Identity and Access Management for the Internet of Things

Ishaq Azhar Mohammed

Sr. Data Scientist & Department of Information Technology

Dubai, UAE

Abstract*-The main aim of this paper is to investigate the idea of identity and access control for Internet of Things applications. Organizations collect enormous amounts of data from their activities nowadays. This information is derived from transactions performed by a person or a paired device. The internet has now become the preferred method of contemporary communication, raising the need for a way to monitor and protect various connections [1]. To guarantee the system's credibility, interconnected equipment gathering data must be protected. A company should not only verify the identities of its network users and be able to track their activities, but also trust the technology that provides this information. The Internet of Things is a broad-based network of devices, which may interconnect and cooperate in the production of a range of services, anywhere and in any manner [1]. Balancing access control, authentication, and mobile identity management while interacting with other equipment, resources and infrastructure is a major issue for identity management. In the modern Internet communication environment, the maintenance of identities poses major difficulties. These difficulties on the internet are compounded by the unlimited number of users and anticipated resource limits [2]. Modern identity management systems focus primarily on the identities often used by end-users as well as on networked services. Even so, these identity management systems are developed because substantial resources are available and their application to the resource-laden Internet of things requires careful study. To effectively manage the myriad of applications and believe that the identity of a machine would be verified, businesses need to implement digital credential solutions with a robust foundation of trust [2,3]. Historically, this has been accomplished via the use of Public Key Infrastructure (PKI) and a smart card. Combining blockchain with public key infrastructure solutions*

enables the provision of identity and access management platforms for the internet of things (IoT). RFID security measures and different blockchain solutions provide are viable alternatives for securing IoT device authentication and authorization.

Keywords: *Identity and access management, Symmetric Cryptography, Asymmetric Cryptography, Internet of Things, Radio Frequency Identification (RFID), blockchain, Public Key Infrastructure (PKI)*

I. INTRODUCTION

Even as the general public starts to embrace smart homes and Internet of Things wearables, IoT devices and apps are expanding their scope and becoming more widely used in corporate, governmental, and other settings. The network connection required to enable it is becoming ever more omnipresent and devices must be recognized and accessed in various settings and organizations. The identity life cycle is examined and a discussion is conducted on the infrastructure components needed to give authentication credentials that concentrate heavily on PKI. We also explore various kinds of authentication credentials and propose innovative methods for IoT device authorization/access control. The IoT requires the exponential management of more identities than current IAM solutions. There is a paradigm change in the security sector that means that IAM no longer only manages people, but now manages the hundreds of thousands of objects linked with a network. These objects are sporadically linked in many cases and may need to interact with other things, mobile devices, and backend infrastructures. The industry is only starting to develop and implement IoT, therefore it is important to examine how IoT IAM connects to other safety services needed for an IoT-connected company. Services like asset and cryptographic key management are included. In certain cases, IoT solution providers have already started including IAM as a by-product for connecting IoT assets. The IoT solutions tend to depend significantly on cloud computing. This dependence on cloud computing adds to the requirement for security beyond the standard authentication, access control, and secure channels presently in use. For better identification, authentication, and authorization, industrial standards drive demand for trustworthy digital identities [3]. A trust chain demands that every part of the firmware be digitally certified before it is connected to the network. After a single code item is verified, the next part may be checked, and so on, until each item in the chain is validated. The trust chain needs a solid basis at the lowest level that prevents a malevolent person from compromising. This article examines the usage of the IoT Identity and Access Management (IAM) architecture for Radio Frequency Identification (RFID) and blockchain technologies, coupled with PKI [4]. This paper will explore in detail how IAM works well with IoT to improve operations in the IT sector.

II. PROBLEM STATEMENT

The main problem to be solved in this article is how IAM is applied to IoT devices. The number of Internet-linked devices has recently increased by one-third each year, from 5 billion in 2015 [5]. This increases the desire of hackers to compete for a growing number of IoT devices (Internet of Things). One of the main concerns is thus the IoT botnets engaged in the assaults on the Distributed Denial of Service (DDoS) [5,6]. There are numerous risks for an unsafe IoT gadget. In addition to cloud services, IoT devices are increasing, which will continue to challenge cybersecurity experts to secure the perimeter [2]. Identity And access management application by the Internet of Things helps towards identity management in the Internet of Things for everyday gadgets [6]. It introduces the motivating elements in the context of the Internet of Things together with the identity management issues and offers an identity management paradigm. It then talks about key

problems for the management of identity and offers several identity models. This book also shows links between identity and trust, various ways of managing the trust, authentication, and access control [6]. Clusters with the hierarchical identifier, user authentication, reciprocal access control, and mutual authentication are key recognized breakthroughs for identity management. Identity Management for the Internet of Things is excellent for computer/communication workers and academics, wireless communications, informatics, industrial engineering, electrical and telecommunication services systems, and cloud services students [7].

III. LITERATURE REVIEW

A. Identity and access management (IAM)

Identity and Access Management (IAM) is usually described as a system of rules and technology that ensures that authorized persons have access to network resources inside an organization [8]. Identity management systems offer access control over the resources of an organization and monitor the behavior of users while operating inside these resources. The IAM offers a method to control user permissions depending on their position inside the company. This may be done by providing a way to safeguard organizational resources and data via policies and regulations that need passwords, user rights, and user accounts [8]

B. Management of IoT Access

Devices and ecosystems that use the Internet of Things must provide secured access to IoT features and settings. The ability to access devices via the cloud through a managed app or an on-premises website must be protected regardless of how they are connected. Allegro's first IoT software was especially intended to allow for safe on-site IoT device administration. The Supply Chain and Beginning of Life (BoL) phases of a device's lifetime are when secure access control methods are applied [8]. This is when the confidence and cryptography root is installed. The secure storing of parameters is generated using many keys known as an asset. By establishing a digital signature over the keys, cryptography will safeguard such assets, verifying their validity and authenticity [9]. Default user names and passwords may be the greatest risk for protecting access to devise parameters and configuration management. This is the most frequent hacking method for compromising IoT and embedded devices - usernames and passwords should never be used by default [10]. One method to protect against this issue is to provide unique user names and passwords when creating an IoT device in the configuration settings. Tools such as the ACE toolkit from Allegro ensure the safe management of assets via the generation of unique keys inside an asset. Key Factor, one of Allegro's strategic partners, offers unique keys and access management to previously deployed IoT devices.

C. IoT Identity for Device Management

We are moving towards the omnipresent age of networked communication networks and networked gadgets. Things like a fridge, a vehicle, and even a taste of tea are also linked to the network in this ubiquitous world of computers and communication. New technologies, such as RFID and advancing smart computer gadgets, make the world of completely linked devices the world with soaring networks and applications [10,11]. The merging of various technologies culminates in a wireless network comprised of heterogeneous devices capable of self-configuration, dubbed the Internet of Things (IoT). IoT envisions connecting any device having computing, communication, and sensor capabilities to the Internet. IoT encompasses a diverse variety of devices, ranging from RFID tags to sensor nodes and even footwear. Therefore, the Internet of Things enables mobile cooperation and communication between people and devices, as well as between technologies and networks. Due to fast technological developments in mobile communications, data from an infinite number of networks and devices converging on user devices, telecommunications networks, and the World wide web are now an essential part of computer networks today. The Internet of Things amplifies information and communication overload owing to objects, digital phones, applications, and sensors. In such an environment, the increased size and breadth of IoT expands how a user may engage with the real and virtual objects in his or her surroundings. This wider scope of interactions highlights the need of extending existing Identity Management (IdM) models to account for how people engage with devices as well as how devices interact with one another [12}. Through verified identification, users connect with their devices and receive IoT services. This notion of identification is extended to devices/things in the Internet of Things.

In comparison to today's world, where interactions with technologies and networks are limited by ownership and subscription, IoT users can explore and use public devices, partially or completely add items to their private space, and start sharing their devices with others. Additionally, public devices can be part of the personal environment of multiple users. The primary difficulties include safe interaction inside and with the IoT, secure communications exchange and sharing, authenticating, decentralized access control, and device identity management [12]. The study conducted in the context of this paper addresses key areas of IdM by pinpointing unresolved issues and offering new methods for resolving them. The objective is to provide efficient and effective IdM techniques for achieving authentication, access control, and trust management for objects or devices in the Internet of Things. Additionally, the aim is to provide vulnerability assessment and attack modeling in IoT, as well as mitigation methods that are lightweight and resistant to assault due to IoT's dispersed nature. In ubiquitous contact between devices or objects whose identities are unknown in advance, trustworthiness and trust management are critical. In the Internet of Things, trust is contingent on many changeable factors, necessitating a particular emphasis on this front. This section of the thesis discusses the connection between trust and access control and introduces a fuzzy method for calculating the trust score. This section of the thesis also introduces a novel framework for trust-based access control. The primary difficulty in developing an IdM for IoT devices is designing a scalable and attack-resistant mutual authentication system. Threat analysis and attack modeling are critical in dispersed IoT, and this section of the thesis discusses the dangers in-depth [12].

D. Radiofrequency identification (RFID)

Radio Frequency Identification (RFID) platform is a low-power system that transfers data wirelessly. The tags are typically passive devices, which means they do not need a power source, while the readers are more complex computer devices that require adequate power, storage, communication protocols, and their clock to function properly [13]. RFID began as a method to replace barcodes but has now expanded to encompass a broad range of uses, including toll sensors, passports, debit cards, entrance badges, pet GPS trackers, pharmaceutical, clothing, library books, and many other items [13,14]. As a result, RFID has emerged to become the primary way of delivering wireless communication between Internet of Things devices. This has raised the need of establishing a safe system of

identification and identity management. Lightweight encryption techniques have been created using basic cryptographic features for authentication. RFID systems are comprised of RFID tags and RFID readers, among other components. To make use of a PKI IAM, each tag must have its public/private key pair, as well as a public key certificate. The main function of RFID tags is to enable readers to identify them. Tag identification and tracking may be accomplished using a reader that has been taken into the hands of a malevolent user (i.e., stolen, lost, or hacked). As a result, having faith in the reader is more important than having faith in the tag. Near-field communication [14] has been proposed as a means of establishing confidence despite the dangers involved with the reader.

Fig i: A basic RFID system

1. Symmetric Cryptography

Near Field Communication (NFC) is a more simplified version of the Rfid system. The NFC system consists of two wireless devices that communicate over short distances (between 5 and 10 cm). There are two options to choose from: active and passive mode. The communication is initiated by an active mode device. These devices are collectively referred to as initiators. The initiator produces its energy and transmits data via amplitude shift keying, which is unique to this technology. For passive mode, the device is known as the target, and it communicates with the initiator by using the Radio Frequency (RF) field generated by the initiator as power [15,16]. The distinction between reader and tag is eliminated with NFC, which eliminates the main problems associated with RFID PKI use. For instance, NFC-enabled cellphones can flip between being a reader and being a tag in a matter of seconds. When transmitting, the smartphone serves as the tag, and when obtaining, the smartphone serves as the reader (or reader tag). To defend NFC tags from cyberattacks, a cryptographic challenge-response system based on public-key cryptography and public key infrastructure (PKI) has been created. The suggested system makes use of symmetric cryptography [16] to secure data transmissions. The NFC chip [16] is equipped with a secure protocol, which helps to increase security. A data/information processing unit is being integrated into NFC-enabled systems to add a layer of security to the system. In addition to the security protocol, there is a processing stack. The procedure starts with the handshaking scheme requesting a certificate from the user. As long as the certificates and the signatures are the same, the data is saved for further analysis [16]. If there is a mistake at any point, for example, if the certificate and signature cannot be validated, the data is deleted from the system and warning messages are sent [16,17]. In testing, it was discovered that the suggested NFC system provides sufficient protection against tag modification and data injection. When the signature size is increased, there is a little increase in the processing time required. As a result, a smaller signature [17] may be used to save processing time.

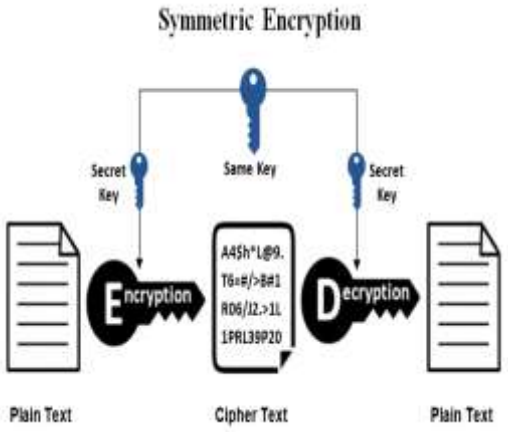

Fig ii: Symmetric encryption

2. ***Asymmetric Cryptography***

For IAM to function properly, strong authentication must be used. Asymmetric encryption such as the Advanced Encryption Standard (AES) or symmetric cryptography such as Elliptic Curve Cryptography (ECC) [18] is used by the vast majority of top services to offer robust authentication [17]. Asymmetric solutions, such as ECC, are difficult to implement and inefficient in many situations. Cryptographic Protected Tags (CPTs) are a secure NFC technology with a flexible design that has been found by researchers (CRYPTA). The latter operates passively, using a low-area design that makes the most efficient use of available resources. This passive solution offers a safe NFC/RFID for usage in IoT devices such as smartphones NFC-enabled [17]. Authenticity and secrecy are needed to communicate between a sender and receiver, thus a server has to verify its identity with the client and vice versa [9]. The CRYPTA Tag offers authenticated strength utilizing an analog antenna, demodulating and modifying data, extracting power, and providing a steady clock and reset signal [18]. A part of the frame logic is responsible for dealing with time-critical low-level instructions. In the crypto unit, the cryptographic actions are carried out, and the microcontroller has access to this unit via the use of microcode patterns. The tag is powered by the RF field and serves as the feed, clock, and reset interface. CRYPTA utilizes an 8-bit microprocessor with a small chip size and low power consumption, creating more efficiency than anything presently in use [18]. The main disadvantage of CRYPTA is that it is a suggested real-world RFID system that contains all hardware components necessary for chip manufacturing in practice. However, additional testing will be required to establish the system's feasibility as an IoT solution.

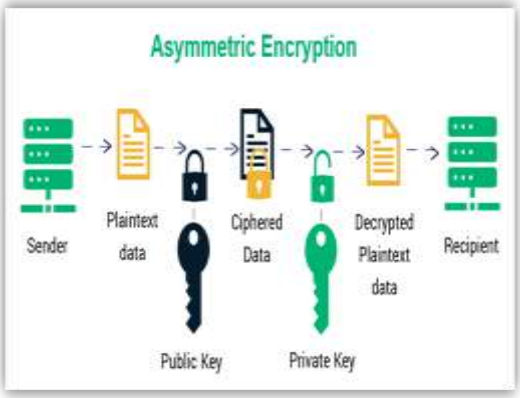

Fig ii: Asymmetric encryption

E. ***Permissions and access are the cornerstones of the IoT evolution***

While the IoT has exploded in recent years, it is an extension of concepts that have been around for decades, if not centuries, and which have seen technical advances achieved in our military transferred to the private sector and across sectors. Take, for example, railways, which were one of the driving forces of the Industrial Revolution in the United States. Through multimodal transportation, they were able to transfer products effectively throughout the nation and then across the globe. As technology has progressed, so have the management systems and indicators that ensure trains remain on the correct tracks and are traveling in the proper direction, as well as the control systems that monitor the environmental effect, such as wastewater treatment systems, have developed. Forward to now, and society has taken that concept and applied it to the commercial, virtual environment, rather than just the industrial one. It's now possible to communicate with automatic equipment such as thermostats and door locks. Nevertheless, the concept of control systems developed in the 1950s and 1960s was not designed with identity management, security, or access restrictions in mind [18]. As opposed to this, they were constructed based on physical access restrictions.

F. Identity management in a shifting threat environment

While security and identity access control is no longer as physical—they are outsourced digitally in IoT—our consumer sector continues to see gadgets in a very detailed manner. With this in mind, new vulnerabilities have been formed as IoT devices are exposed to increasing dangers. As we transmit those assumptions into the changing country. For instance, when workers take work outside of the office to their homes, personal IoT devices, and personal networks, companies must consider the security measures that will be required to safeguard critical information and data. Emphasizing hardware security, such as strong passwords and up-to-date software on business laptops, while also scanning personal home networks for weaknesses before joining, may assist to minimize problems and threat exposures. Implementing multifactor authentication can also assist to guarantee that your company's network and systems are only accessible by those who have been granted access to them.

G. IoT must extend its role in managing identity access

By recognizing the holistic system and proactively protecting the edge, there is tremendous potential in the realm of IoT. Instead of focusing on each particular gadget in the home, take a holistic view of the whole house. Consider the surrounding area as well. It ultimately boils down to governance: what kind of control mechanisms do we have in place. Is it possible to mandate that governance be carried out following best practices or secure design principles? Those standards are beginning to take shape today, particularly in light of the rise of smart buildings, but given the way the threat environment has evolved, there is still enormous room for advancement.

Blockchain technology

A blockchain is a kind of data system that makes use of public-key cryptography to create tamper-resistant digital certificates that can be exchanged between parties. [19] To put it simply, these are online transactions that allow for decentralized and verifiable data exchange. In E-commerce, cryptocurrencies are the technologies that underpin bitcoins, which have proven to be very profitable. [6] Because blockchains depend on cryptographic evidence rather than trust, they do away with the need for an intermediary to verify transactions and allow for complete anonymity in online transactions. The establishment of trust would be required to deploy blockchain effectively inside IAM to put in place security measures to protect against interference, breach, and eavesdropping [20]. Dependence on a centralized cloud is a significant risk for Internet of Things apps and platforms. Because the PKI is centralized and relies on trusted third parties, it is not suitable for use in a distributed environment. To overcome skepticism, it is necessary to decentralize and include blockchain technologies.

Fig i: Properties of a blockchain ledger

IV. FUTURE IN THE U.S

Over the last several years, digital identities have grown in popularity and application, particularly within national governments. Today's government agencies in the United States generate, analyze, and transmit data at an unparalleled, exponentially increasing pace. The information technology (IT) environment of the modern-day is continuously evolving, bringing with it new possibilities and dangers. Agencies throughout the federal government face growing pressure to stay up with technological advancements, accelerate digital transformation, and embrace cloud solutions and mobile applications. With the growth of digital interactions and transactions, protecting access to sensitive and classified data becomes even more important for mitigating insider threats, strengthening an agency's cyber posture, and delivering government services [20]. To maintain a secure organization, federal and military officials must have a firm grasp on who has access to documents and how that access is evaluated. Developing encryption algorithms will be essential in allowing the government's digital ecosystems to expand and progress securely. While organization-specific requirements may differ, sophisticated encryption will be a critical component of any modernized digital infrastructure. Post-quantum cryptography will be required in the future years for workplaces with data that must remain safe for extended periods after initial encryption.

V. ECONOMIC ADVANTAGES

Economic advantages of IAM for IoT include the development of the Blockchain sector. Since identities may be individually verified in an unchangeable and secure ledger, blockchain technology may be able to address a variety of digital identity issues. Cryptocurrency systems rely on identity verification through public key cryptography-based digital signatures. The sole verification done with this technique is to ensure that the transaction was verified with the proper private key. We deduce that the owner is the individual who has access to the keys. The

identity of the owner is irrelevant. Biometrics enhances the capacity to verify a client's identification with a high degree of confidence, enabling automated onboarding and remote access to public services. A variety of biometric technologies are becoming cheaper [20]. This technology allows automatic user identification based on physical (fingerprints, veins, and iris) and/or behavioral features (voice, keystroke, and signature recognition) [21]. The worldwide biometrics industry, which was valued at US$5 billion in 2010, is expanding at a CAGR of 18.5 percent and is expected to reach US$17 billion by the end of 2017. According to Deloitte43, by the end of 2017, there will be one billion smartphones equipped with fingerprint scanners in use. Nonetheless, by 2018, iris and face recognition will begin to compete with fingerprint recognition.

VI. CONCLUSION

This paper demonstrated how identity and access management play a critical role when IoT devices are integrated. IoT devices provide unprecedented access to a wealth of useful data. As a result, identity management's involvement in IoT design must incorporate strong data security measures. Without a framework of trust, the IoT will remain unmanageable and unsafe. The industry is interested in who connects to their networks and what they do while connected. If the industry wants to safeguard itself against the most serious dangers facing it today, an effective IAM for IoT must be developed. This article discusses options that claim to address the issue of providing an IAM for IoT. With a little more testing and study of the suggested technologies, a clear route to creating a cryptocurrency PKI IAM for IoT may be achieved. Rather than relying on a CA server that needs records, management, and upgrades, and constructed on a blockchain that is distributed among thousands of machines. Cryptocurrency offers a decentralized and infrangible worldwide computer system without depending on third parties to integrate a trust chain into an RFID-based blockchain PKI architecture. Any future development should incorporate cloud-based integration, as the industry shifts more and more to the cloud. The development of IoT identity and access management is handled via the integration of modern methods.

REFERENCES

[1] S. Ganguli and T. Friedman. (2017). IoT Technology Disruptions: AGartner Trend Insight Report (Report ID G00331334). [Online]. Available: https://www.gartner.com/en/doc/3738060-iot-technology- disruptions

[2] F. J. M. Thomas, J. S. Pasquier, and J. Bacon, “Clouds of things needinformation flow control with hardware roots of trust,” in Proc. IEEE 7th International Conference on Cloud Computing Technology andScience, Vancouver, BC, Canada, 2015, pp. 468-470.

[3] V. Zimmer and M. Krau, (2016). Establishing the Root of Trust. [Online]. Available: http://www.uefi.org/sites/default/files/resources/ UEFI%20RoT%20white%20paper_Final%208%208%2016%20% 28003%29.pdf.

[4] J. C. Asenjo, Three Reasons why You Need a Root of Trust whenOrchestrating Machine Identities, San Jose, CA: Thales eSecurity, 2017.

[5] G. Goth, "Identity management, access specs are rolling along", IEEE Internet Computing, vol. 9, no. 1, pp. 9-11, 2005.

[6] D. Li, R. Zhang, Y. Dong, F. Zhu and D. Pavlovic, "A Multisecret Value Access Control Framework for Airliner in Multinational Air Traffic Management", IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1853-1867, 2017.

[7] Y. Zhang and J. Wen, “The IoT electric business model: Usingblockchain technology for the internet of things,” Peer-to-PeerNetworking and Applications, vol. 10, no. 4, pp. 983-994, 2017.

[8] M. A. Thakur and R. Gaikwad, “User identity and access management trends in IT infrastruture–An overview,” in Proc. InternationalConference on Pervasive Computing (ICPC), Pune, India, 2015, pp.1-4.

[9] A. Sharma, S. Sharma, and M. Dave, “Dentity and access management –A comprehensive study,” in Proc. International Conference on GreenComputing and Internet of Things (CGCIoT), Noida, India, 2015, pp.1481-1485.

[10] S. Matsumoto, R. M. Reischuk, P. Szalachowski, T. H. Kim, and A. Perrig, “Authentication challenges in a global environment,” ACMTransactions on Privacy and Security, vol. 20, no. 1, pp. 1-38, 2017.

[11] P. P. Rahoof, L. R. Nair, and T. Ijyas, “Trust structure in public keyinfrastructures,” in Proc. 2nd International Conference on Anti-CyberCrimes (ICACC), 2017. [11] Y. Ma, “Research on the solution of PKI interoperability based onvalidation authority,” in Proc. International Conference on ComputerScience and Service Ssytem (CSSS), Nanjing, China, 2011, pp. 697-700.

[12] M. Denis, J. C. Leon, E. Ormancey, and P. Tedesco, “Identity federation in openstack – an introduction to hybrid clouds,” Journal ofPhysics: Conference Series, vol. 664, no. 2, 2015.

[13] D. Gritzalis, R. Nithyanand, G. Tsudik, and E. Uzun, “User-aidedreader revocation in PKI-based RFID systems,” Journal of ComputerSecurity, vol. 19, no. 6, pp. 1147-1172, 2011.

[14] B. Abdolmaleki, K. Baghery, B. Akhbari, and M. R. Aref, “Cryptanalysis of two EPC-based RFID security schemes,” in Proc. 12th International Iranian Society of Cryptology Conference onInformation Security and Cryptology (ISCISC), Rasht, Iran, 2015, pp. 116-121.

[15] A. Asaduzzaman, S. Masumder, and S. Salinas, “An auspicious secureprocessing technique for near field communication systems,” in Proc. IEEE 7th Annual Ubiquitous Computing, Electronics, & MobileCommunication Conference (UEMCON), New York, 2016, pp. 1-6.

[16] A. Asaduzzaman, S. Mazumder, S. Salinas, and M. F. Mridha, “A security-aware near field communication architecture,” in Proc. International Conference on Networking, Systems and Security(NSysS), Dhaka, Bangladesh, 2017, pp. 33-38.

[17] T. Plos, M. Hutter, M. Feldhofer, M. Stiglic, and F. Cavaliere, “Security-enabled near-field communication tag with flexiblearchitecture supporting asymmetric cyptography,” IEEE Transactionson Very Large Scale Integration (VLSI) Systems, vol. 21, no. 11, pp. 1965-1974, 2013.

[18] N. Kshetri, “Can blockchain stregthen the internet of things,” ITProfessional, vol. 19, no. 4, pp. 68-72, 2017. [20] C. Robey, “Whom do you trust? Part 2 blockchain technology & smartcontracting,” Contract Management, McLean, VA: National ContractManagement Association, 2017.

[19] J. Cheng, L. Narn, C. Chien, and C. Yi-Hua, “Blockchain and smartcontract for digital certificate,” in Proc. IEEE International Conference on Applied System Innovation, Chiba, Japam, 2017, pp. 1046-1051.

[20] S. Matsumoto and R. Reischuk, “IKP: Turning PKI around withdecentralized automated incentives,” in Proc. IEEE Symposium onSecurity and Privacy (SP), San Jose, CA, USA, 2017, pp. 410-426.

[21] L. Ducas, V. Lyubashevsky, and T. Prest, “Efficient identity-based encryption over NTRU lattices,” in Advances in Cryptology—ASIACRYPT 2014, P. Sarkar and T. Iwata, Eds., pp. 22–41, Springer, Berlin, Germany, 2014.