Implementation of Distributed Light weight trust infrastructure for automatic validation of faults in an IOT sensor network

Isaac Henderson Johnson Jeyakumar[1], Sven Wagner[2] and Heiko Roßnagel[3]

Abstract: The goal of the paper is to design and implement a distributed trust infrastructure, which makes use of the existing Internet Domain Name System (DNS) and its global trust anchor. Since it has high scalability and eases the burden on relying parties in turn, allows for highly efficient queries to support individual trust decisions. In this implementation, a stand-alone private DNS infrastructure including top level domains was developed with Raspberry Pi Cluster. Further, the security of the DNS for the trust infrastructure is enhanced by implementing DNSSEC and DANE protocol with TLSA resource records. It also includes the core functionality of the LIGHTest infrastructure like developing trust lists, Trust Scheme Publication Authority (TSPA) and a Delegation Publisher (DP). In this paper, a distributed trust infrastructure is developed and visualized practically by designing an infrastructure for validation and authentication of faults in the sensor system of an organization using a Raspberry Pi Cluster.

Keywords: Distributed trust infrastructure, DNS, DNSSEC, Raspberry Pi Cluster, Trust Scheme Publication Authority.

1 Introduction

Globally, every second enormous amount of transactions are conducted virtually over the Internet, in which decision on verifying who is on the other end of the transaction is important. Therefore, it is necessary to have assistance from trust infrastructure authorities to certify the trustworthiness of electronic identities, which is already implemented by many security algorithm and certificate authorities. But querying the trust infrastructure authorities in a secured manner without disturbing the end to end trust is a challenging task leading the verifiers to deal with high number of formats and protocols. To address this problem, the EU-funded LIGHTest project (https://lightest.eu/) attempts to build a global distributed trust infrastructure [BL16], which provides a solution that allows distinguishing legitimate identities from scoundrel

[1] University of Stuttgart, Masters in INFOTECH, 70569, Stuttgart. jisaachenderson@gmail.com

[2] University of Stuttgart, Institute of Human Factors and Technology Management, Allmandring 35, 70569 Stuttgart, {firstname.name}@iat.uni-stuttgart.de

[3] Fraunhofer IAO, Fraunhofer Institute of Industrial Engineering IAO, Nobelstr. 12, 70569 Stuttgart, {firstname.name}@iao.fraunhofer.de

ones. This efficient trust infrastructure finds its application ranging from verification of electronic signatures, over e-Procurement, e-Justice, e-Health, and law enforcement, up to the verification of trust in sensors and devices in the Internet of Things (IOT). In the paper, the importance of security in the IOT network and drawbacks of the current security infrastructures is analyzed in section 2. The concept and components of LIGHTest is discussed in section 3. The proposed implementation of the distributed lightweight infrastructure for an IOT sensor network is discussed in section 4. Finally, one of the fast developing authentication technique called Block Chain technology is analyzed with the proposed trust infrastructure using DNS in section 5.

2 Related Work

2.1 Importance of Security in Industry 4.0

With the increased connectivity and use of standard communication protocols that come with Industry 4.0 [Bl17], the need to protect critical industrial systems and manufacturing lines from cybersecurity threats increases dramatically. As a result, secure, reliable communications, as well as sophisticated identity and access management of machines and users, are essential. The term Cyber-Physical Systems (CPS) has been defined as the systems in which natural and human-made systems (physical space) are tightly integrated with computation, communication and control systems (cyberspace). Decentralization and autonomous behaviour of the production process are the main characteristics of CPS. The evolution of CPS mainly depends on the adoption and reconfiguration of product structures and supply networks. For example: when a city traffic control system is brought into CPS, it has to adopt to the standards and configurations of CPS network. The continuous interchanging of data is carried out by linking cyber-physical systems intelligently with the help of cloud systems in real time. Use of proper sensors in CPS should find out the failure occurring in machines and automatically prepare for fault repair actions on CPS. Which in turn finds the optimum utilization of each work station with the help of cycle time required for the operation performed on that station. An example of cyber-physical system is the connected smart vehicle which represents the development of Industry 4.0. US Commerce Department's National Institute of Standards and Technology (NIST) developed five critical functions [Ar17] necessary to make security effective on an ongoing basis namely Identity, Protect, Detect, Respond and Recover.

2.2 Cyber security threats to IOT systems

IOT facilitate integration between the physical world and computer communication networks. Applications (apps) such as infrastructure management and environmental monitoring makes privacy and security techniques [RJ13] critical for future IOT systems [ACH15]. Consisting of radio frequency identifications (RFIDs), wireless sensor networks (WSNs), and cloud computing, IOT systems are vulnerable to network attacks, physical attacks, software attacks and privacy leakage. The IOT security threats are as follows.

•**DoS**: Denial of Service (DoS) attackers aim to restrain IOT devices from inheriting the network and computation resources.

•**DDoS**: Distributed Denial of Service (DDoS) attackers with hundreds of IP addresses make it more difficult to distinguish the genuine IOT device traffic from attack traffic. Distributed IOT devices with light-weight security protocols are especially prone to DDoS attacks.

•**Jamming**: Attackers send fake signals to suspend the ongoing radio transmissions of IOT devices and further diminish their energy, bandwidth, central processing units (CPUs) and memory resources of IOT devices or sensors during their failed communication attempts.

• **Spoofing**: A spoofing node impersonates a legal IOT device with its identity such as the Medium Access Control (MAC) address, Universally Unique Identifier (UUID) and RFID tags to gain illegal access to the IOT network system.

•**Man-in-the-middle attack**: A Man-in-the-middle attacker sends jamming and spoofing signals with the goal of secretly monitoring, eavesdropping and altering the private communication between IOT devices.

•**Software attacks**: Mobile malicious software's such as Trojans, ransomware, worms, and the virus can result in privacy leakage, data theft, economic loss, power depletion and network performance deterioration of IOT systems.

•**Privacy leakage**: IOT systems have to protect the privacy of the user during data caching and exchange. Some caching owners are inquisitive about the data contents stored on their devices and analyze and sell them to third parties for a large amount of money. For example: In recent days wearable devices that collect user's personal information such as location and health had witnessed an increased risk of personal privacy leakage.

2.3 PKI based open source Infrastructures

A Public Key Infrastructure (PKI) [CBH02] is a cryptographic technique that binds public keys with respective identities of entities (like organizations). The binding is established through a process of registration and issuance of certificates at and by a Certificate Authority (CA). Which allows creating a set of roles, policies, procedures and in turn manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. Nowadays due to the increase of devices in IOT, there are open source PKI infrastructures like IOT_pki [DLL18] which can be used to create certificate easily and verify digital signatures.

2.4 Disadvantages of current security infrastructures

In general, there are many certificate-based solutions which are suitable for the IOT. For example: PKI, in which verification of all identities are allowed, provided they are appropriately registered with equipped certificates. But PKI are often limited for the current IOT standards because they are often too expensive [Ss07] since a large number of devices are connected to the network. The critical weakness of the current X.509 scheme implementation is that any CA trusted by a particular party can then issue certificates for any domain they choose. Such certificates will be accepted as valid by the trusting party, whether they are legitimate and authorized or not. This is a serious shortcoming as most commonly encountered technologies employs X.509 certificates [CBH02]. For example: All major web browsers are distributed to their end-users pre-configured with a list of trusted CAs that numbers in the dozens. This means that any one of these pre-approved trusted CAs can issue a valid certificate for any domain.

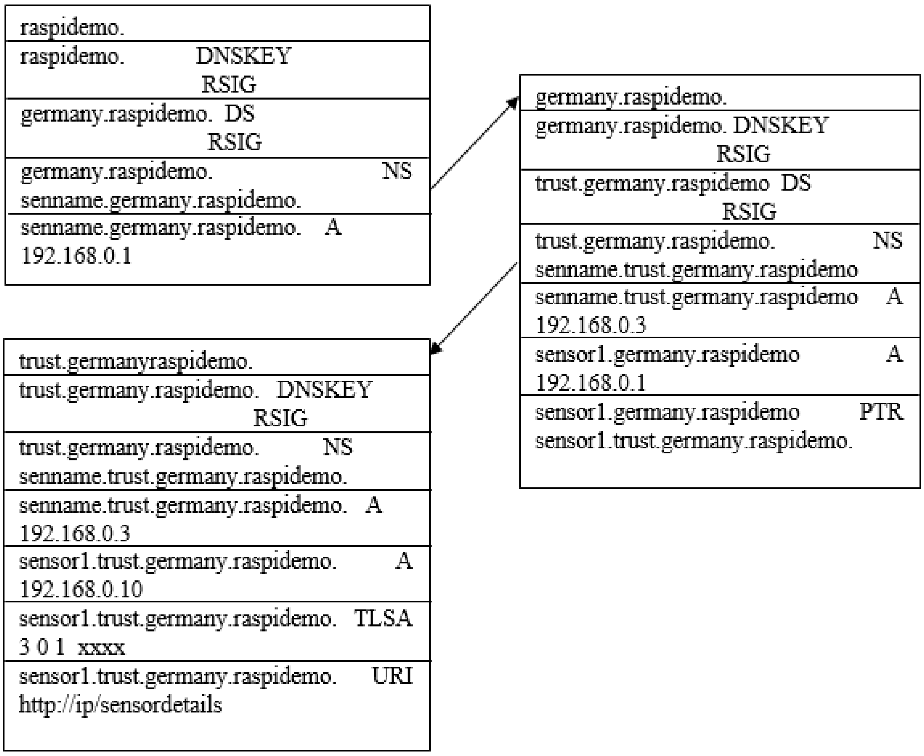
This issue is the driving impetus behind the development of the *DNS-based Authentication of Named Entities* (DANE) protocol. If adopted in conjunction with *Domain Name System Security Extensions* (DNSSEC), DANE will greatly reduce the role of trusted third party CAs in a domain's PKI.

3 Concept of light weight trust infrastructure using DNS in fault authentication of sensor management system

The EU research project LIGHTest proposed to develop a light weight identity management system which uses the DNS infrastructure of the internet. The security mechanisms of the DNS is enhanced DNSSEC and DANE which offer together a worldwide available and accepted central root certificate (trust anchor) and also the ability to operate in a hierarchical structure. With DNSSEC a certificate chain is developed from child till root to make the zones secured, thereby reducing the man in the middle attack. The distributed hierarchy infrastructure of DNS can be used to create distributed trust schemes which are independent of each other. The hierarchical structure also reduces the complexity and management of devices in the IOT network. For example, the manufacturer of sensors has its own trust policies and certificates to verify the certificate of the sensor. LIGHTest offers the possibility to reduce the customer overload not by storing and managing each and every sensor certificates in its IOT network, but it will be taken care of by the manufacturer. The customer DNS server has to trust the trust scheme publication authority of the manufacturer. This reduces the complexity of the network and also it gives the manufacturer possibility to take care of all the certificates and decide the entries of the trust lists based on the situation.

3.1 Distributed Authority of DNS

In the concept of fault authentication in an IOT sensor network, a company which has locations in many countries is considered. And how their sensors are brought into the DNS server and linked to the corresponding Trust Scheme Publication Authority will be explained. For simplification, how a sensor transaction e.g. from a machine component located in Germany is authenticated will be explained. The hierarchy binding of the zone in DNS is shown in Fig 1: The top level of the domain is considered as *.raspidemo* and under this comes secondary domain with respect to country *germany. raspidemo.* And all the details of the sensors are located in the corresponding zone file. The implementation has the flexibility to accommodate many zones. For example: for sensor in other country like India, Austria.



raspidemo.
raspidemo. DNSKEY RSIG
germany.raspidemo. DS RSIG
germany.raspidemo. NS senname.germany.raspidemo.
senname.germany.raspidemo. A 192.168.0.1

germany.raspidemo.
germany.raspidemo. DNSKEY RSIG
trust.germany.raspidemo DS RSIG
trust.germany.raspidemo. NS senname.trust.germany.raspidemo
senname.trust.germany.raspidemo A 192.168.0.3
sensor1.germany.raspidemo A 192.168.0.1
sensor1.germany.raspidemo PTR sensor1.trust.germany.raspidemo.

trust.germanyraspidemo.
trust.germany.raspidemo. DNSKEY RSIG
trust.germany.raspidemo. NS senname.trust.germany.raspidemo.
senname.trust.germany.raspidemo. A 192.168.0.3
sensor1.trust.germany.raspidemo. A 192.168.0.10
sensor1.trust.germany.raspidemo. TLSA 3 0 1 xxxx
sensor1.trust.germany.raspidemo. URI http://ip/sensordetails

Fig 1 : Hierarchy binding of zones in DNS using DNSSEC

Since each country sensors may have different trust schemes, it is added in the third zone of the DNS server as *trust.germany.raspidemo.* This points to the corresponding trust scheme of the sensor, which in turn point by URI to the corresponding trust lists which are managed by the manufacturer.

3.2 Querying sensor data using DNS and TSPA

In this approach of querying sensor data from DNS, it is very essential to ensure the entries of sensor data in DNS zone file and the entries of trust lists has already been published via TSPA. For example, when sensor1 from a machine component located in Germany needs to be verified, the verifier of the company sends a DNS request based on sensor name and location to the DNS server which in turn gets the location of the trust scheme. The trust scheme is further queried for the URL of the trust scheme publication authority, which has the access to the trust lists. A distributed trust scheme publication authority is developed as a stand-alone server separated from DNS and is responsible for maintaining all the trust lists of the different sensors. In Trust scheme publication authority each sensor manufacturer has independent login credentials to publish their trust lists and details of the sensor. So by using this distribution different manufactures of sensors can be easily linked and brought together in a single network using DNS infrastructure.

4 Implementation of fault authentication in sensor management systems using Raspberry Pi Cluster.

4.1 Hardware and Software used

The hardware used for this fault authentication in IOT network is Raspberry Pi 3B development microcomputers, a temperature sensor used as a sensing device and also LEDs for denoting the fault.

The software used for this experiment is python accompanied by crypto libraries, DNS BIND software and django framework.

4.2 Design description

Let us assume an Industrial Internet of Things (IIOT) scenario where there are machines with a temperature sensor connected to it, due to some malfunction the machine may get overheated at some course of time and it notifies to the corresponding person by giving a notification message. In this paper, an authentication system is developed which uses LIGHTest infrastructure to authenticate data from a sensor in an IIOT network.

For example, as shown in Fig. 2: a temperature sensor is used, which gives a notification message when the temperature goes beyond certain threshold only after corresponding integrity check and Authentication with trust scheme publication authority using DNS.

SENSOR: when the temperature goes beyond certain threshold, the sensor establishes communication with the verifier and notifies about the fault in the device.

VERIFIER: It is the powerful system or a super computer of the network which co-ordinates and takes all the decisions with respect to integrity, confidentiality verification of the system and authentication of the data.

DNS SERVER: In the implementation a three level domain was developed with *.raspidemo* as top level domain and also acting as a resolver. Under this domain comes the secondary level domain which contains different zone files based on different countries. And in the corresponding country zone files all the sensor details will be stored based on their names. There is a possibility to create different trust schemes for different sensors. The trust scheme is maintained in the third level domain. It contains the details of the trust scheme publishing authority for the corresponding sensor.

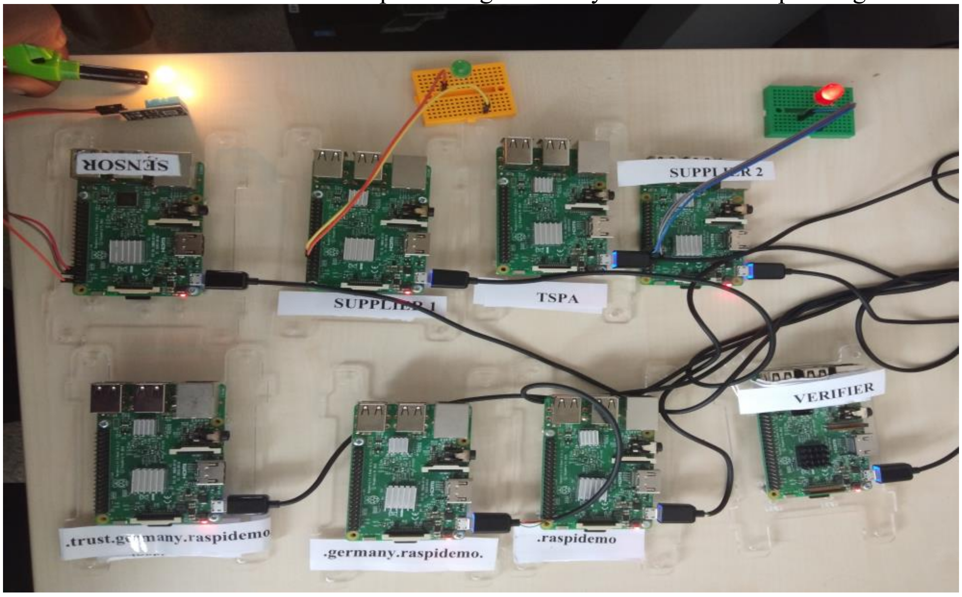


Fig. 2: Implementation of fault authentication in Raspberry Pi Cluster

TRUST SCHEME PUBLICATION AUTHORITY: The TSPA is stand-alone component and is separated from the DNS server. For example: the trust lists contents of the sensors in the TSPA can be generated and maintained in a flexible way, which can be changed according to the manufacturer interests. The trust lists contents used in the implementation has the public key or certificate of the sensor, supplier name and IP. When there is some fault from the sensor the verifier notifies the corresponding supplier pointed by the trust scheme publication authority. There is also a possibility to connect different trust scheme publication authorities for different sensors.

SUPPLIER: A company can have different suppliers to take care of the maintenance. Based on the availability of supplier, it'll be updated to the corresponding trust scheme publication authority. Verifier then redirects to the corresponding supplier.

4.3 Block diagram of infrastructure with functionality

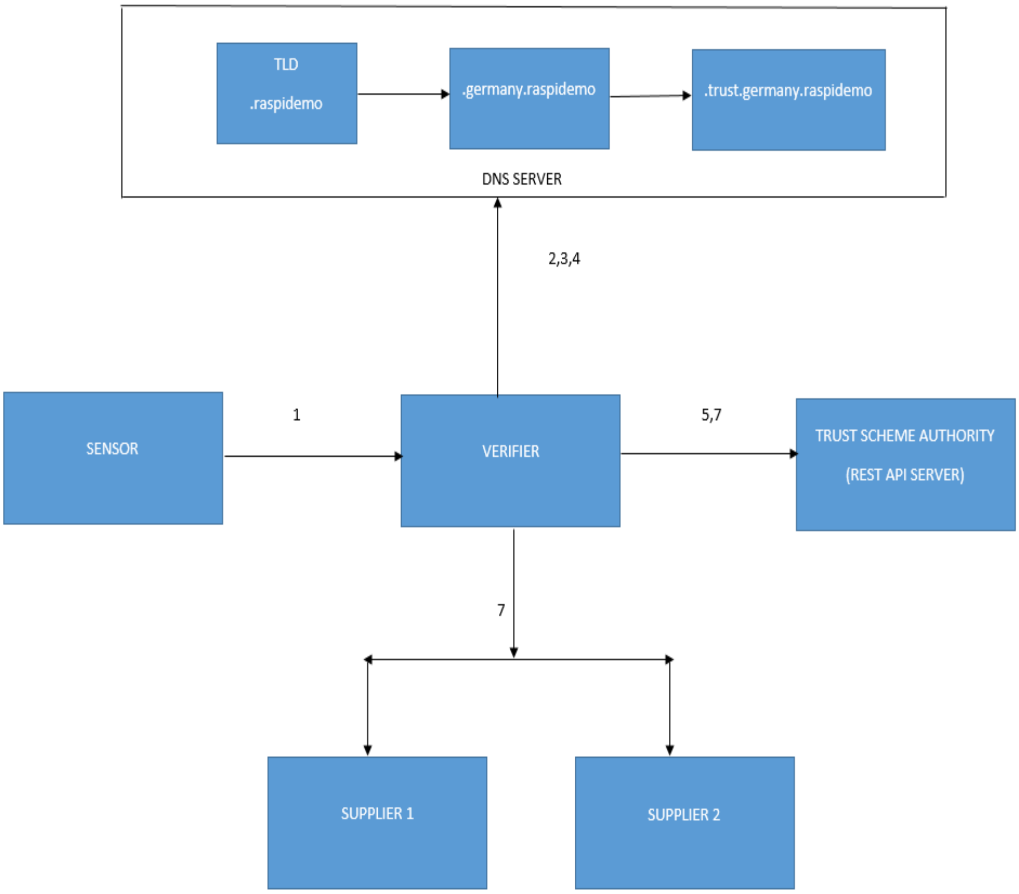


Fig. 3 : Block diagram for fault authentication in sensor network

The block diagram of the complete infrastructure for fault authentication in IOT sensor network is shown in Fig. 3. And the details about the functionality of block diagram is explained below.

STEP 1: When the temperature is above 25°C the sensor notifies to the Verifier by sending sensor name, location and the signed data.

STEP 2: The Verifier develops a DNS query (*sensor1.germany.raspidemo*) based on the sensor name and location and sends it to the DNS resolver to make sure the corresponding query is DNSSEC protected.

STEP 3: Once DNSSEC is verified, the same query is sent again to look for pointers to the trust scheme provider and in turn gets *(sensor1.trust.germany.raspidemo).*

STEP 4: The trust scheme provider domain is verified for DNSSEC in order to ensure integrity among the domains. And also the transport layer security of trust scheme provider is ensured by verifying its certificates with the TLSA record stored in the zone file. If it passes the integrity check, then using the trust scheme provider domain corresponding URI of the trust scheme authority is queried which contains information certificates to verify the signed data of the sensor.

STEP 5: The corresponding URI is queried to fetch the certificates of the sensor1, which is used to verify the signed data of sensor1.

STEP 6: Once this signed data is verified, the integrity among the domain is ensured including the transport layer and also the certificate used for signing is believed to be a trusted one.

STEP 7: The verifier looks for the supplier address in the URI of the trust scheme authority. Based on the supplier address provided, it establishes the connection with the corresponding supplier. In this example there is an LED blink at the supplier denoting the warning of the sensor.

5 Discussion of competitive authentication technologies

In this section the functionality of lightweight DNS trust infrastructure is analyzed with existing authentication technology called block chain technology [LK18] based on standard security parameters namely confidentiality, integrity, availability, non-repudiation, authentication and cost of implementation. Block chain [Na08] is also a growing distributed ledger based technology, which can be used for different authentication process [Gu13]. The data is distributed and shared by everyone involved in the process, so it’s difficult to tamper the data. But when meaningful data is stored in block chain [Be14] [Cr15] and since it’s available in public to everyone [Qu90], hackers can study the pattern of data and exploit the data. For example: smart contracts [Sz97] [Sz94] in block chain Ethereum has the capacity to eliminate all the third part arbitrators by executing the policies by itself. This can help in reduction of the transaction costs but it requires high capital costs to shift to a new decentralized network. If a block chain is not a robust network with a widely distributed grid of nodes [Ch14], it becomes more difficult to reap the full benefit in turn affecting the confidentiality of the service.

Whereas LIGHTest is a light weight infrastructure which can be easily build on existing DNS system there by reducing the capital costs. The hierarchical structure of DNS is used to achieve a distributed environment which can be easily adopted by companies that are present globally. DANE along with DNSSEC also offers good confidentiality by providing transport layer security, so man in the middle of attack can be prevented. DNS doesn't overload by storing all the data where as it contain only pointers to the trust scheme publication authorities, which in turn hold the corresponding trust lists with the sensor information for verifying the transaction.

6 Conclusion

In this paper security threats to the IOT network were analyzed. In order to overcome the threats globally, LIGHTest proposed decentralized trust security infrastructure using DNS which has the potential to increase the confidentiality and thereby reduce security threats, example: man in the middle attack. The concept of LIGHTest is proved by building an Implementation of automatic validation of faults in an IOT sensor network using Raspberry Pi Cluster. Since DNS infrastructure is accepted globally, LIGHTest has the ability to connect across domains. It can be easily adopted by multi-national companies. The application is not only limited to Industrial IOT, it can be also used in authentication applications.

Bibliography

[ACH15] Andrea, I; Chrysostomou, C.; Hadjichristofi., G.: Internet of Things: Security vulnerabilities and challenges, IEEE Symposium on Computers and Communication (ISCC). pp. 180–187.DOI: 10.1109/ISCC.2015.7405513, July 2015.

[Ar17] Arrunadayy, K.: What's the 5 pillars of information security?, 2017; https://www.quora.com/Whats-the-5-pillars-of-information-security.

[Be14] Ben-Sasson, E. et.al: Zerocash: Decentralized Anonymous Payments from Bitcoin, IEEE Symposium on Security and Privacy, 2014.

[BL16] Bruegger, B.P.; Lipp, P.: LIGHTest-A Lightweight Infrastructure for Global Heterogeneous Trust Management, In: Open Identity Summit 2016, 13.-1 14.October 2016, Rome, Italy. 2016, pp. 15–26. https://dl.gi.de/20.500.12116/593.

[Bl17] Blighwall, S.: Industry 4.0: Security imperatives for IoT — converging networks, increasingrisks,2017,http://www.dxc.technology/security/insights/141481-industry_4_0_security_imperatives_for_iot_converging_networks_increasing_risks.

[CBH02] Choudhury, S.; Bhatnagar, K.; Haque, W.: Public Key Infrastructure Implementation and Design (1st ed.). John Wiley & Sons, Inc., New York, NY, USA, 2002.

[Ch14] Cheu, R. et.al: An Implementation of Zero Knowledge Authentication, Massachusetts Institute of Technology Narwhal, 2014.

[Cr15] Crosby, M. et.al: Block Chain Technology, Sutardja Center for Entrepreneurship Technology Technical Report, Oct. 2015.

[DLL18] Duan, L.; Li, Y.; Liao, L: Flexible certificate revocation list for efficient authentication in IoT, In Proceedings of the 8th International Conference on the Internet of Things (IOT '18). ACM, New York, NY, USA, Article 7, 8 pages, 2018, https://doi.org/10.1145/3277593.3277595.

[Gu13] Gungor, V.C.et.al: Survey on Smart Grid Potential Applications and Communication Requirements, IEEE Transactions on Industrial Informatics 9.1, pp. 28–42. ISSN: 1551-3203. DOI: 10.1109/TII.2012.2218253, Feb. 2013.

[LK18] Lee, C. H. and Kim, K.: Implementation of IoT system using block chain with authentication and data protection, *2018 International Conference on Information Networking (ICOIN)*, Chiang Mai, Thailand, pp. 936-940. doi:10.1109/ICOIN.2018.8343261, 2018.

[Na08] Nakamoto, S.: Bitcoin: A Peer to Peer Electronic Cash System, https: //bitcoin.org/bitcoin.pdf

[Qu90] Quisquater, J.-J.et.al: How to Explain Zero-Knowledge Protocols to Your Children, Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology. CRYPTO ’89,Berlin, Heidelberg: Springer-Verlag, pp. 628–631. ISBN: 3-540-97317-6, 1990,http://dl.acm.org/citation.cfm?id=646754.705056.

[RJ13] R. Roman, J. Z.; Javier Lopez: On the features and challenges of security and privacy in distributed internet of things, The International Journal of Computer and Telecommunications Networking, 2013.

[Ss07] ssh, Advantages and disadvantages of public key authentication, 2007, https://www.ssh.com/manuals/server-zos- product/55/ch06s02s02.html.

[Sz94] Szabo, N.: Smart Contracts, 1994, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

[Sz97] Szabo, N.: The Idea of Smart Contracts, 1997, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html

[Wa17] Wagner, S.et.al: A Mechanism for Discovery and Verification of Trust Scheme Memberships: The Lightest Reference Architecture, In:Open Identity Summit 2017, Karlstad: GI-Edition, Lecture Notes in Informatics.pp. 81–92.