security mechanisms seem robust, difficult to guess and introduce barriers at all hierarchical levels to handle malicious activities. The requirement of light weight security algorithms can be met by using embedded security at sensor nodes and deployment of available tools at Edge- and Fog- computing levels.

6. REFERENCES

[1] A. Gilchrist, **Industry 4.0: Th e Industrial Internet of Things**, ISBN-13 (pbk): 978-1-4842-2046-7 ISBN-13 (electronic): 978-1-4842-2047-4 DOI 10.1007/978-1-4842-2047-4 Library of Congress Control Number: 2016945031

[2] M. Younan, E. H. Houssein, M. Elhoseny et al., **Challenges and recommended technologies for the industrial internet of things: A comprehensive review**, Measurement, https://doi.org/10.1016/j.measurement.2019.107198

[3] M. Bagaa ,T. Taleb, J. B. Bernabe and A. Skarmeta, **A Machine Learning Security Framework for IoT Systems,** May 21, 2020, DOI 10.1109/ACCESS.2020.2996214

[4] P. Malhotra , Y. Singh, P. Anand , D. K. Bangotra, P. K.Singh and W.C. Hong, **Internet of Things: Evolution, Concerns and Security Challenges**, Sensors 2021, doi.org/10.3390/s21051809

[5] A.G. Ruzzelli, C. Muldoon, A. Schoofs, G.M.P. O'Hare and R. Tynan, **Autonomous management and control of sensor network-based applications**, CSE 2009 : 12th IEEE International Conference on Computational Science and Engineering, August 2009 Vancouver, Canada : Volume 2 http://dx.doi.org/10.1109/CSE.2009.480

[6] K. Boeckl M. Fagan Wi. Fisher Naomi L. Katerina, N. Megas, **Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks**, https://doi.org/10.6028/NIST.IR.8228 National Institute of Standards and Technology Interagency or Internal Report 8228

[7] A.K.M. Jahangir, A. Majumder and C. Veilleux , **Smart Health and Cybersecurity in the Era of Artificial Intelligence**, http://dx.doi.org/10.5772/intechopen.97196

[8] S. Majumder, E. Aghayi , M. Noferesti, H. Memarzadeh, T. Mondal, Z. Pang and M. J. Deen, **Smart Homes for Elderly Healthcare—Recent Advances and Research Challenges**, Sensors 2017, doi:10.3390/s17112496

[9] K. I. Ahmed, M. Tahir, M. H. Habaebi and S. L. Lau and A. Ahad, **Machine Learning for Authentication and Authorization in IoT: Taxonomy, Challenges and Future Research Direction**, https://doi.org/10.3390/s21155122 Sensors 2021

[10] O. Rahaman, A. Shuvo and M. A. Kashem, **Cyber Physical Systems for Healthcare International Journal of advanced Research**, http://dx.doi.org/10.21474/IJAR01/7968

[11] M. Bajer, **IoT for smart buildings - long awaited revolution or lean evolution,** 23rd International Workshop of the European Group for Intelligent Computing in Engineering June 29th – July 1st, 2016, Kraków, Poland

[12] G.K. Behara, G. Naik, **A Primer on Open Source IoT Middleware for the Integration of Enterprise Applications,** https://www.opensourceforu.com/2019/10/a-primer-on-open-source-iot-middleware-for-the-integration-of-enterprise-applications/

[13] M. Albano, S. Chessa, **Programming a Sensor Network in a layered middleware architecture**, InTechOpen.com, ISBN 978-953-307-297-5

[14] T. G. Zewdie, A. Girma, **IOT Security and the Role of AI/ML to Combat Emerging Cyber Threats in Cloud Computing Environment**, Nov 2020 DOI: 10.48009/4_iis_2020_253-263ISBN: 1365-2575

[15] R. Sailer, L. Doorn, J. Ward, **The Role of TPM in Enterprise Security**, Computer Science IBM Research Report RC23363 (W0410-029) October 6, 2004

[16] Jurcut, A., Niculcea, T., Ranaweera, P. et al., **Security Considerations for Internet of Things: A Survey**, SN COMPUT. SCI. 1, 193 (2020). https://doi.org/10.1007/s42979-020-00201-3

[17] M. Abomhara and G. M. Køien, **Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks**, Journal of Cyber Security, Vol. 4, 65–88. doi: 10.13052/jcsm2245-1439.414

[18] M. Faisal , I. Ali, M. S. Khan , S. M. Kim , J. Kim, **Establishment of Trust in Internet of Things by Integrating Trusted Platform Module: To Counter Cybersecurity Challenges, Complexity**, vol. 2020, Article ID 6612919, 9 pages, 2020. https://doi.org/10.1155/2020/6612919

[19] F. Fraternali, **Towards Large-Scale Autonomous Wireless Sensor Networks**, https://arxiv.org/abs/1906.12001v1, June 2019

[20] R. Shujaee, M. Nasiruddin, **Optimization of A Smart IOT Gateway International Journal on Recent and Innovation Trends in Computing and Communication**, July 2017 ISSN: 2321-8169, Volume: 5 Issue: 7 494 – 501, http://www.ijritcc.org

[21] Y. Jung, **Smart Disaster Response Through Localized Short-Term Cooperation**, ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2017, E. Sucar et al. (Eds.): AFI 2016, LNICST 179, pp. 12–21, 2017. DOI: 10.1007/978-3-319-49622-1_3

[22] R. K. Naha et al., **Fog Computing: Survey of Trends, Architectures, Requirements, and Research Directions**, IEEE Access, vol. 6, pp. 47980-48009, 2018, doi: 10.1109/ACCESS.2018.2866491.

[23] B. Mukherjee, R. Neupane, P. Calyam, **End-to-End IoT Security Middleware for Cloud-Fog Communication**, IEEE Cyber Security and Cloud Computing (CSCloud) June 2017 DOI:10.1109/CSCloud.2017.62

[24] B. Mukherjeea, S. Wangb, W. Lua, R. Neupanea, D. Dunna, Y. Rena, Qi Sua, P. Calyamb, **Flexible IoT Security Middleware for End-to-End Cloud-Fog Communication**, Future Generation Computer Systems February 7, 2018