Optimisation of the Public Key Encryption Infrastructure for the Internet of Things

Daniel Kelly, Mohammad Hammoudeh
School of Computing, Mathematics, & Digital Technology
Manchester Metropolitan University
Manchester, M1 5GD
daniel.kelly5@stu.mmu.ac.uk,M.Hammoudeh@mmu.ac.uk

ABSTRACT

The Internet of Things (IoT) faces unique security challenges due to its resource constrained devices. Limited processing, storage, memory and power of IoT objects do not support the deployment of advanced security protocols, which are often resource intensive, e.g., the use of Public Key Infrastructure (PKI) to ensures secure end-to-end communications between devices and services over the Internet. There are several approaches in the literature to improve the efficiency of communication protocols employed in PKI environments. Some researchers advocate decreasing the size of the x.509 certificates or fine tuning the DTLS handshake. Others investigated using neighbouring or virtual resources to perform the complex cryptographic algorithms on behalf of IoT constrained devices or using two factor authentication via an authorisation server to delegate authentication and authorisation. This paper surveys attempts in the literature to reduce the overhead incurred by IoT devices running complex PKI security protocols. It is evident from the literature that there is no universal solution for IoT constrained devices, instead, a selection of algorithms and frameworks is needed depending on the levels of interoperability, network scalable needs and ultimately how constrained the IoT devices are.

CCS CONCEPTS

•**Security and privacy** → **security services;** *Intrusion/anomaly detection and malware mitigation;* •**Computer systems organization** → Dependable and fault-tolerant systems and networks; •**Networks** → Network reliability;

KEYWORDS

Internet of Things, Public Key Infrastructure, IoT Threats, Computer Security, Privacy, Offloading, Key escrow

ACM Reference format:
Daniel Kelly, Mohammad Hammoudeh. 2016. Optimisation of the Public Key Encryption Infrastructure for the Internet of Things. In *Proceedings of International Conference on Future Networks and Distributed Systems, Amman, Jordan, June 26–27, 2018 (ICFNDS'18),* 5 pages.
DOI: 10.1145/3231053.3231098

ICFNDS'18, Amman, Jordan

DOI: 10.1145/3231053.3231098

1 INTRODUCTION

The Internet of Things (IoT) is a network of devices such as light bulbs, thermostats and cars that communicate with other devices and services over the Internet [7, 10, 13]. They can be heterogeneous in nature with some devices characterised by limited CPU, RAM, ROM, energy and bandwidth [17]. Other devices have less constrained access to these resources. Table **??** shows example protocols which are designed to be reliable and efficient on standard Internet connected devices and their alternatives when deployed on IoT networks.

A report by Hewlett Packard [11] has stated that 70% of IoT devices used unencrypted network services. This means that IoT devices are vulnerable to leaking sensitive data and worse [3, 22]. Gartner has reported that by 2020 there is expected to be 26 billion IoT devices [18]. This means that the potential to lose sensitive data is increasing as the use of IoT proliferates [4, 8].

The Public Key Infrastructure (PKI) and asymmetric encryption is a best practise used for securing communications between resource-rich Internet connected devices. It is commonly used in the process of exchanging session keys over an insecure medium. These keys are then used for symmetric encryption of communication making them secure. The use of PKI and asymmetric encryption pose a unique challenge for IoT devices, in that asymmetric encryption is expensive and may be too costly for resource constrained IoT devices. Other challenges faced by employing traditional PKI is the fact that IoT devices can act as both a client and a server. This would require IoT devices to store their own x.509 certificate and to have their own public and private keys. Lastly the use of IoT devices in the near future is likely to increase dramatically, which poses scaling challenges for PKI. This paper reviews the current literature on the state of PKI and potential adaptations, extensions and alternatives to address problems it faces in respect to the challenges of IoT devices.

The rest of the paper is organised as follows: Sections 2 to 4 present the various approaches taken in the literature to optimise and adapt PKI protocols to resource-limited IoT devices. Section 3 discusses the research gaps and open research questions. Section 4 concludes the paper.

2 REDUCED X.509 CERTIFICATES AND FINE TUNING OF DTLS

x.509 certificates in PKI are used to store public keys and identity. They are signed by a trusted Central Authority (CA) to validate a certificate holders identity. Alternatively the certificates can be self signed. These are commonly used in protocols such as TLS

Table 1: Protocols designed for standard Internet devices and their optimisation for IoT devices (adopted from [16])

Standard Internet Device	IoT Device
JavaScript Object Notation (JSON)	Concise Binary Object Representation (CBOR)
Hyper Text Trasnfer Protocol Secure (HTTPS)	Constrained Application Protocol (CoAP)
Tunnel Layer Security (TLS)	Datagaram Tunnel Layer Security (DTLS)
Transmission Control Protocol (TCP)	User Datagram Protocol (UDP)
Internet Protocol (IP)	IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN)

and SSL to secure communications over the Internet [2, 9, 12]. The issue for constrained IoT devices is that the certificates are too large. The use of trust chains mean that multiple certificates are needed to be stored. This is a larger issue for constrained IoT devices communicating within a network as the large footprint of x.509 keys consumes too much resource.

Schukat et al. [19] propose a change to the x.509 certificate to provide it with a smaller foot print. This makes it more piratical for constrained IoT devices to adopt and use. This is based on the v3 x.509 specification that includes extensions. In a typical IoT network containing constrained IoT devices a base station would act as a CA and be responsible for signing all of the certificates for a network. This is because IoT devices in many cases do not need to validate trust chains globally, rather they are often confined to their own network. This means that a local CA can be used to self sign all certificates with an IoT deployment or network. A Registration Authority (RA) is used to generate the public private keys for all devices ensuring strong cryptographic keys are created and used. The certificates are pre installed on devices in a network by the manufacturer and would be long lasting. This means that the certificates will not be updated or expire. This is to avoid back doors being created for attackers to gain control of constrained IoT devices. This has been shown to work in a experimental set-up. The strength of this approach is that it describes a network that can communicate securely using asymmetric and symmetric encryption, it reduces the size of the certificates and uses a local RA to ensure that strong cryptographic keys are used. Future work is needed to address updating and revoking certificates both of which are crucial to the secure working proposed IoT networks.

The use of x.509 certificates inside DTLS can course packets to fragment. This can be a problem on 802.15.4 network that can experience greater packet loss when compares to other networks. Using DTLS on these networks means that the handshake of a fragmented packet can mean that losing one packet can cause the whole handshake to be retransmitted. This results in unacceptable delays in the network for secure communication with constrained IoT devices.

Keoh et al. [14] suggests using a raw public key to reduce the impact on resource constrained IoT devices. The IoT device would be preconfigured with the raw public keys of the servers which it needs to communicate with as well as a public key for the device itself. For the public key based handshake, Elliptic Curve Cryptography (ECC) encryption is used. Further extensions of DTLS could be compressing the headers of the packet. This is reliant on the server and the device having a shared pairwise key. This will make DTLS more efficient in terms of bandwidth as a DTLS packet can be shown to fit inside an 802.15.4 packet reducing fragmentation and easing congestion associated with the DTLS handshake on a lossy network. One of the main drawbacks of this approach is the loss of the chain of trust as raw public keys are unsigned by a CA or other trust mechanism.

Using a CA in PKI introduces a single point of failure in a network [3]. To address security issues authentication, authorisation and trust management comes down to the problem of generating and managing cryptographic keys.

Shahzad et al. [20] suggest a locally centralised authentication and authorisation framework for IoT deployments and networks. This framework has an Auth entity, e.g., a base station acting as a CA. The Auth entity is an edge computing device keeping information in the network and not on the IoT devices nor in the cloud. The local authorisation process distributes session keys to IoT devices that are valid for specific access activities. The Auth framework supports multiple communication protocols such as TCP, UDP, WIFI and BLE to aid the interoperability of devices. The trust relationship between Auth entities is performed over HTTPS using Open PGP. Certificates are signed by trusted neighbours Auth entities. This means that a central PKI CA is not required to secure communications between Auth entities. Operating Open PGP between Auth entities the network makes this approach more resilient and scalable. A drawback to the OpenPGP nature of the Auth entities communicating with one another is that it is vulnerable to collusion. They are also harder to keep track and manage the systems as a whole. Finally, the individual overhead on each Auth entity is high. Future work include investigating a process to automate/semi-automate the registration process for IoT devices as well as authorisation for mobile devices.

3 OFFLOADING TO NEIGHBOURS OR VIRTUAL RESOURCES

Asymmetric cryptography protocols such as DTLS, HIP-DEX and IKEv2 are all reliant on PKI. These all have considerable RAM and ROM requirements. This is a problem for resource constrained IoT devices that would find the resource requirements of performing these expensive operations prohibitive.

Iqbal et al. [1] suggest offloading the highly resource consuming cryptographic functions from the constrained IoT devices to neighbouring nodes provided that they have enough spare capacity to perform these functions. In this protocol, neighbouring nodes are selected based on three factors: how trusted they are, the resources they have available and their past performance. The Diffe-Hellman protocol is used for the key establishment process as depicted in Figure 1.

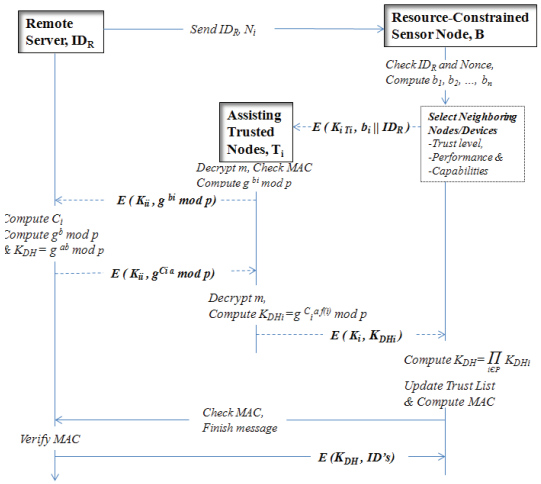

Figure 1: Message flow of key establishment (adopted from [1])

The remote server sends a request to the resources constrained IoT device. The device then selects neighbours to perform key establishment. The neighbours then communicate with the remote server and obtain secret shares. The neighbours then process the cryptography for their secret share and pass the result to the resource constrained device. The latter combines the results from the neighbours and reconstructs the secret pair wise key and has now established secure communications with the remote server. One of the strengths of this approach is that a compromised neighbour will be unable to reconstruct the pair wise secret key. This is because it will have $1/n$ of the shared secret. This protocol is scalable as it means that pair wise keys can be installed after deployment and new devices can be dynamically added to an IoT deployment or network regardless of it constraints on resources. The behaviour of neighbouring nodes is also monitored and neighbours that fail in this process are forced to re-authenticate with the remote server. This also provides information for threat detection on the network. One of the drawbacks of this approach would be that it is a new protocol that not all remote servers will implement. This results in a lower interoperability of the constrained IoT device.

Constrained IoT devices often fail to adopt best practise when securing their communications. This includes the adoption of certificate based authentication and protocols such as TLS. Effort has been made to make the protocols less costly in terms of processing and energy requirements, however, the adoption of these protocols is still low.

ElAffendi et al. [6] suggests a protocol in which virtual resources are created to manage resource constrained IoT devices. This will enable these device to use standard protocols to communicate over the Internet. When a physical constrained IoT device needs to be added to a network a gateway will create a virtual resource under the control of the co-ordinator. Each virtual resource has its own ECC based x.509 certificate for secure communication. Virtual resources collect and aggregate data as well as receive all requests and responding on behalf of all associated devices. This solution logically separates the IoT network into two parts. The first is the upper back bone, which contains the gateway, co-ordinator, routers and non constrained IoT devices. The second contains virtual resources associated with the constrained IoT devices. The main drawback of this approach is the possibility of the gateway device being compromised. This would then compromise all the attached constrained IoT devices connected through the virtual resources.

4 KEY MANAGEMENT AND TWO FACTOR AUTHENTICATION

Communication between IoT devices and Internet devices need to be authenticated [5, 15, 15]. Applications relating to IoT devices are also very different and implement different security standards and protocols. As such, they face very different security vulnerabilities. Some of the more widely used IoT protocols do not have security built in. These include MQTT and CoAP. Although CoAP and other protocols can make use of DTLS, SSL and TLS to improve their security. This means that IoT devices with single factor authentication is not sufficient for secure communication.

Shivraj et al. [21] suggests that two factor authentication would mitigate this risk and increase the security in an IoT network. They propose that a remote server would request a one time password from a trusted third party that is part of the IoT network. A one time password is the provided to both the remote server and the IoT device. This will then allow the IoT device to authenticate the request from the remote server. The one time password is based on Identity Based Elliptic Curve Cryptography (IBE-ECC). As it is identity based there is no key for the IoT device to store. This requires less resource compared to other protocols such as HOTP and TOTP. There is a smaller key and less infrastructure for this protocol and the security is the same as other protocols, which make it an ideal candidate for resource constrained IoT devices.

Any solution relying on certificates, signatures and Difffe-Hellman like key agreement use too much computational resources. This makes use of these protocols impractical for resource constrained IoT devices. Hence, a more efficient protocol is needed for the key establishment between these devices.

Navas et al. [16] proposes a new protocol that relies on extending OAuth 2.0 proof of possession to run Berson and Feiertag for Authenticated Key Establishment (BBF AKE). In this scenario, there is a client wishing to access a resource, a trusted third party or authorisation server that has a symmetric key with a resource server or a constrained IoT device. They communicate as shown in Figure 2.

A client requests a resource from a resource server. The resource server responds with its ID and a nonce. The client then forwards this with its ID and nonce to the authorisation server The authorisation server replies with an encrypted message containing a key for the client, its nonce and the ID for the resource server. The key is to encrypt messages to the resource server. Only the client can decrypt this message. It also sends an encrypted message containing the key for the resource server to communicate with the client securely, its nonce and the client ID. Only the resource server can decrypt this message. The client forwards the encrypted message for the resource server to the resource server. The client

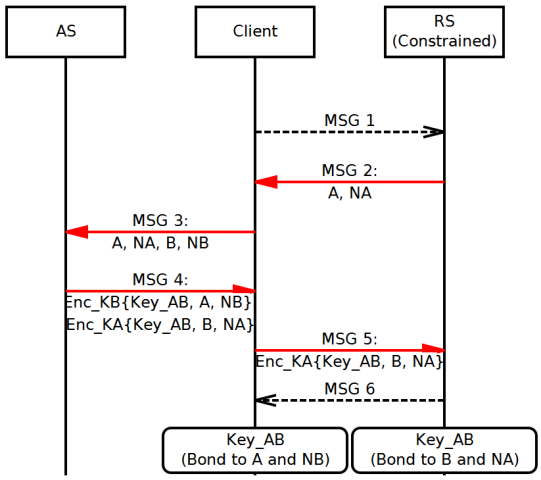

Figure 2: BBF AKE protocol with OAuth (adopted from [1])

and the resource server now share a key and can efficiently communicate via symmetric encryption. This means the resource server or constrained IoT device has a way of establishing a key with a client through a authorisation server that does not involve costly asymmetric encryption. It also has the added advantage of two factor authentication as the client and the constrained device can not communicate without the authorisation server. Potential drawbacks include the authorisation server will be a single point of dependency for all attached IoT devices. This is a new protocol and as such would mean interoperability with existing devices would decrease.

5 GAPS AND OPPORTUNITIES

This brief analysis of some recent literature identified some gaps in terms of the PKI and trust chains. Currently, they CAs act as single points of failure and distributing them as suggested in [20] in a Open PGP manner would make the PKI more scalable and resilient. It would however open CA's to collusion attacks and other vulnerabilities.

Another important gap is concerning the use of encryption keys for IoT devices that in the future will be susceptible to quantum attacks. This is not a problem for the immediate future and is reliant on quantum computer becoming powerful and distributed enough that they become a threat to modern day PKI and asymmetric encryption. This would apply to algorithms such as ECC and RSA. NTRU being resistant to quantum attack could be a potential solution to this problem. It is worth noting that the research reviewed has a large focuses on ECC for secure communication for constrained IoT devices for efficiency reasons.

Table 2 comments on the usage of CPU, ROM and RAM of a constrained IoT device. Scalable is determined by if a new device can easily be added to the network. If a pair wise key needs to be installed specifically during manufacturing then the network is said not to be scalable. Interoperability is the ability of IoT devices running the proposed protocols and or frameworks to communicate with other heterogeneous IoT devices or services.

As can be seen from Table 2 solutions in the literature have an aim to reduce the amount of resources needed for IoT devices to communicate with one another and with other internet entities. ElAffendi et al. [6] is of interest as it delegates the work of securing communication onto a gateway device that is not constrained in terms of resources. This may be ideal for a smart home IoT deployment. This has a number of problems, one of which is what happens if the gateway device is compromised. Ultimately it would be the risk of the gateway device being compromised to the risk of the IoT device being compromised and which would have the greatest reduction of the attack surface of the network. Another problem is in terms of how it could be applied to widely distributed wireless sensor network that could only be contacted remotely. These devices could be physically compromised and without tampering detection could cause security issues. The key strength however is that it does not rely on new protocols and can wrap modern security protocols around resource constrained devices.

Iqbal et al. 2016 [1] delegates encryption to neighbouring nodes, this may be ideal in the situation for IoT devices that may be implanted in patients that are hard to access and must remain secure. Interoperability may be less important in these cases as the pacemaker would likely only need to interact with specific devices. Also of interest would be the incorporation of the new protocols and frameworks and zero trust networks. This is where a network is separated into trusted and untrusted zones. In an IoT deployment or network the devices may be separated into a untrusted network protecting over critical systems and or service in the network from potentially compromised from IoT devices. This has not been discussed in this survey however would be an area of interest in the future.

6 CONCLUSIONS

This survey has found various protocols that attempt to reduce the overhead faced by IoT devices in general and in some cases constrained IoT devices specifically. The protocols suggested would make more efficient use of standard Internet protocols and allow for IoT devices to communicate more securely and more reliably. This can be seen by the use of offloading encryption to either neighbouring devices or to virtual resources, or in the reduction in x.509 certificate in a network or the more efficient use of DTLS to make frames fit into a 802.15.4 packet to avoid fragmentation of encryption handshakes. The introduction of two factor authentication with one time passwords or slightly more adapted to establish symmetric key encryption both provide a solution for securing what is currently a fragmented implementation of security standards that are leaving current IoT devices vulnerable to attacks. Given time IoT constrained devices may have access to greater resources allowing them to run more reliable and secure protocols for communication that no longer need to be adapted for efficiency. Overall it is clear that there is no protocol that can be universally adopted that will fit all IoT devices and deployments use cases. Rather a selection of an appropriate protocol is needed depending on the requirements of the IoT device and network. this will be until either resources for constrained IoT devices permits the adoption of better performing and/or more secure protocols or a new protocol is discovered that is much more efficient than those currently available.

Table 2: Comparison of standard CoAP, DTLS on 6LoWPAN and proposed new protocols

Approach	Resources Increased	Interoperability Increased	Scalable
Schukat et al. 2015 [19]	no	no	no
Keoh et al. 2014 [14]	no	no	yes
Iqbal et al. 2016 [1]	no	no	yes
ElAffendi et al. 2017 [6]	no	yes	yes
Shahzad 2017 et al. [20]	no	no	yes
Shivraj et al. 2015 [21]	-	no	yes
Navas et al. 2017 [16]	no	no	yes
Shahzad 2017 et al [20]	n/a	n/a	n/a

REFERENCES

[1] Muhammad A. and Magdy Bayoumi. 2016. Secure End-to-End key establishment protocol for resource-constrained healthcare sensors in the context of IoT. *2016 International Conference on High Performance Computing and Simulation, HPCS 2016* (2016), 523–530. https://doi.org/10.1109/HPCSim.2016.7568379

[2] K. Anoh, C. Tanriover, B. Adebisi, and M. Hammoudeh. 2018. A New Approach to Iterative Clipping and Filtering PAPR Reduction Scheme for OFDM Systems. *IEEE Access* 6 (2018), 17533–17544. https://doi.org/10.1109/ACCESS.2017.2751620

[3] Sana Belguith, Nesrine Kaaniche, Maryline Laurent, Abderrazak Jemai, and Rabah Attia. 2017. Constant-size threshold attribute based signcryption for cloud applications. In *SECRYPT 2017: 14th International Conference on Security and Cryptography*, Vol. 6. Scitepress, 212–225.

[4] Sana Belguith, Nesrine Kaaniche, Maryline Laurent, Abderrazak Jemai, and Rabah Attia. 2018. PHOABE: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted IoT. *Computer Networks* 133 (2018), 141 – 156. https://doi.org/10.1016/j.comnet.2018.01.036

[5] Andrew Carlin, Mohammad Hammoudeh, and Omar Aldabbas. 2015. Intrusion detection and countermeasure of virtual cloud systems-state of the art and current challenges. *International Journal of Advanced Computer Science and Applications* 6, 6 (2015).

[6] M A ElAffendi and A Lateef Alamudy. 2017. Could Virtualization be the Ultimate Solution for IoT Resource Constrained Devices Problem? A Multilevel Security Framework Based on Device Virtualization. In *2017 International Conference on Computer and Applications (ICCA)*. IEEE, 232–237. https://doi.org/10.1109/COMAPP.2017.8079750

[7] Muhammad Farhan, Sohail Jabbar, Muhammad Aslam, Mohammad Hammoudeh, Mudassar Ahmad, Shehzad Khalid, Murad Khan, and Kijun Han. 2018. IoT-based students interaction framework using attention-scoring assessment in eLearning. *Future Generation Computer Systems* 79 (2018), 909 – 919. https://doi.org/10.1016/j.future.2017.09.037

[8] Mohammad Hammoudeh. 2008. Modelling Clustering of Sensor Networks with Synchronised Hyperedge Replacement. In *Graph Transformations*, Hartmut Ehrig, Reiko Heckel, Grzegorz Rozenberg, and Gabriele Taentzer (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 490–492.

[9] M. Hammoudeh, S. Mount, O. Aldabbas, and M. Stanton. 2010. Clinic: A Service Oriented Approach for Fault Tolerance in Wireless Sensor Networks. In *2010 Fourth International Conference on Sensor Technologies and Applications*. 625–631. https://doi.org/10.1109/SENSORCOMM.2010.98

[10] Mohammad Hammoudeh, Robert Newman, Sarah Mount, and Christopher Dennett. 2009. A Combined Inductive and Deductive Sense Data Extraction and Visualisation Service. In *Proceedings of the 2009 International Conference on Pervasive Services (ICPS '09)*. ACM, New York, NY, USA, 159–168. https://doi.org/10.1145/1568199.1568228

[11] HPE. 2015. Internet of Things Research Study. (2015). http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf

[12] Olamide Jogunola, Augustine Ikpehai, Kelvin Anoh, Bamidele Adebisi, Mohammad Hammoudeh, Haris Gacanin, and Georgina Harris. 2018. Comparative Analysis of P2P Architectures for Energy Trading and Sharing. *Energies* 11, 1 (2018).

[13] Olamide Jogunola, Augustine Ikpehai, Kelvin Anoh, Bamidele Adebisi, Mohammad Hammoudeh, Sung-Yong Son, and Georgina Harris. 2017. State-Of-The-Art and Prospects for Peer-To-Peer Transaction-Based Energy System. *Energies* 10, 12 (2017).

[14] Sye Loong Keoh, Sandeep S. Kumar, and Hannes Tschofenig. 2014. Securing the internet of things: A standardization perspective. *IEEE Internet of Things Journal* 1, 3 (2014), 265–275. https://doi.org/10.1109/JIOT.2014.2323395

[15] J. K. Mohsin, Liangxiu Han, Mohammad Hammoudeh, and Rob Hegarty. 2017. Two Factor Vs Multi-factor, an Authentication Battle in Mobile Cloud Computing Environments. In *Proceedings of the International Conference on Future Networks and Distributed Systems (ICFNDS '17)*. ACM, New York, NY, USA, Article 39, 10 pages. https://doi.org/10.1145/3102304.3102343

[16] Renzo E. Navas, Manuel Lagos, Laurent Toutain, and Kumaran Vijayasankar. 2017. Nonce-based authenticated key establishment over OAuth 2.0 IoT proof-of-possession architecture. *2016 IEEE 3rd World Forum on Internet of Things, WF-IoT 2016* (2017), 317–322. https://doi.org/10.1109/WF-IoT.2016.7845424

[17] R. Newman and M. Hammoudeh. 2008. Pennies from Heaven: A Retrospective on the Use of Wireless Sensor Networks for Planetary Exploration. In *2008 NASA/ESA Conference on Adaptive Hardware and Systems*. 263–270. https://doi.org/10.1109/AHS.2008.46

[18] Rob Rivera, Janessa, van der Meulen. 2013. Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020. (2013). https://www.gartner.com/newsroom/id/2636073

[19] Michael Schukat and Pablo Cortijo. 2015. Public key infrastructures and digital certificates for the Internet of things. *2015 26th Irish Signals and Systems Conference, ISSC 2015* ii (2015). https://doi.org/10.1109/ISSC.2015.7163785

[20] Muhammad Shahzad, Munindar P Singh, and North Carolina. 2017. Authentication and Authorization for the Internet of Things. *IEEE Internet Computing* 21, 2 (2017), 86–90. https://doi.org/10.1109/MIC.2017.33

[21] V L Shivraj, M A Rajan, Meena Singh, and P Balamuralidhar. 2015. One time password authentication scheme based on elliptic curves for Internet of Things (IoT). *National Symposium on Information Technology: Towards New Smart World* c (2015), 1–6. https://doi.org/10.1109/NSITNSW.2015.7176384

[22] S. Walker-Roberts, M. Hammoudeh, and A. Dehghantanha. 2018. A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure. *IEEE Access* (2018), 1–1. https://doi.org/10.1109/ACCESS.2018.2817560