Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 16 Issue 7 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Review on Internet of Things (Iot): Security and Privacy Requirements and the Solution Approaches

By Muhammad A. Iqbal, Oladiran G.Olaleye & Magdy A. Bayoumi

University of Louisiana at Lafayette

Abstract- The world is undergoing a dramatic rapid transformation from isolated systems to ubiquitous Internet-based-enabled 'things' capable of interacting each other and generating data that can be analyzed to extract valuable information. This highly interconnected global network structure known as Internet of Things will enrich everyone's life, increase business productivity, improve government efficiency, and the list just goes on. However, this new reality (IoT) built on the basis of Internet, contains new kind of challenges from a security and privacy perspective. Traditional security primitives cannot be directly applied to IoT technologies due to the different standards and communication stacks involved.

Keywords: internet of things (IOT), security, privacy issues, wireless sensor networks, RFID, authentication, key management.

GJCST-E Classification: C.2.0 K.4.1

A Review on Internet of Things (Iot): Security and Privacy Requirements and the Solution Approaches

Muhammad A. Iqbal [α], Oladiran G. Olaleye [σ] & Magdy A. Bayoumi [ρ]

Abstract- The world is undergoing a dramatic rapid transformation from isolated systems to ubiquitous Internet-based-enabled 'things' capable of interacting each other and generating data that can be analyzed to extract valuable information. This highly interconnected global network structure known as Internet of Things will enrich everyone's life, increase business productivity, improve government efficiency, and the list just goes on. However, this new reality (IoT) built on the basis of Internet, contains new kind of challenges from a security and privacy perspective. Traditional security primitives cannot be directly applied to IoT technologies due to the different standards and communication stacks involved. Along with scalability and heterogeneity issues, major part of IoT infrastructure consists of resource constrained devices such as RFIDs and wireless sensor nodes. Therefore, a flexible infrastructure is required capable to deal with security and privacy issues in such a dynamic environment. This paper presents an overview of IoT, security and privacy challenges and the existing security solutions and identifying some open issues for future research.

Keywords: internet of things (IOT), security, privacy issues, wireless sensor networks, RFID, authentication, key management.

I. Introduction

The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it". This was Mark Weiser's central statement in his seminal paper [Weis 91] in Scientific American in 1991. IoT concept has begun to shape our modern world including a common man's everyday life in the society, a world in which devices of every shape and size are manufactured with "smart" capabilities that allow them to communicate and interact not only with other devices but also with humans, exchange their data, make autonomous decisions and perform useful tasks based on preset conditions. IoT is becoming well-known concept across many horizontal and vertical markets with its numerous applications [1].Just to give an example how IoT would affect our daily life: You enter the supermarket and receive your fridge's text message: "You are out of milk." In the dairy section, sensors signal your grocery cart that you've taken a milk carton. As you walk towards the pharmacy, your fitness wristband vibrates as it takes your vitals and streams the results to your doctor to adjust your prescription. When you're finished shopping, you simply walk out the door. Your credit card is charged when you exit the supermarket's geofence. As you drive home, your car communicates with other cars on the roadway to prevent accidents.

The early years of Internet of Things (IoT) started with Machine to Machine (M2M) communication. M2M communication indicates two machines communicating with each other, usually without human involvement. The communication platform is not defined, and can be both wireless and wired communication. The term M2M stems from telephony systems. In these systems, different endpoints needed to exchange information between each other, such as the identity of the caller. This information was sent between the endpoints without a human being needed to initiate the transmission. The M2M term is still very much in use, especially in the industrial market, and is commonly regarded as a subset of IoT [5].

The term internet of things was devised by Kevin Ashton, cofounder and executive director of Auto-ID Center at MIT in 1999 and refers to uniquely identifiable objects and their virtual representations in an "internet-like" structure [25]. The Oxford Dictionary perhaps offers a concise definition that invokes the Internet as an element of the IoT:

Internet of things (noun): The interconnection via the Internet of computing devices embedded in everyday objects enabling them to send and receive data.

Nevertheless, in the past decade, this concept has been extended because of new IoT network applications such as e-healthcare and transport utilities [25]. The evolution of the IoT has its origin in the convergence of wireless technologies, advancements of micro electromechanical systems (MEMS) and digital electronics where has been as a result miniature devices with the ability to sense and compute and communicate wirelessly. In the era of IoT, the interaction or relationship between humans and machines is ever more considered as machines getting smarter and starting to handle more human tasks, and in this situation humans

Author α σ: The Center for Advanced Computer Studies, University of Louisiana at Lafayette, LA 70504 USA working in the area of security for Internet of Things, Wireless Sensor Networks and Cognitive Radio Networks. e-mail: mxi1678, ogo8842@cacs.louisiana.edu

Author ρ: Dr. Magdy Bayoumi is Professor at The Center for Advanced Computer Studies, University of Louisiana at Lafayette, LA 70504 USA. e-mail: mab@cacs.louisiana.edu

are required to trust the machine and feel safe. In this way, a thing might be a patient with a medical implant to facilitate real-time monitoring in a healthcare application or an accelerometer for movement attached to the cow in a farm environment [26].

These things or devices in IoT include familiar scannables and wearables and more complex systems like home appliances, vehicles, and smart roads and bridges. It is predicted that IoT will consist of 50 billion connected devices by 2020 and that the worldwide IoT market will be more than a $10 trillion industry. These projections depict the possibility of a smarter, efficient and safer world of inter-connected devices [27] while some observers show concerns that the IoT represents a darker world of surveillance, privacy and security violations, and consumer lock–in. Attention-grabbing headlines about the hacking of internet-connected automobiles, surveillance concerns arising from voice recognition features in "smart" TVs, and privacy fears stemming from the potential misuse of IoT data have captured public attention. This "promise vs. peril" debate along with an influx of information though popular media and marketing can make the IoT a complex topic to understand [22].

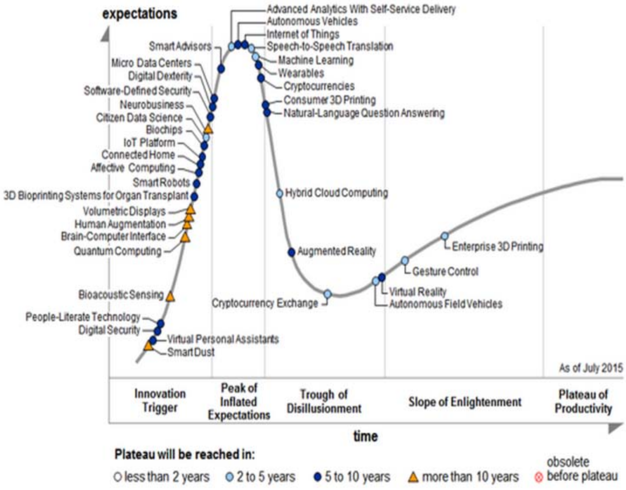

Figure 1: Hyper Cycle for Emerging Technologies, 2105[12]

Garter's Hype Cycle is a way to represent emergence, adoption, maturity and impact on applications of specific technologies. The latest Gartner Hype Cycle for Emerging Technologies places it at the peak. IoT has been identified as one of the emerging technologies as shown below in the Hype Cycle in Emerging Technologies Report for the year 2015[28].

II. Security for Internet of Things

If one thing can prevent the Internet of things from transforming the way we live and work, it will be a breakdown in security. While security considerations are not new in the context of information technology, the attributes of many IoT implementations present new and unique security challenges. Addressing these challenges and ensuring security in IoT products and services must be a fundamental priority. Users need to trust that IoT devices and related data services are secure from vulnerabilities, especially as this technology become more pervasive and integrated into our daily lives. Important challenge is the integration of security mechanisms and the user acceptance. User must feel that they control any information that is related to them rather than they feel they are being controlled by the system. This integration generates new requirements, not been previously considered.

The interconnected nature of IoT devices means that every poorly secured device that is connected online potentially affects the security and resilience of the Internet globally. This challenge is amplified by other considerations like the mass-scale deployment of homogenous IoT devices, the ability of some devices to automatically connect to other devices, and the likelihood of fielding these devices in unsecure environments. As a matter of principle, developers and users of IoT devices and systems have a collective obligation to ensure they do not expose users and the IoT infrastructure itself to potential harm. Accordingly, a collaborative approach to security will be needed to develop effective and appropriate solutions to IoT security challenges that are well suited to the scale and complexity of the issues [22].

Full potential of the IoT depends on strategies that respect individual privacy choices across a broad spectrum of expectations. The data streams and user specificity afforded by IoT devices can unlock incredible and unique value to IoT users, but concerns about privacy and potential harms might hold back full adoption of the Internet of Things. This means that privacy rights and respect for user privacy expectations are integral to ensuring user trust and confidence in the Internet, connected devices, and related services. Indeed, the Internet of Things is redefining the debate about privacy issues, as many implementations can dramatically change the ways personal data is collected, analyzed, used, and protected. For example, IoT amplifies concerns about the potential for increased surveillance and tracking, difficulty in being able to opt out of certain data collection, and the strength of aggregating IoT data streams to paint detailed digital portraits of users. While these are important challenges, they are not insurmountable. In order to realize the opportunities, strategies will need to be developed to respect individual privacy choices across a broad spectrum of expectations, while still fostering innovation in new technology and services [22].

The remainder of this paper is organized as follows: Section II further gives an overview of the IoT features, layers; we first identify properties that make the IoT unique in terms of the security and privacy challenges. In the next section, we describe the security primitives and solutions approaches that take into account to secure the network communication and protect user's data. Finally, Section IV concludes the paper and gives insights regarding current research gaps and possible future directions.

a) *IoT Features And Security Requirements*

In this section, we identify the features that constitute the uniqueness of the IoT in terms of the security and privacy challenges and the layers of IoT. We will see how security issues are different in IoT as compared to traditional internet networks. Moreover, we will establish a number of security and privacy requirements, based on the described properties, and will discuss them in detail.

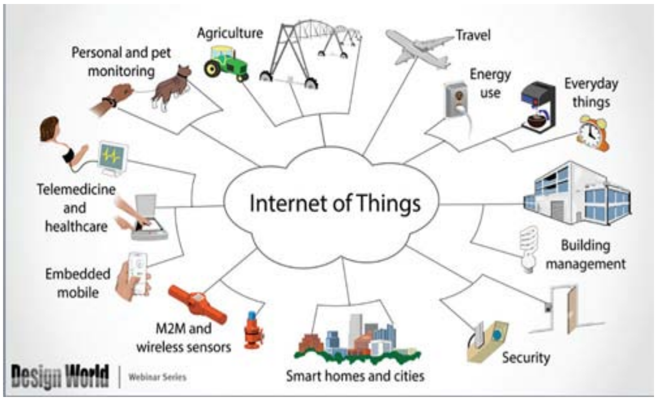

Figure 2: Internet of Things Applications

In contrast to traditional IT systems such as enterprise applications, cloud computing, and big data, a combination of a number of properties makes the IoT unique in terms of the challenges that need to be coped with. We identify these properties by analyzing related IoT research [29]–[30]. A major barrier to realizing the full promise of IoT is that around 85% of existing things were not designed to connect to Internet and cannot share data with the cloud according to IMS research. Addressing this issue, gateways from mobile, home, and industrial act as intermediaries between legacy things and the cloud, providing the needed connectivity, security and manageability described by Intel.

The identified distinguishing properties are four, namely: the uncontrolled environment, the heterogeneity, the need for scalability, as well as the constrained resources utilized in the IoT

Uncontrolled Environment: Many things will be part of a highly uncontrolled environment; things travel to untrustworthy surroundings, possibly without supervision. Sub properties of the uncontrolled environment *Mobility:* Stable network connectivity and constant presence cannot be expected in such an environment.

Physical Accessibility: In the IoT, sensors can be publicly accessible, e.g., traffic control cameras, and environmental sensors.

Trust: A priori trusted relationships are unlikely for the large amount of devices interacting with each other and users [22]. Thus, automated mechanisms to measure and manage trust of things, services, and users are crucial for the IoT.

Heterogeneity: IoT is expected to be a highly heterogeneous ecosystem as it will have to integrate a multitude of things from various manufacturers. Therefore, version compatibility, and interoperability have to be considered.

Scalability: The vast amount of interconnected things in the IoT demands highly scalable protocols. This also has an influence on security mechanisms. For instance, centralized approaches, e.g., hierarchical Public Key Infrastructures (PKIs), as well as some distributed approaches, e.g., pairwise symmetric key exchange schemes, cannot scale with the IoT.

Infrastructures (PKIs), as well as some distributed approaches, e.g., pairwise symmetric key exchange schemes, cannot scale with the IoT.

Constrained Resources: Things in the IoT will have constraints that need to be considered for security mechanisms. This includes energy limitations, e.g., battery powered devices, as well as low computation power, e.g., micro sensors. Thus, heavy computational cryptographic algorithms cannot be applied to all things. IoT and traditional network security issues are different in many ways. IoT is composed of RFID nodes and WSN nodes, whose resources are limited, while the Internet is composed of PC, severs, smart phones whose resources are rich. In the Internet, we use combinations of complex algorithms and lightweight algorithms to maximize security with less considerations of resource usage such as computation power. While in IoT, most of the cases, we can only use lightweight algorithms to find the balance between security and power consumptions. Connection between IoT nodes are always through slower, less secure wireless media, which results in easy data leakage, easily node compromising and all other insecure issues. Whereas in Internet, most communications are through faster, more secure wire or wireless communications. Even with the Mobile Internet, wireless connections are built on top of complex secure protocols which are almost impossible to implement for resource limited IoT nodes.

Although there are various devices in the Internet, but with the abstraction of operating system, their data formats are almost the same with Window Family and Unix-like operating systems. However, in IoT, what we have is just bare wireless node. There is no operating system, just a simple embedded program for the chip. With the diversity of nodes perception goal, there comes different chip hardware which result in heterogeneous data contents and data formats. There are all kinds of IoT applications in application layer, used in our everyday life; they gather our private information every second automatically to make our life easier. These applications can even control our everyday life environment. It would be of great potential security problems if we lose control of IoT system. While in the Internet, if we do not provide our information ourselves, there is no way for attackers to get our information. And with the help of operating system and plenty of security software, the environment is more secure.

So in one word, IoT system lives in a more dangerous environment with limited resources and less network guards. So we need to implement lightweight solutions to deal with this more dangerous environment.

b) *Internet of Things Layers*

In order to analyze the security issues of IoT in more detail, IoT layers are divided into perception layer, transportation layer and application layer. Perception layer can further be divided into perception nodes and perception network, divide transportation layer into access network, core network, and LAN, and the application layer into application support layer and IoT applications.

Each layer has a corresponding technical support, these technologies at all levels play irreplaceable roles, but these techniques are more or less related to the existence of the range problems that can cause insecurity, privacy and other security issues of data. IoT must ensure the security of all layers. In addition, IoT security should also include the security of whole system crossing the perception layer, transportation layer and application layer.

- Perception layer includes RFID security, WSNs security, RSN security and any others.
- Transportation layer includes access network security, core network security and local network security. There are 3G access network security, Ad-Hoc network security, WiFi security and so on for these sub layers. Different network transmission has different technology.
- Application layer includes application support layer and specific IoT applications. The security in support layer includes middleware technology security, cloud computing platform security and so on. IoT applications in different industries have different requirements.

Perception layer is mainly about information collection, object perception and object control. Perception Network that communicates with transportation network. Perception node is used for data acquisition and data control, perception network sends collected data to the gateway or sends control instruction to the controller. Perception layer technologies include RFID, WSNs, RSN, GPS, etc.

c) *LOT Security and Privacy Requirements*

Security and privacy are crucial enabling technologies and thus among the biggest challenges for the IoT [31]. Therefore, it is compelling for the IoT architectures to consider and resolve these challenges upfront. Otherwise, applications as well as whole ecosystems building on top of such architectures may repeat the security fallacies of the past decades. For that, a precise understanding of security requirements in the context of the IoT is indispensable.

Prior technology trends, e.g., cloud computing and big data, are likely to share security requirements with the IoT. However, the uniqueness of the IoT introduces new challenges to security requirements, different from previous technology trends. Big data solutions for instance are designed to scale and deal with heterogeneity of data sources. Nevertheless, big data solutions are not required to deal with an uncontrolled environment and constrained resources; big data analytics run in isolated silos with time or resources to spare. Likewise, cloud computing by design is supposed to scale and overcome challenges of constrained resources. However, cloud computing hardly deals with mobility of devices and physical accessibility of sensors. Related IoT security surveys are incomplete with respect to requirements. To provide a comprehensive overview, we summarize these security requirements from the domain of the IoT and split them into five groups: Network Security, Identity Management, Privacy, Trust, and Resilience. It is obvious that with regard to network security the constrained resources should have the strongest connection, mainly due to the restrictions that they apply to traditional security mechanisms, e.g., cryptography. Moreover, identity management is influenced by the heterogeneity of the IoT. Privacy is mostly connected with scalability and the constrained resources as restrictions are posed to the technology candidates that can be utilized. Furthermore, the uncontrolled environment and the heterogeneity of the IoT have a serious impact on trust. Lastly, resilience is directly connected to the need of the IoT for scalability [23].

Network Security: Network security requirements are divided into confidentiality, authenticity, integrity, and availability [34]. Factors like heterogeneity and constrained resources must be considered while applying these to IoT architectures. Interconnecting the devices require to have better confidentiality so technologies such as IPSec [35] and Transport Layer Security (TLS) [33] are employed to meet this requirement. There's another dedicated secure network stacks of IoT available in case overhead exceeds the resource constraints of things [32]. Authenticity confirms that the connection established is with an authenticated entity and authenticity also includes integrity of data but can be required separately to detect and recover failures so mechanisms such as TCP and TLS suffice this requirement.

Privacy: Privacy is considered to be one of main challenges in IoT [24] due to the involvement of humans and increasingly ubiquitous data collection. Privacy of data includes confidential data transmission in a way that it shouldn't expose undesired properties, e.g. identity of a person. This requirement is considered as big challenge as almost every other sensing device collect personal information and large amount of such data becomes Personally Identifiable Information (PII) when combined together; enough to identify a person [38].

A single person not being identifiable as the source of data or an action is anonymity, another challenge to face in IoT as mobile devices and wearable sensors may leak PII such as IP addresses and location unknowingly. There are some technologies already being employed such as anonymous credentials and onion routing, though may not scale well with IoT. Unlinkability protects from profiling in the IoT while pseudonyms may solve unlink ability. With pseudonymity, actions of a person are linked with a pseudonym, a random identifier, rather than an identity [23].

Intel Security also announced, its Enhanced Privacy Identity (EPID) technology will be promoted to other silicon vendors. EPID has anonymity properties, in addition to hardware-enforced integrity, and is included in ISO and TCG standards. The EPID technology provides an on-ramp for other devices to securely connect to the Intel IoT Platform [1].

Identity Management: A comprehensive attention should be given for identity management in IoT due to the number of devices and the complex relationship between devices, services, owners and users [38]. Methods for authentication, authorization including revocation, and accountability or non-repudiation are required. There may be multiple domain scenarios in IoT, authorization solutions, e.g., Kerberos [13], assume a single domain that encloses devices, owners, users, and services. Therefore, new authorization solutions that work with un-trusted devices, allow delegation of access across domains, and capable of quick revocation are needed. Accountability in trust management ensures that every action is clearly bound to an authenticated entity, is another challenge in IoT. It must be capable to deal with huge amounts of entities, delegation of access, actions that span organizational domains along with continuous derivation of data.

Resilience: Resilience and robustness against attacks and failures becomes another important challenge due to large scale of devices. IoT architectures must provide mechanisms to proficiently select things, transmission paths, and services according to their robustness (failure/attack avoidance). Also, fail-over and recovery mechanisms must be provided to maintain operations under failure or attacks, and to return to normal operations [2].

d) Cryptographic Primitives Goals and Attack Techniques

Cryptographic primitives are in general utilized to comply with the main security goals for exchanged messages and the system itself [3].

Main security requirements are

Confidentiality: message only disclosed to authorized entities

Integrity: Original message is not tempered
Authenticity: message is sent from a genuine entity
Availability: system keeps serving its purpose and stays uninterruptedly available for legitimate entities
It is also important to understand the attack techniques in order to rationalize security mechanisms in communication protocols. Some important attacks with respect to IoT are: *Eavesdropping:* process of

overhearing an ongoing communication, i.e. is as well preliminary for launching next attacks. In wireless communication, everyone has in general access to the medium so takes less effort to launch as compared to wired communication. Confidentiality is a typical counter-measurement against eavesdropping but if keying material is not exchanged in secure manner, eavesdropper could compromise the confidentiality. Secure key exchange algorithms such as Diffe-Hellman (DH) are used.

Impersonation: a malicious party pretends to be a legitimate entity for instance by replaying a generic message, in order to bypass the aforementioned security goals.

MITM Attack: Man-in-the-middle attack takes place when a malicious entity is on the network path of two genuine entities. Capable of delaying, modifying or dropping messages. Interesting within the context of PKC, malicious entity doesn't attempt to break the keys of involved parties but rather to become the falsely trusted MITM.

DoS Attack: targets the availability of a system that offers services, is achieved by exhaustingly consuming resources at the victim so that the offered services become unavailable to legitimate entities. A common way to launch this attack is to trigger expensive operations at the victim that consume resources such as computational power, memory bandwidth or energy. This attack is critical for constrained devices where existing resources are already scarce.

III. Internet of Things Security Solutions Approaches

Different approaches are being employed for secure End-to-End communication in WSNs and IoT, they can be classified into major research directions as follows

- Centralized Approaches
- Protocol-based Extensions and Optimizations
- Alternative Delegation Architectures
- Solutions that Require Special Purpose Hardware Modules

a) *Centralized Approaches*

Centralized security solution approaches are considered as efficient and suitable for the resource-constrained sensor networks but the common issue is the scalability of the key management; node must be pre-configured with shared keys of all entities before deployment. Some of the common centralized based approaches are SPINS (A centralized architecture for securing uni- and multicast communication in constrained networks, composed of two security protocols; SNEP and μTESLA) and the Polynomial-based scheme (Polynomial schemes aim at simplifying the key agreement process in distributed sensor networks, main idea is to assign every node n a polynomial share F(n; y) derived from a secret symmetric bi-variate polynomial F(x; y). This allows any possible pair of nodes with a polynomial share to be able to establish a common secret) [3].

b) *Protocol-based Extensions and Optimizations*

Approaches such as compression aim at optimizing the protocol without breaking the security properties. There are several compression schemes proposed such as the compression of IPV6 header, extension headers, and UDP (User Datagram Protocol) header now standard in 6LoWPAN. Some of these approaches are Abbreviated DTLS Handshake (allows for a shorter handshake that reuses the state information from the previous session, in order to resume the session). TLS Session Resumption without Server-Side State where server does not hold any state required to resume a session rather server's encrypted state is offloaded during the handshake towards the client and in caching, TLS Cached Information extension allows for omitting cached information, such as these large certificate chains from the handshake. Compression of header information is an approach to reduce the transmission overhead of packets in constrained environments, 6LoWPAN defines already header compression mechanism for IP packets.

c) *Delegation-based Architectures*

Delegate computationally intensive tasks, such as public-key-based operations involved in session establishments, to more powerful devices. Some important approaches are:

Server-based Certificate Validation Protocol (SCVP), it enables a client to delegate the complex task of certificate validation or certificate path construction to a trusted server. SCVP server should be trusted.

Another delegation approach: by Bonetto [4]. It delegates the public-key-based operations to a more powerful device, such as the Gateway (GW). They describe the procedure for IKE session establishment, where the GW intercepts session establishment and pretends to be the end-point. After calculation of the session key, this key is handed over the constrained device and both peers can directly protect their communication with the session key. But in the vision of IoT, not always a trusted GW is present e.g. in the home automation scenario, constrained devices of different manufacturers might be present in the constrained network.

Tiny 3-TLS [6]: It requires a strong trust level between the constrained resource device and the GW, offloads expensive public-key-based operations to the GW. The constrained resource device trusts the GW and the unconstrained device authenticates itself to the GW and hence, GW trusts the unconstrained device.

constrained resource device trusts the GW and the unconstrained device authenticates itself to the GW and hence, GW trusts the unconstrained device.

Consequently, Tiny 3-TLS assumes that by means of transitive trust the constrained device could trust the unconstrained device. Tiny 3-TLS distinguishes between partially and fully trusted GWs.

Sizzle [7] implements a complete SSL-secured HTTP web server for constrained devices with support for ECC-based authentication. This approach, in contrast to previous delegation-based architectures, delegates only the task of adapting the underlying transport-layer protocol. This is achieved by terminating the incoming TCP connection at the GW and sending the payload via a UDP-based reliable protocol to the constrained device. Sizzle only allows for certificate-based authentication towards powerful clients and does not implement certificate handling for constrained devices.

Peer authentication and End-to-End data protection are crucial requirements to prevent eavesdropping on sensitive data or malicious triggering of harmful actuating tasks in the context of Internet of Things (IoT). Symmetric key cryptography such as AES provides fast and lightweight encryption and decryption on smart devices and their integrated hardware supports it as well. However, when number of devices connected becomes high, exchanging symmetric keys becomes a challenging task and an efficient scalable key establishment protocol is required. Asymmetric key cryptography is another method for key establishment at two ends, but it involves high computational overheads which are the main concerns for resource-constrained devices [9]. Sensors with low resources (energy, computation) are not meant to perform complex asymmetric cryptographic operations.

Key establishment protocols are used to provide shared secrets between two or more parties, typically for subsequent use as private keys for a variety of cryptographic objectives [12]. These objectives are in turn used as security primitives for enabling various security protocols such as source authentication, integrity protection or confidentiality [8]. To afford interoperable network security between endpoints from independent network domains, variants of traditional End-to-End IP security protocols have recently been proposed for resource-constrained devices and the networks formed by them [9].

- Protocol variants such as Datagram Transport Layer Security (DTLS) [14], HIP-DEX [15], and minimal IKEv2 [16] consider public-key cryptography in their protocol design. As public-key cryptography acquires significant computational processing and transmission overheads in resource-constrained network environments, research and standardization currently focuses to reduce the public-key related overheads during the protocol handshake.
- Another interesting approach has been suggested in [20] and [8]. In these papers, a proxy-based solution is proposed to delegate the heavy cryptographic operations from a resource-constrained device to less constrained nodes. A similar approach might be found in [11] for ambient-assisted living and also in [21] where communication is made from one resource-constrained node to another resource-constrained sensor node. These approaches have assumed the sensor nodes to be trustworthy and the mechanism in case if nodes are compromised, misbehave, authentication fails or nodes fail to deliver its assigned share. Still the risk involved is there for the secret shared key to be revealed by the attacker from the compromised nodes. Selection criteria are described for these assisting nodes to evaluate their abilities before they are assigned computational tasks to work as proxies.

Other approaches proposed including session resumption mechanisms [17] and caching of static handshake information such as certificates [18]. However, the considerable RAM and ROM requirements make the use of public-key cryptography unsuitable for a wide range of constrained devices [9]. One such implementation of two-way authentication scheme for the IoT based on DTLS protocol is described in [19]. This approach even generates considerable overheads to the network traffic due to the utilization of X.509 certificates and RSA public keys with DTLS handshake. Both these X.509 certificate and RSA public key with DTLS handshake involve heavy computations for the low performing and high resource-constrained sensor nodes.

d) Hardware-based Approaches

A class of security solutions relies on additional hardware security modules, such as TPMs. A Trusted Platform Module (TPM) is tamper-proof hardware that provides support for cryptographic computations especially public-key-based cryptographic primitives. TPMs can hold keys, such as RSA private keys, in a protected memory area. Furthermore, the cryptographic accelerator of TPMs is capable of

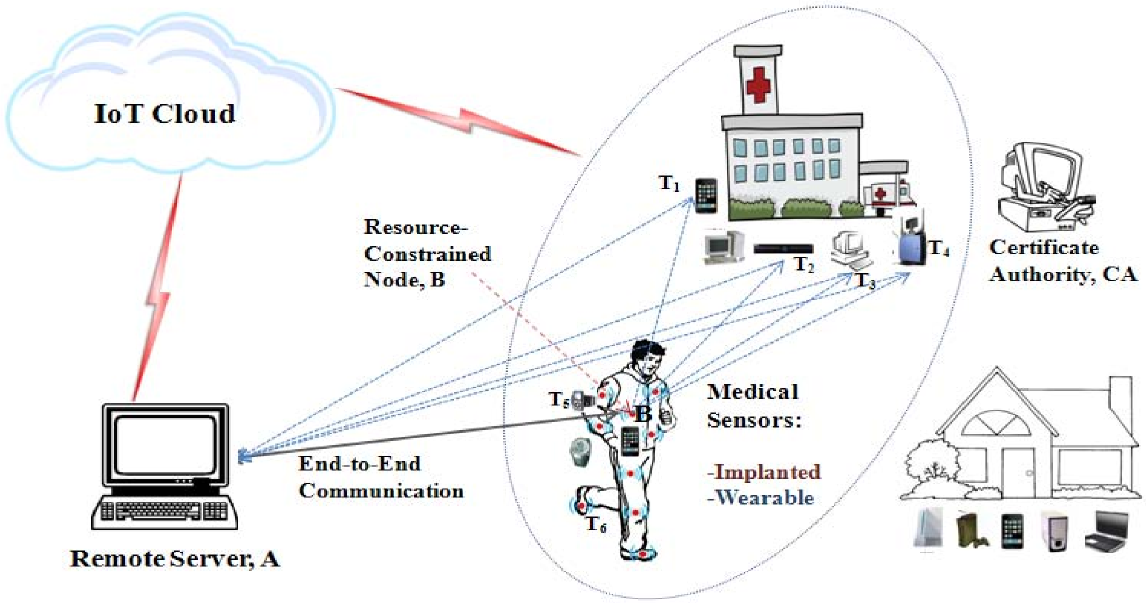

Figure 2: Network Model Scenario for Body Area Network in the context of Internet of Things (IoT)

computing the cryptographic computations with a higher performance. In contrast, ECC provides the same level of security with considerably smaller key sizes [3]. Therefore, ECC is preferred and recommend for constrained environments.

IV. Conclusion

This paper aims to provides the reader a basic overview about Internet of Things, the major security and privacy challenges because of its exponential growth and what kind of security primitives and solution approaches are being taken to make communication secure and to protect the user's data. Conventional security primitives cannot be applied due to the heterogeneous nature of sensors, low resources and the system architecture in IoT applications. To prevent unauthorized use of user's data, protect their privacy and to mitigate security and privacy threats, strong network security infrastructures are required. Peer authentication and End-to-End data protection are crucial requirements to prevent eavesdropping on sensitive data or malicious triggering of harmful actuating tasks. Any unauthorized use of data may restrict users to utilize IoT based applications. This review paper provides the security solution approaches been proposed recently identifying both the challenges related to security and privacy and the attack techniques used to compromise/fail the sensor nodes in Internet of Things as well. Current approaches are focused on pre-deployed, pre-shared keys on both ends whereas certificate-based authentication is generally considered infeasible for constrained resource sensors. New security paradigm are needed for End-to-End secure key establishment protocols that are lightweight for resource-constrained sensors and secure through strong encryption and authentication.

References Références Referencias

1. Somayya Madakam, R. Ramaswamy, Siddharth Tripathi "Internet of Things (IoT): A Literature Review"
2. Emmanouil Vasilomanolakis, Jorg Daubert, Manisha Luthra, Vangelis Gazis, Alex Wiesmaie and Panayotis Kikiras "On the Security and Privacy of Internet of Things Architectures and Systems"
3. Hossein Shafagh (2013) "Leveraging Public-key-based Authentication for the Internet of Things" Master Thesis, RWTH Aachen University, Germany
4. R. Bonetto, N. Bui, V. Lakkundi, A. Olivereau, A. Serbanati, M. Rossi. "Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples". In IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'12), San Francisco, CA (June 2012), pp. 1–7. http://dx.doi. org /10.1109/WoWMoM.2012.6263790
5. Christian Dancke Tuen "Security in Internet of Things Systems" Master Thesis Norwegian University of Science and Technology.
6. Sepideh Fouladgar, Bastien Mainaud, Khaled Masmoudi, Hossam Afifi. "Tiny 3- TLS: a trust delegation protocol for wireless sensor networks". In Proceedings of the Third European conference on Security and Privacy in Ad-Hoc and Sensor Net works (ESAS'06), Hamburg, Germany (Nov 2006), pp. 32–42. http://dx. doi.org/10.1007/11964254_5
7. Vipul Gupta, Michael Wurm, Yu Zhu, Matthew Millard, Stephen Fung, Nils Gura, Hans Eberle, Sheueling Chang Shantz. (2005) "Sizzle: A standards-based end-to-end security architecture for the

embedded Internet. In Pervasive and Mobile Computing".

8. Y. B. Saied, A. Olivereau, D. Zeghlache, and M. Laurent, (2014) "Lightweight collaborative key establishment scheme for the Internet of Things" Computer Networks, vol. 64, pp. 273 – 295.
9. R. Hummen, H. Shafagh, S. Raza, T. Voigt, and K. Wehrle, (2014) "Delegation based Authentication and Authorization for the IP-based Internet of Things," in IEEE SECON.
10. Ashton, K. "That 'Internet of Things' thing". Available online: http://www.rfidjournal.com/ (accessed on 22 June 2009).
11. Muhammad A Iqbal, Magdy Bayoumi (2016) "Secure End-to-End Key Establishment Protocol for Resource-Constrained Healthcare Sensors in the Context of IoT" The 14th Annual IEEE International Conference on High Performance Computing and Simulations (HPCS) 2016, Innsbruck Austria.
12. A. J. Menezes, S. A. Vanstone , P. C. Van Oorschot, "Handbook of Applied Cryptography", CRC Press, Inc., Boca Raton, FL, 1996.
13. Jennifer G. Steiner, B. Clifford Neuman, and Jeffrey I. Schiller. Kerberos: An authentication service for open network systems. In Proceedings of the USENIX Winter Conference. Dallas, Texas, USA, January 1988, pages 191–202. USENIX Association, 1988
14. E. Rescorla and N. Modadugu, (2012) "Datagram Transport Layer Security Version 1.2," RFC 6347, IETF.
15. R. Moskowitz and R. Hummen, (2012) "HIP Diet EXchange (DEX)," draftmoskowitz-hip-dex-01 (WiP), IETF.
16. T. Kivinen, (2012) "Minimal IKEv2," draft-kivinen-ipsecme-ikev2-minimal-01 (WiP), IETF.
17. R. Hummen, H. Wirtz, J. H. Ziegeldorf, J. Hiller, and K. Wehrle, (2013) "Tailoring End-to-End IP Security Protocols to the Internet of Things," in Proc. of IEEE ICNP.
18. S. Santesson and H. Tschofenig, (2014) "Transport Layer Security (TLS) Cached Information Extension," draft-ietf-tls-cached-info-16 (WiP), IETF·
19. T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, (2013) "DTLS based security and two-way authentication for the Internet of Things," Ad Hoc Networks, vol. 11, no. 8, pp. 2710–2723.
20. Y. Saied and A. Olivereau, (2012) "D-HIP: A distributed key exchange scheme for HIP-based Internet of Things," in Proceeding of IEEE World of Wireless, Mobile and Multimedia Networks (WoWMoM) 2012, pp.1–7.
21. P. Porambage, A Braeken, A Gurtov, M Ylianttila and Susanna Spinsante "Secure end-to-end communication for constrained devices in IoT-enabled Ambient Assisted Living systems" in proceedings of 2nd World Forum on Internet of Things (WF-IoT), 2015.
22. "Internet of Things: An overview" by Internet Society https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf.
23. Emmanouil Vasilomanolakis, Jorg Daubert, Manisha Luthra, Vangelis Gazis, Alex Wiesmaier and Panayotis Kikiras "On the Security and Privacy of Internet of Things Architectures and Systems".
24. Joerg Daubert, Alexander Wiesmaier, and Panayotis Kikiras. 2015 A view on privacy & trust in iot. In IOT/CPS-Security Workshop, IEEE International Conference on Communications, ICC 2015, London, GB, June 08-12, 2015, page to appear. IEEE.
25. Sundmaeker, H.; Guillemin, P.; Friess, P.; Woelfflé, S. Vision and Challenges for Realising the Internet of Things; European Commission—Information Society and Media: Brussels, Belgium, 2010.
26. Bruce Ndibanje, Hoon-Jae Lee, and Sang-Gon Lee Security Analysis and Improvements of Authentication and Access Control in the Internet of Things.
27. Benjamin Kleine, Bethany Lobo, Amanada Levendowski March 2015 Internet of Things: The new frontier for data security and privacy (Part 1).
28. Gartner's Hype Cycle Special Report for 2015, Gartner Inc.,2015. http://www.gartner.com/technology/research/ hype-cycles/
29. Ahmad W Atamli and Andrew Martin. 2014 Threat-Based Security Analysis for the Internet of Things. In Secure Internet of Things (SIoT), pages 35–43. IEEE
30. Rolf H. Weber. Jan 2010, Internet of Things – New security and privacy challenges. Computer Law & Security Review, 26(1): 23–30.
31. Mohamed Abomhara and Geir M. Koien. 2014 Security and Privacy in the Internet of Things: Current Status and Open Issues. In Privacy and Security in Mobile Systems (PRISMS), pages 1–8. IEEE.
32. Riccardo Bonetto, Nicola Bui, Vishwas Lakkundi, Alexis Olivereau, Alexandru Serbanati, and Michele Rossi. 2012 Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples. 2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2012 - Digital Proceedings.
33. T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246 (Proposed Standard), August 2008. Updated by RFCs 5746, 5878, 6176.
34. Gunter Sch ¨ afer. ¨ Security in fixed and wireless networks - an introduction to securing data communications. Wiley, 2003.
35. S. Kent and R. Atkinson. Security Architecture for the Internet Protocol. RFC 2401 (Proposed Standard), November 1998. Obsoleted by RFC 4301, updated by RFC 3168.

This page is intentionally left blank