Modern IoT Architectures Review: A Security Perspective

Ali H.Ahmed, Nagwa M. Omar, and Hosny M. Ibrahim

Deptartment of Information Technology,
Assiut University
Assiut, Egypt

***Abstract*—Internet of Things [IoT] enables a number of heterogeneous internet enabled devices to communicate through different protocols and network technologies. The last few years witnessed rapid improvements in different IoT fields e.g. smart energy, defense and public safety, smart farming and smart health. The heterogeneity nature of IoT is a key challenge against standardizations efforts, and hence the interoperability among IoT devices is reduced. In addition to interoperability problems, the limited capabilities hinder the application of security mechanisms. The recent research work focused on how to dynamically manage and secure IoT components across heterogeneous objects, transmission technologies, and networking architectures through proposing various IoT protocol stacks and security techniques. The need for standardized stack increases interoperability and applications development for human life. Many technologies such as software defined networks [SDN], Cloud, and Fog computing have integrated either to IoT applications or architectures to maintain and secure large-scale heterogeneous networks. In this paper, the most recent proposed IoT architectures and a fair discussion to their security benefits are presented and compared according to many factors such as QoS support for applications, security&privacy, mobility, and manageability.**

***Keywords*— IoT, IoT Architecture, IoT Applications, SDN, Interoperability, IoT Security, Cloud Computing, Fog Computing.**

I. INTRODUCTION

IoT is an integrated part of the future internet which can be briefly defined as dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols. IoT definition is fuzzy due to the concepts and technologies it includes [1]. For example, in [2] The IoT stands for a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols. While Atzori et al. [3] consider IoT as much more than uniquely addressable objects, it envisages the existence of services that may interface Things having identities and virtual personalities operating in smart spaces and using intelligent interfaces to connect and communicate within social, environmental, and user contexts. Further conceptual designs, visions and applications of the IoT are exposed in [4]–[10] all of which converge to the view that simple embedded sensor networking is now evolving to the much-needed standards and Internet enabled communication infrastructure between objects. IoT mainly consisting of an enormous number of objects connected to achieve different objectives according to the application context. Objects can include simple home sensors, medical devices, cars, airplanes, nuclear reactors and other things [11]. RFID and relevant technologies help in defining the identities to the IoT devices [12]. In 2010 the number of Internet-connected devices had surpassed the earth's human population [3]. There are already over 50 billion smart devices [13], anything that can be joined with a processing unit and connected to the internet is considered a thing in the IoT world. The challenge for IoT is related to connecting these devices in a manner that makes a complete distribution of application among things. Other problems such as addressing are treated by utilizing IPv6 and 6LowPAN which is a customized version of IPv6 for limited power IoT devices. IPv6 not only handles address depletion problem, but also solves the NAT barrier, involves strong authentication&security, and better support for mobility to end nodes as well. Interoperability is a challenge for IoT due to the need to handle a large number of heterogeneous things that belong to different platforms [17]. Application developers, and IoT device manufactures should consider interoperability to ensure the delivery of services for all customers regardless of the hardware platform they use. For example, most of the smart phones nowadays support communication technologies such as WiFi, NFC, and GSM to guarantee the interoperability in different scenarios. Also, programmers of the IoT should build their applications to allow for adding new functions without losing another or causing problems during integration with communication technologies. Consequently, interoperability is a significant criterion in designing and building IoT services to meet customers requirements [14]. Besides a variety of protocols, different implementations of the same standard present a challenge for interoperability [15]. To avoid such ambiguities, interoperability testing between different products in a testbed like ETSI Plugtests would be helpful. PROBE-IT4 [16] is a research project that aims to ensure the interoperability of validated IoT solutions. A standard architecture is considered the backbone for the IoT to create a competitive environment for companies and better support for interoperability [17]. IoTA [18], the European Lighthouse Integrated Project addressing the Internet-of-Things Architecture, proposes the creation of an Architectural Reference Model (ARM). Using an experi-

8th Annual International Conference on ICT: Big Data, Cloud and Security (ICT-BDCS 2017)

ISSN 2251-2136
doi: 10.5176/2251-2136_ICT-BDCS17.30

mental paradigm, IoT-A combine's top-down reasoning about architectural principles and design guidelines with simulation and prototyping to explore the technical consequences of architectural design choices. There are several design goals for ideal IoT architecture [19]:

1) Manageability: A large number of IoT nodes can be deployed to support a single application. Thus, having to manage Fault, Configuration, Accounting, Performance and Security (FCAPS) capabilities is necessary. Besides managing FCAPS of nodes, the manageability also involves the existence of intelligence or self-management In the architecture. The common types of manageability include centralized and distributed based control.
2) Security and Privacy: as the IoT network has expanded rapidly and the corresponding communication network environment has increased, the security issues are more complex than any existing network systems. This design goal also deals with the ability of how immune the architecture to outside attacks, it deals with various issues such CIA (Confidentiality, Integrity, and Availability). To achieve CIA, security techniques such as encryption, key exchange, authentication, etc. are used.
3) Mobility support must be considered while nodes are moving from place to another.
4) Cost-effectiveness determines the affordability of the architecture.
5) Efficiency is described in terms of resource consumption and power management of the connected devices.
6) The quality of service (QoS): a technique for the prioritization of different data traffic from devices according to application requirements.

In this paper a fair review for the IoT standardization efforts are presented as well as the modern proposed secure IoT architectures. The IoT security challenges also are presented. The paper sheds light on the modern converging technologies such as SDN, cloud, and fog computing in addition to their effect on IoT architectures. Also a comparison among the discussed Architectures is produced. Finally a proposed technique for securing IoT service discovery mechanism is presented. This paper is organized as follows: Section II provides an overview of modern IoT architectures, also it examines possible uses of SDN, cloud computing, and fog computing in the context of IoT, Section III presents the security challenges that hinder the development of powerful IoT applications and services, this section provides a comparison between the modern these architectures regarding the Mentioned design goals for ideal IoT architecture. Section IV proposes a secure layer that can be integrated into IoT architecture that aims secure service discovery in IoT by securing Multicast DNS (mDNS) and DNS Service Discovery(DNS-SD) protocols. Sections V concludes this paper.

II. IOT ARCHITECTURES REVIEW

IoT heterogeneity motivates authors to build several Architectures that focus on different perspectives. In [20] the author assumes that IoT architecture contain three layers; the Perception layer, network, and application layer. The author presented a four-layer secure architecture for IoT, every layer separately address the physical security of terminal equipment deployed in perception layer and local data storage, the safety of wireless transmission of sensor networks, the safety of computer networks and mobile communication transmission ,and the data service security on the application layer. The authors' proposed architecture is depicted in figure 1. Another secure architecture was proposed in [21], the IoT architecture is composed of four layers: Data Perception Layer, Heterogeneous Network Access Layer, Data Management Layer, and Intelligent Service Layer. The author presented security requirements for every layer and derived a secure architecture for IoT. The security requirements for every layer are listed in Table I.

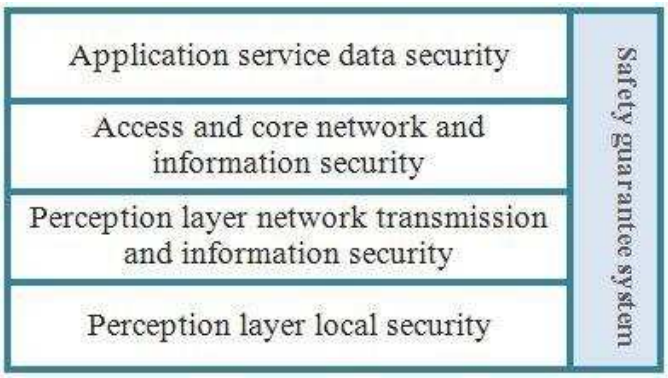


Fig. 1. The security architecture of the IoT proposed in [20].

TABLE I
SECURITY REQUIREMENTS FOR EVERY LAYER IN THE ARCHITECTURE PROPOSED IN [21]

IoT Layer	Security Requirements
Data Perception Layer	Secure routing. Key management. Intrusion detection. Wireless encryption. Reputation evaluation.
Heterogeneous Network Access Layer	User privacy. Data encryption. Data integrity. Multicast Security. Entity authentication. Access security.
Data Management Layer	Behavior entities certification. Data metric. Key generation and distribution. Security computation. Secure communication. Service multi-party computation.
Intelligent Service Layer	Access control management/ Security Management Privacy protection strategy

However, the authors in [20], [21] are pioneered in proposing secure architectures, they defined only bold lines and didn't describe any details regarding security mechanisms and

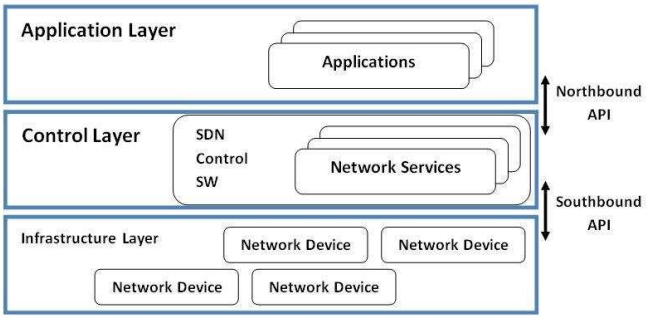


Fig. 2. The SDN system architecture

protocols required to fulfill the unique IoT security requirements such as security concerns, device and protocols heterogeneity, Limited device resources and mobility support. For example, the tremendous number of objects willing to connect to The Internet should be considered in many underlying protocols.

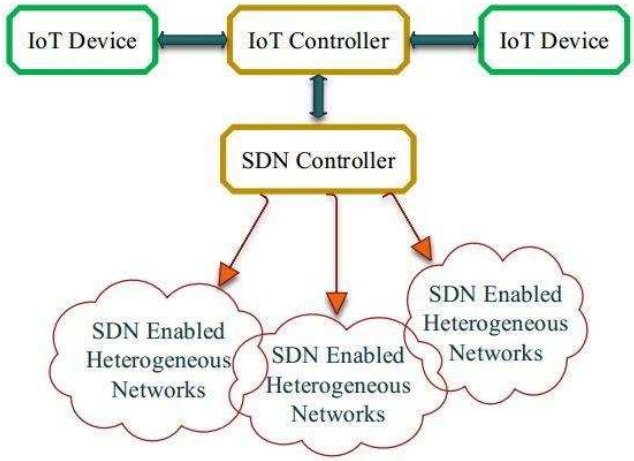
A. SDN-Based IoT Architectures

Open Networking Foundation (ONF) [22] is the group that is most associated with the development and standardization of SDN. According to ONF, SDN is an emerging architecture that is manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth and dynamic nature of todays applications. This architecture decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services. The OpenFlow [23], [24] protocol is a foundational element for building SDN solutions. Figure 2 highlights SDN architecture. IoT SDN-based architectures have evolved since 2015, the convergence of SDN to the IoT enables better objects managing, service installation in large scale. In [25], [26] standardization issues and possible uses of SDN in the context of IoT were presented. Integrating SDN and IoT will eliminate bottlenecks to efficiently process the data generated by IoT without placing a strain on the network, especially on Wi-Fi network as well as simplifying the information acquisition, information analysis, decision making, and action implementation process. Also, this integration will provide visibility of the network resources and management of access based on user, group, device, and application that eventually enables the ability to exchange data between users and even devices. In figure 3, we provide a typical high-level view of integrated SDN and IoT architecture.

In [25] the authors uses SDN to establish a flexible solution for IoT since it could enable node retasking, better resource sharing and reuse, and network management. According to [25] SDN can help in IoT standardization as following:

1) SDN can add the multicast feature to RPL-based applications [17] by configuring flow tables easily through the SDN controller. Since RPL RFC does not mention anycast addressing, anycast addressing can be implemented as it is similar to multicast but packets are delivered topologically to the nearest node in the des-

Fig. 3. Typical architecture of integration of SDN and IoT, a



high-level view proposed in [26]

tination group.SDN can take advantage of the topology knowledge to the nearest node beforehand.

2) To improve IoT scalability, nodes can be hierarchically organized. But unfortunately, RPL is not classified as hierarchical protocol. SDN controller can centralize the flow of packets from chosen nodes similar to cluster heads; the final packets flow are similar to multiple DODAG instances. Hence scalability and RPL hierarchical support are achieved for IoT Applications.
3) The SDN paradigm provides a centralized view for the nodes in IoT; this view enables node and resource management. The controller can consider the nodes' remaining energy during planning flow of packets.

The main disadvantages of [25] is that it doesn't cover all aspects of standardization, it only provides solutions to RPL shortages in the context of SDN. The literature ignores standardization issues in other IoT layers and doesn't provide solutions for security problems.

In [27] the authors attempts to utilize SDN to allow bidirectional data exchange between the Constrained Application Protocol (CoAP) [17] and Message Queuing Telemetry Transport(MQTT) [17] protocols without any modification. Both CoAP and MQTT are application protocols for IoT. In order to preserve the traditional MQTT and CoAP communication scenarios and enable bi-directional communication between the two protocols, a hybrid IoT communication framework based on SDN was presented. The SDN network intercepts all packets from CoAP to MQTT, and vice versa. If packets are belonging to the same protocols, they operate as the original communication scenarios and the SDN network just Ignore these traffic. Figure 4 depicts the authors proposed architecture.

However this architecture solves application protocols heterogeneity, it ignores security issues related to message interception during the bi-directional data exchange between CoAP And MQTT. Also, the author doesn't provide the

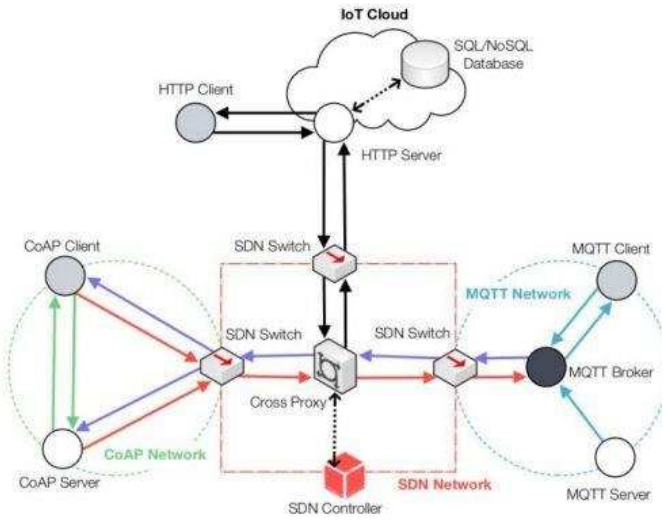


Fig. 4. The proposed hybrid IoT communication framework based on SDN in [27]

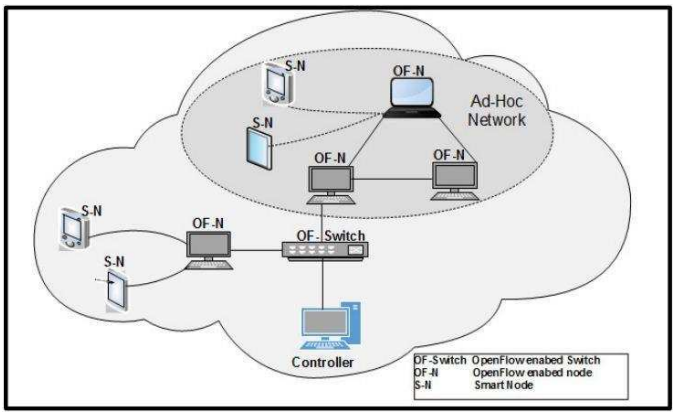


Fig. 5. An SDN Domain defined in [29]

detailed steps of message reformatting held during the bidirectional communication. Other application protocols such as Extensible Messaging and Presence Protocol (XMPP) [17], Data Distribution Service (DDS) [17], and Advanced Message Queuing Protocol (AMQP) [17] have not integrated into this architecture.

In [28], [29] a secure SDN-based architecture for IoT is proposed. The authors introduce the concept of SDN domain as a collection of wired, wireless, and Ad-Hoc network devices with or without infrastructure. Multiple domains are connected to form sensor networks or the IoT. Security policies can be executed on every domain to enforce specific service such as authentication. Every domain contains a set of nodes; these nodes are assumed to have an integrated SDN-Controller or connected to a node with an integrated SDN-Controller. Figures 5, 6 depicts the authors' idea.

To secure network access and resources, the SDN controllers begin by authenticating the network devices. Once the OpenFlow secure connection between the switch and the

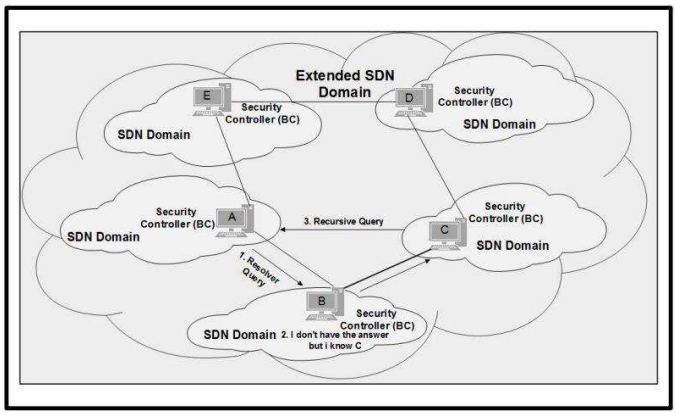


Fig. 6. SDN Domain interconnection [29]

controller is established, the controller blocks switch ports directly connected to the users. After that, the controller authorizes only users authentication traffic. Once the user is authenticated, and based on the authorization level of the user, the controller will push the appropriate flow entries to the software or the hardware access switch. The Authentication process is extended to devices. Each device has to associate itself with an OpenFlow enable node, each of which is connected to one controller in their domain. Although this is a secured architecture, it assumes every node or at least most nodes with an integrated SDN-Controller which may not be available in specific cases.

The benefits of importing ideas from SDN architecture into IoT architecture can be gained through different implementations. In [30] some promising solutions for the IoT-based on SDN architectures were studied. The authors introduced solutions for managing the sensing layer in terms of:

1) SDNs can play a crucial role in management sensors Objects or ZigBee-based WSNs. The SDN controller can Be at the sink node or gateways. The location of the controller made it possible to control the sleep/active cycle intervals of the sensors.
2) Based on the application requirements, the controller can optimize routing decisions for better QoS.
3) Multiple applications can be used over the underlying IoT sensory network without the need for network redesign.

The author also mentioned the sensing as a service (SaaS) [31] which is a cloud paradigm that is expected to exist on top of IoT infrastructure to facilitate sensing services in a wide area network. SaaS also provides a business model that allows organizations or individuals to sell the sensing services. However, this model can't succeed because the only mining technique for sensory data is keyword-based which may not be suitable for capturing sensor characteristics for specific application contexts.

A context-aware IoT architecture is proposed in [32] that can forward and process IoT traffic in data plane based on contextual information exposed from both high application layer and low sensor-layer, to fill the gap between IoT and IP Network through software-defined data plane. Figure 7 depicts the authors proposed architecture.

According to [33] the software-defined data plane defines new services for Mobile Virtual Network Operators (MVNOs)

that obtain network services from mobile network operators and resell network services to customers at their own prices without owning the wireless network infrastructure on Their own. There are a large number of MVNOs all over The world and most of them are competing on price. The advantages of the authors' proposed architecture are high security and privacy inherited from MVNOs network, high cost-performance with low-cost MVNO, and new value-added service for MVNOs.

Table II provides a fair comparison between the previously mentioned architecture regarding manageability, security and privacy, mobility support, cost-Effectiveness, Efficiency and QoS.

B. Cloud and Fog Computing and its possible uses in IoT architecture

Cloud computing paradigm [34] realizes the delivery of hardware and software resources over the Internet according To on-demand utility-based model. Depending on the type of computing resources delivered via the cloud, cloud services take different forms such as Network as a Service (NaaS),

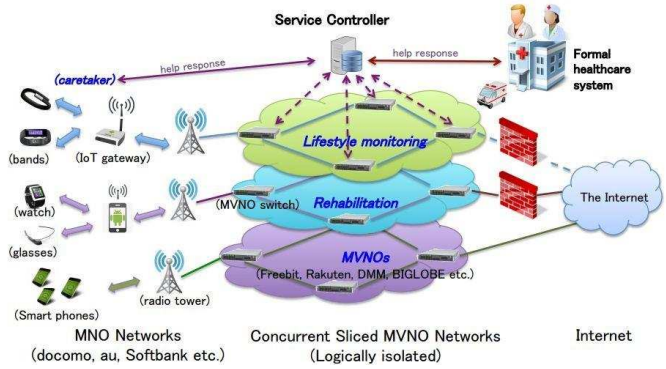


Fig. 7. Architecture of IoT framework on top of MVNO in [32]

Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Storage as a service (STaaS) and more. These services hold to promise to deliver increased reliability, security, high availability and improved QoS at an Overall lower Total Cost of Ownership (TCO). The integration of cloud computing in IoT have many of challenges [17] such as synchronization and standardization between the different cloud vendors.

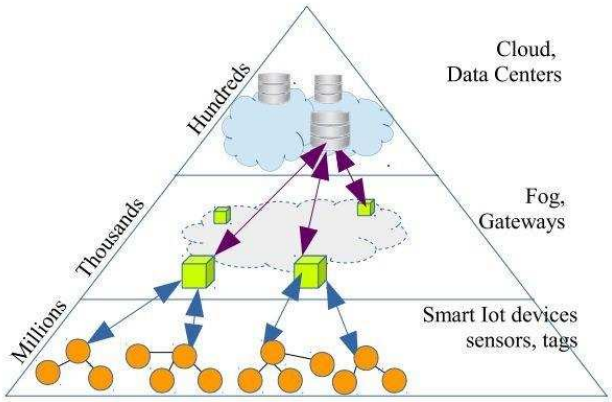
Fog computing [35] is an architecture that moves computations closer to the end user, its found in large cloud systems And big data, making reference to the growing difficulties in accessing information in large scale. Fog networking supports the IoT, in which most of the devices used by humans on a daily basis will be connected to each other. The Fog Computing pushes intelligence from the cloud to the edge and localizes certain kinds of analysis and decision-making. The benefits of localization are quicker response times, independence from network latency, as well as reduced traffic And hence low resources consumption. In Fog Computing, processing happens on nodes physically closer to where the data is collected instead of sending vast amounts of IoT data to the cloud, this enhances IoT services, security, resources consumptions, and latency [35].

Fig. 8. The role of cloud and fog computing in IoT services [17]

In [17], [36] the authors presented how fog and cloud computing can be integrated into IoT services in hierarchical manner which is depicted in figure 8.

III. IOT SECURITY CHALLENGES

1) CIA Requirements. Which means that IoT traffic must Has Confidentiality, Integrity, and Availability. Confidentiality is to ensure IoT traffic is secure, come from Confident users, and available only to specific users. The Integrity mainly focuses on preventing IoT traffic from Tampering or modification. Integrity can be implemented by end-to-end security in IoT communication. Also IoT traffic can be managed via firewalls, but it does not guarantee the security at endpoints because of low computational power at IoT devices [37]. Finally the availability means having IoT data and services available whenever they are needed. The availability issue is strongly related to scalability of the IoT, i.e. the IoT must operate smoothly, and service can be accessed on large scale set of connecting devices



and services. The limited resources for most IoT devices in addition to their heterogeneity, large scale, different edge technologies and countries security policies are the main factors that ban the implementation of a holistic CIA solution for IoT. According to [38] 70 percent of IoT devices analyzed did not encrypt communications to the internet and local network, while half of the devices mobile applications performed unencrypted communications to the cloud, Internet or local network. Transport encryption is crucial given that many of the tested devices collected and transmitted sensitive data across channels.

TABLE II IOT ARCHITECTURES COMPARISON

Architecture Reference	Manageability	Security&Privacy	Mobility	Cost-Effectiveness	Efficiency	QoS
[20], [21]	N/A	Yes	Yes	Yes	N/A	Yes
[25]	Yes Inherited from SDN	No	N/A	Yes	Yes	N/A
[27]	Yes Inherited from SDN	No	Yes	Yes	Yes	N/A
[28], [29]	Yes Inherited from SDN	Yes	Yes	No	Yes	Yes
[30]	Yes Inherited from SDN	N/A	Yes	Yes	No	No
[32]	Yes Inherited from SDN	N/A	Yes	No	Yes	N/A

2) Authentication is the process of verifying the identity of a user. Each object in the IoT must authenticate other objects. IoT objects may include devices, service providers, and humans; this heterogeneity made authentication challenging. Authentication is achieved through many methods such as ID/password, pre-shared Secrets, and public-key cryptosystems which involve key management procedures to save and distribute key. The lack of existence of global Certificate Authority mainly hinders authentication between IoT entities also issuing a certificate for every entity in IoT is not feasible. Delegated authentication solves this problem so it must be taken into consideration for IoT.
3) Lightweight security solutions. The public key crypto is considered the most secure solution for authentication, confidentiality and integrity, but the problem that hinders its uses in IoT is that it has a lot of computations to be performed by a device. Due to the limited processing and resource capabilities of the IoT devices, lightweight solutions are a key feature for IoT security. It is not a goal in itself rather a restriction that must be considered while designing and implementing protocols either in encryption or authentication of data and devices in IoT [37].
4) Key Management Systems(KMS) protocols are classified in four main categories [39]:
   a) Key Pool Framework: whose first protocol wasintroduced by Eschenauer and Gligor [40], considers that a node stores a small subset of keys Retrieved from a global key pool. If two nodes find a common key, they can use them to establish a Session key.
   b) Negotiation framework: more simplistic approach,where nodes negotiate all shared keys after the deployment [41]–[43].
   c) Mathematical framework: certain KMS protocols[44]–[46] use mathematical concepts such as Linear Algebra, Combinatorics, and Algebraic Geometry for calculating the pairwise keys of the nodes.
   d) The public key framework: relies on PKC to securely bootstrap the pairwise key of two nodes over the public communication channel

In IoT, the devices and IoT sensors need to exchange key for either public or symmetric cryptographic algorithms. For this purpose, there needs to be a lightweight key management system for all frameworks that can enable trust between different things, and can distribute keys by consuming devices minimum capabilities [47]. Table III summarizes the characteristics for every key management protocol in IoT devices.

TABLE III
KMS AND REQUIREMENTS IN IOT

Framework	Scalability	Computations	Storage
Key Pool	Yes	Low	Large
Negotiation	No	Moderate	Moderate
Mathematical	Yes	Heavy	Moderate
Public key	Yes	Heavy	Low

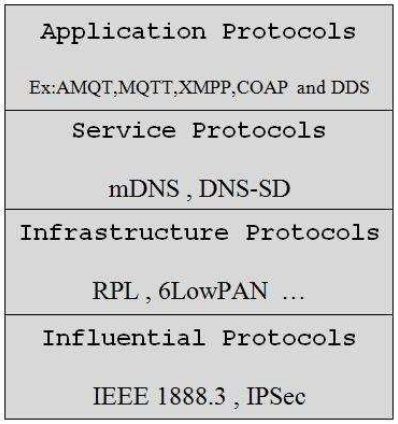


Fig. 9. Service discovery protocols inside the big picture.

IV. SECURITY IN IOT SERVICE DISCOVERY

The enormous number of devices in most IoT applications requires an efficient, dynamic and Zero Configurations technique For services discovery. Figure 9 shows the position of service discovery protocols in IoT protocol stack.

Multicast DNS (mDNS) and DNS Service Discovery (DNSSD) protocols have been designed originally for service discovery in resource- rich devices, there are research studies

that adapt light versions of them for IoT environments [48], [49]. The goal of the Zero Configuration Networking (Zeroconf) is to enable networking in the absence of administration. Zero configuration networking is required for environments where the administration is impractical or impossible, such as in the home or small office. Essentially, to reduce network configuration to zero (or near zero) in Internet Protocol (IP) networks, it is necessary to:

1) Distribute IP addresses (without a Dynamic Host Configuration Protocol [DHCP] server).
2) Provide name translation (without a [DNS] server). 3) Find and list services (without a directory service).
4) Distribute multicast IP addresses, if necessary (without a multicast server).

A. Multicast DNS and DNS Service Discovery

The multicast Domain Name System (mDNS) [50] resolves host names to IP addresses within small networks that do not include a local name server. It is a zero-configuration service, using the same programming interfaces, packet formats and operating semantics as the unicast Domain Name System. In IoT world, mDNS is considered serverless messaging. The mDNS technology provides the ability to perform DNS-like operations on a local link in the absence of any conventional unicast DNS server.

DNS Service Discovery [51] is a way of using standard DNS programming interfaces, servers, and packet formats to browse the network for services.DNS Service Discovery is compatible with Multicast DNS. DNS-SD is a convention for naming and structuring DNS SRV records such that a client can dynamically discover a domain for a service using only standard DNS queries.

B. Possible Vulnerabilities

The following attacks can be successful because all data needed for service discovery is sent in plaintext, each responder answers queries from each querier and each querier accepts answers from each responder.

1) Passive: The passive attacker wants to get as much information as possible by just listening to the multicast traffic. All plaintext information will be gained by this attacker.
2) Active: An active attacker wants to get information by sending queries for services he is interested in. He might ask for all presence service instances, extract the version numbers from the TXT records, identify the vulnerable versions and attack the corresponding hosts. He can also offer (fake) services to make someone connect.

C. Securing Services Discovery in IoT

Secure service discovery can be achieved using mutual authentication between communication parities (service requester SR, and target device TD). The following building blocks can be used to fulfill mutual authentication:

1) Private Mutual Authentication. In this case, SR only reveals his identity to a set of TD and TD will do the same. Finally, one part must reveal his identity first, it strongly recommends to be the SR.
2) Identity and Authorization Model. Every part has a signing + verification key, and a collection of humanreadable names bound to their public keys via a certificate chain.
3) A secure key exchange such Diffie-Hellman.

V. CONCLUSION

The new technology of IoT is rapidly invading our modern life to improve its quality. The IoT combines several heterogeneous technologies together to achieve a specific set of services or applications. The increasing number of IoT proposed architectures has not converged to a reference model or a common architecture. This paper presented a fair set of modern proposed architectures for IoT. Also it provided the possible advantages and disadvantages for every architecture, finally a comparison produced to put all the ideas together. IoT until the time of these words still haven't any reference model, the next few years will produce interesting results and reference architecture can be found.

REFERENCES

[1] Maria Rita Palattella, Nicola Accettura, and Xavier Vilajosana, "Standardized Protocol Stack for the Internet of (Important) Things", IEEE Communications Surveys & Tutorials, vol.15, no. 3, pp.1389-1406, 2013.

[2] INFSO D.4 Networked Enterprise RFID INFSO G.2 Micro Nanosystems in Co-operation with the Working Group RFID of the ETP EPOSS, Internet of Things in 2020, Roadmap for the Future, Version 1.1, European Commission, Information Society and Media, Tech. Rep., May 2008.

[3] L. Atzori, A. Iera, and G. Morabito, The Internet of Things: A survey, Computer Networks, vol. 54, no. 15, pp. 27872805, October 2010.

[4] M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, From Todayss INTRAnet of Things to a Future INTERnet of Things: A Wireless- and MobilityRelated View, IEEE Wireless Commun., vol. 17, no. 6, pp. 44 51, December 2010.

[5] L. Coetzee and J. Eksteen, The Internet of Things - Promise for the Future? An Introduction, in IST-Africa Conference Proceedings, May 2011.

[6] E. Fleisch, What is the Internet of Things? - An Economic Perspective, Auto-ID Labs, Tech. Rep., 2010.

[7] European Research Cluster on Internet of Things (IERC), Internet of Things - Pan European Research and Innovation Vision, IERC, Available online: http://www.internet-of-things-research.eu/documents.htm, October 2011.

[8] L. Mainetti, L. Patrono, and A. Vilei, Evolution of Wireless Sensor Networks towards the Internet of Things: A Survey, in 19th International Conference on Software, Telecommunications and Computer Networks, SoftCOM, September 2011.

[9] J. P. Vasseur and A. Dunkels, Interconnecting Smart Objects with IP: The Next Internet. Morgan Kaufmann, 2010.

[10] O. Hersent, D. Boswarthick, and O. Elloumi, The Internet of Things:Key Applications and Protocols. Wiley, 2012.

[11] Flauzac Olivier, Gonzalez Carlos and Nolot Florent, "New Security Architecture for IoT Network", ELSEVIER , pp.1028-1033,2015.

[12] Vimal Jerald. A , Albert Rabara. S, and Daisy Premila Bai,"Secure IoT Arcitecture for Integrated Smart Environment ", IEEE, pp. 800-805,2016.

[13] Gaitan N. Cristina, Gaintan V. Gheorghita, and Ungurean Ioan, "Gradual Development of an IoT Architecture for Real-World Things", IEEE, pp.344-349, 2015.

[14] A. Dunkels, J. Eriksson, and N. Tsiftes, Low-power interoperability for the IPv6-based Internet of Things, in Proc. 10th Scandinavian Workshop Wireless ADHOC, Stockholm, Sweden, pp. 1011, 2011.

[15] I. Ishaq et al., IETF standardization in the field of the Internet of Things (IoT): A survey, J. Sens. Actuator Netw., vol. 2, pp. 235287,2013.

[16] Available online: http://www.probe-it.eu/, last accessed 30/1/2017.

[17] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash ,"Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications", IEEE Communications Surveys & Tutorials, vol. 17, no.4, pp.2347-2376, 2015.

[18] Available online: http://www.iot-a.eu/public, last accessed 30/1/2017.

[19] Ravi Teja Guthikonda , Sai Srikar Chitta, Shraddha Tekawade, and Tripti Attavar ,"Comparative Analysis of IoT architectures", TLEN 5710 Capstone, 2014.

[20] Bing Zhang, Xin-Xin Ma, and Zhi-Guang Qin,"Security Architecture on the Trusting Internet of Things ", JOURNAL OF ELECTRONIC SCIENCE AND TECHNOLOGY, VOL. 9, NO. 4, DECEMBER 2011

.

[21] Dong Chen, Guiran Chang, Lizhong Jin, Xiaodong Ren, Jiajia, and Fengyun Li, "A Novel Secure Architecture for the Internet of Things ", Fifth International Conference on Genetic and Evolutionary Computing, 2011.

[22] Available online:https://www.opennetworking.org/, last accessed 2/2/2017.

[23] Available online: https://www.opennetworking.org/sdn-resources/ openflow, last accessed 2/2/2017.

[24] Bruno Astuto A. Nunes, Marc Mendonca, and Xuan-Nam Nguyen,"A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks", IEEE Communications Surveys & Tutorials, vol.16, no.3, pp. 1617 - 1634, 2014.

[25] Bruno Trevizan de Oliveira, Renan Cerqueira Afonso Alves, and Cintia Borges Margi, "Software-defined Wireless Sensor Networks and Internet of Things standardization synergism",2015 IEEE Conference on Standards for Communications and Networking (CSCN),pp. 60-65, 2015.

[26] Keshav Sood, Shui Yu, and Yong Xiang, "Software Defined Wireless Networking Opportunities and Challenges for Internet of Things: A Review" , IEEE INTERNET OF THINGS JOURNAL, pp. 1-12, 2015.

[27] Chao-Hsien Lee,Yu-Wei Chang, and Chi-Cheng Chuang,"Interoperability enhancement for Internet of Things protocols based on software-defined network",2016 IEEE 5th Global Conference on Consumer Electronics, 2016.

[28] Olivier Flauzac, Carlos Gonzlez, Abdelhak Hachani, and Florent Nolot, "SDN Based Architecture for IoT and Improvement of the Security", IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, pp. 688-693, 2015.

[29] Olivier Flauzac, Carlos Gonzlez, and Florent Nolot," New Security Architecture for IoT Network", Elsevier, International Workshop on Big Data Challenges on IoT and Pervasive Systems (BigD2M 2015), 2015.

[30] Amr El-Mougy, Mohamed Ibnkahla, and Lobna Hegazy, "SoftwareDefined Wireless Network Architectures for the Internet-of-Things", 40th Annual IEEE Conference on Local Computer Networks, pp. 804-8011, 2015.

[31] C. Perera, A. Zaslavsky, C. Liu, M. Compton, P. Christen and D. Georgakopoulos, "Sensor search techniques for sensing as a service architecture for the Internet of Things," IEEE Sensors Journal, vol. 14, no. 2, pp. 406-420, 2014.

[32] Ping Du, Pratama Putra, Shu Yamamoto, and Akihiro Nakao, "A Context-aware IoT Architecture through Software-defined Data Plane", IEEE Region 10 Symposium (TENSYMP), Bali, Indonesia, pp. 315-320, 2016.

[33] Akihiro Nakao, Ping Du, and Takamitsu Iwai, Application specific slicing for MVNO through software-defined data plane enhancing SDN, IEICE Transactions on Communications, vol. 98, no. 11, pp. 21112120, 2015.

[34] Suciu, George, Suciu, Victor and Martian, Alexandrua," Data, Internet of Things and Cloud ConvergenceAn Architecture for Secure E-Health Applications ", Journal of medical systems Volume: 39 Issue: 11 Pages: 141 , Nov 2015.

[35] Mung Chiang, Tao Zhang, "Fog and IoT: An Overview of Research Opportunities", IEEE INTERNET OF THINGS JOURNAL, VOL. 3, NO. 6, DECEMBER 2016.

[36] Flavio Bonomi, Rodolfo Milito, Jiang Zhu , San Jose, and Sateesh Addepalli , Fog computing and its role in the internet of thingsMCC '12 Proceedings of the first edition of the MCC workshop on Mobile cloud computing pp.13-16, 2012.

[37] Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, and Imran Zualkernan , " Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures", The 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015), pp. 336-341, 2015.

[38] HP News, Available online:http://www8.hp.com/us/en/hp-news/ press-release.html?id=1744676#.WPyG50XyvZ4, last accessed 23-42017.

[39] Liu D, Ning P and Li R.," Establishing pairwise keys in distributed sensor networks". ACM Transactions on Information and System Security (TISSEC), vol. 8 no. 1, pp. 4177, 2005.

[40] L. Eschenauer, V.D. Gligor. A Key-management Scheme for Distributed Sensor Networks. Proceedings of the 9th ACM conference on Computer and communications security (CCS 02), pp. 41-47, 2002.

[41] R. J. Anderson, H. Chan, A. Perrig. Key Infection: Smart Trust for Smart Dust. Proceedings of the 12th IEEE International Conference on Network Protocols (ICNP 2004), pp. 206-215, 2004.

[42] A. Seshadri, M. Luk, A. Perrig. SAKE: Software Attestation for Key Establishment in Sensor Networks. Proceedings of the 2008 International Conference on Distributed Computing in Sensor Systems (DCOSS08), pp. 372-385, 2008.

[43] B. Panja, S. Madria, and B. Bhargava. Energy and Communication Efficient Group Key Management Protocol for Hierarchical Sensor Networks. Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC06), pp. 384-393, 2006.

[44] W. Du, J. Deng, Y. S. Han, P. Varshney, J. Katz, A.

Khalili. A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks. ACM Transactions on Information and System Security (TISSEC), Vol. 8, No. 2, pp. 228-258, 2005.

[45] S. A. Camtepe, B. Yener. Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks. IEEE/ACM Transactions on Networking, Vol. 15, No. 2, pp. 346-358, 2007.

[46] D. Liu, P. Ning, R. Li. Establishing Pairwise Keys in Distributed Sensor Networks. ACM Transactions on Information and System Security, Vol. 8, No. 1, pp. 41-77, 2005.

[47] Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, Shiuhpyng Shieh, " IoT Security: Ongoing Challenges and Research Opportunities", 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, pp. 230-234, 2014.

[48] A. J. Jara, P. Martinez-Julia, and A. Skarmeta, Light-weight multicast DNS and DNS-SD (lmDNS-SD): IPv6-based resource and service discovery for the web of things, in Proc. 6th Int. Conf. IMIS Ubiquitous Comput., 2012, pp. 731738.

[49] R. Klauck and M. Kirsche, Chatty thingsMaking the Internet of Things readily usable for the masses with XMPP, in Proc. 8th Int.
Conf. CollaborateCom, 2012, pp. 6069.

[50] S. Cheshire and M. Krochmal, Multicast DNS, Internet Eng. Task Force (IETF), Fremont, CA, USA, Request for Comments: 6762, 2013.

[51] M. Krochmal and S. Cheshire, DNS-based service discovery, Internet Eng. Task Force (IETF), Fremont, CA, USA, Request for Comments:
6763, 2013.