



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**PKI: THE KEY TO SOLVING THE INTERNET OF
THINGS SECURITY PROBLEM**

by

Lisa M. Gebreamlak

June 2020

Thesis Advisor:
Second Reader:

Glenn R. Cook
Steven J. Iatrou

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE June 2020	3. REPORT TYPE AND DATES COVERED Master's thesis	
4. TITLE AND SUBTITLE PKI: THE KEY TO SOLVING THE INTERNET OF THINGS SECURITY PROBLEM			5. FUNDING NUMBERS	
6. AUTHOR(S) Lisa M. Gebreamlak				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) The concept of combining computers, sensors, and systems to monitor and control gadgets has been around for decades; however, the Internet of Things (IoT) was not born until a few years ago. The IoT, which is an omnipresent cluster of devices bound to the Internet, has, on a fundamental level, altered the way the public thinks about what it implies to be online. The IoT, which guarantees a progressive, completely interconnected "smart" world with connections between objects and their environment and objects and people, is becoming more firmly interlaced in the global sphere. While the potential benefits are numerous, some challenges may yet stand in the way of broader adoption of the IoT. This thesis examines a few of the issues related to the IoT. It also examines the significance of Public Key Infrastructure (PKI) and why PKI should be considered the key to solving the security, privacy, and authenticating risks of the IoT.				
14. SUBJECT TERMS Public Key Infrastructure, Internet of Things, security, digital certificates, encryption			15. NUMBER OF PAGES 137	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**PKI: THE KEY TO SOLVING THE INTERNET OF THINGS SECURITY
PROBLEM**

Lisa M. Gebreamlak
Lieutenant Commander, United States Navy
BA, State University of New York at Binghamton, 1995

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN NETWORK OPERATIONS AND TECHNOLOGY

from the

**NAVAL POSTGRADUATE SCHOOL
June 2020**

Approved by: Glenn R. Cook
Advisor

Steven J. Iatrou
Second Reader

Thomas J. Housel
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The concept of combining computers, sensors, and systems to monitor and control gadgets has been around for decades; however, the Internet of Things (IoT) was not born until a few years ago. The IoT, which is an omnipresent cluster of devices bound to the Internet, has, on a fundamental level, altered the way the public thinks about what it implies to be online. The IoT, which guarantees a progressive, completely interconnected “smart” world with connections between objects and their environment and objects and people, is becoming more firmly interlaced in the global sphere. While the potential benefits are numerous, some challenges may yet stand in the way of broader adoption of the IoT. This thesis examines a few of the issues related to the IoT. It also examines the significance of Public Key Infrastructure (PKI) and why PKI should be considered the key to solving the security, privacy, and authenticating risks of the IoT.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	PROBLEM STATEMENT	3
B.	PURPOSE STATEMENT.....	4
C.	RESEARCH QUESTIONS.....	4
D.	POTENTIAL BENEFITS AND LIMITATIONS.....	5
E.	HYPOTHESIS.....	5
II.	LITERATURE REVIEW	7
A.	EMERGENCE OF THE IOT	7
B.	THE EVOLUTION OF THE IOT	9
C.	UNDERSTANDING THE IOT	13
D.	POTENTIAL IOT OPPORTUNITIES.....	15
E.	ISSUES PRESENTED BY THE IOT	22
	1. Security Issues	22
	2. Potential Threats Unique to IoT Devices	24
F.	PRIVACY ISSUES IN THE IOT	30
G.	INSECURITY IN THE IOT	35
H.	PKI: A STRONG SECURITY FOUNDATION	40
	1. Uses of PKI	42
	2. Challenges of PKI	45
	3. Defining Business Needs	45
I.	LOGICAL COMPONENTS OF A PKI	46
	1. PKI Framework	46
	2. Trust Models.....	47
	3. PKI Security Services	47
J.	PKI PARTICIPANTS	50
	1. Subscribers	50
	2. Relying Parties	51
	3. Registration Authority (RA)	51
	4. Certification Authority (CA)	52
	5. PKI Hardware Security Modules (HSM)	57
	6. Public Key Certificates	59
	7. Certificate Extensions	61
	8. Certificate Depositories (CDs)	62
K.	PKI FUNCTIONS.....	62
	2. Hash Functions.....	64
	3. Symmetric Key Encryption.....	65

4.	Asymmetric Key Encryption	66
5.	Key Separation	67
L.	PUBLIC KEY CERTIFICATE BINDING	69
1.	Entity Authentication	69
2.	Certificate Generation	70
3.	Acquiring the Public Key	70
4.	Verifying the Identify of the End Entity	70
5.	Formatting the Certificate	70
6.	Signing the Certificate	71
M.	PKI'S FLEXIBLE DEPLOYMENT	71
N.	AN EXAMPLE OF A PKI IN ACTION.....	73
O.	PKI FOR MOBILE, CLOUD AND IOT	78
P.	PKI AVAILABILITY AND SCALABILITY	80
Q.	POTENTIAL PKI AND IOT CHALLENGES	81
1.	Physical Security	81
2.	Device Integrity	81
3.	Data Security	81
III.	METHODOLOGY AND FINDINGS	83
A.	METHODOLOGY	83
B.	FINDINGS	85
1.	Survey Respondent Demographics.....	85
2.	Analysis of Survey Responses	86
3.	Analysis of Interview Responses.....	91
IV.	CONCLUSIONS AND RECOMMENDATIONS.....	93
A.	CONCLUSIONS	93
B.	RECOMMENDATIONS.....	98
1.	Business Enablement	99
2.	Technical Enablement	99
3.	Recommendations for IoT Stakeholders	100
C.	CONCLUSION	106
	APPENDIX. SURVEY AND INTERVIEW QUESTIONS.....	107
	LIST OF REFERENCES.....	109
	INITIAL DISTRIBUTION LIST	121

LIST OF FIGURES

Figure 1.	The IoT Was “Born” between 2008 and 2009. Source: Evans (2011, p. 3).	2
Figure 2.	IoT Can Be Viewed as a Network of Networks. Source: Evans (2011, p. 4).	22
Figure 3.	IoT Security Challenges. Source: Nachappa et al. (2018, p. 2).	29
Figure 4.	CA Hierarchy. Source: Afshar (2015, p. 7).	54
Figure 5.	CA Certificates Installed on the Author’s Web Browser.....	54
Figure 6.	Symmetric Encryption. Source: TipTopSecurity (2017).	65
Figure 7.	Asymmetric Encryption. Source: TipTopSecurity (2017).	67
Figure 8.	Structure of a X.509 Digital Certificate. Source: Afshar (2015, p. 11).	71
Figure 9.	PKI Components. Source: Afshar (2015, p. 6).	73
Figure 10.	Overview of Using a Digital Signature. Source: Weise (2001, p. 25).	74
Figure 11.	Overview of the Decryption and Hash Comparison Process. Source: Weise (2001, p. 26).	76
Figure 12.	PKI Process to Issue Digital Certificates. Source: Dener et al. (2011, p. 122).	76
Figure 13.	Working of Digital Certificates. Source: Afshar (2015, p. 14).	77
Figure 14.	Accurate Response Rate for Open-Ended Survey Questions	87
Figure 15.	Technique Best Suited for Revocation of Digital Certificates.....	88
Figure 16.	Preferred Framework to Solve IoT Security Risks	89
Figure 17.	PKI is effective for the IoT	90
Figure 18.	PKI is effective on the IoT.....	91

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AA	Attribute Authority
API	Application Programming Interface
CA	Certification Authority
CDP	CRL Distribution Point
CRL	Certificate Revocation List
DC	Digital certificates
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GSM	Global System for Mobiles
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IT	Information Technology
ICT	Information and Communication Technologies
M2M	Machine to Machine
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
RFID	Radio-Frequency Identification
WI-FI	Wireless Fidelity

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This paper is dedicated to my children and to all the people who contributed their time and effort to this project.

I thank Mr. Glenn Cook, my thesis advisor, for his support, guidance, and encouragement.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The growth rate for the use of digital certificates (DCs) is significant, and many innovators recognize the high value of these certificates in identity authentication, data integrity, and confidential management of data, devices, and identities which make up the IoT. Singh (2018) argues that modern advancements in technology have made the world more reliant on the Internet, which is a unique global network that enhances communication systems. People use devices such as smartphones, tablets, laptops, and personal computers (PCs) to send electronic mail (email), and messages as well as post content on social media using the Internet. All these activities are enabled by IoT, which is a fundamental science that works on devices, interconnectedness, and collected data.

The rapid advancement in IoT has led to the emergence of automated systems that utilize human interaction and has the potential of changing human lives by enhancing our efficiency. Today, many companies are deploying devices and establishing systems of the IoT at people's homes, offices, and other institutions, allowing access to data remotely and creating a high level of convenience. Furthermore, Liping and Lei assert,

The world today is the network of the world, the network is an unprecedented impact on the production of human, scientific research, education, military, economy and trade, medical insurance, cultural and entertainment aspects of social life. More and more people recognize that the network is not only the information platform but also a very convenient platform for transaction processing applications. (2011, p. 1).

Gershenfeld, Krikorian, and Cohen (2004) define IoT as a unique technology that offers both a microscope and telescope into a world that was once invisible by creating links between people, physical objects, and machines. Lee and Lee (2015, p. 1) believe “the IoT, also called the Internet of Everything or the Industrial Internet, is a new technology paradigm envisioned as a global network of machines and devices capable of interacting with each other. The IoT is recognized as one of the most critical areas of future technology, and is gaining vast attention from a wide range of industries.” Data movement over networks is secured from unauthorized access. The IoT system combines objects directly with the Internet, enhancing the rate of tracking, collecting new data types, and

combining these data types to generate higher data and knowledge levels. It thus enables the movement of highly sensitive information such as online banking information or personal information belonging to people transacting over the Internet and has led to the development of smart devices that are connected to a network and the resulting interconnection of said devices.

As of now, the IoT has gone beyond what data scientists fathomed only a few years ago. Greengard (2015) thinks that IoT functions to connect machine and human intelligence in seemingly scary and entirely remarkable ways; the system possesses the ability to explain motions between people and among things, including vehicles, viruses, air currents, and animals. The capability of the IoT surpasses that of the human mind and sense, since it can detect the physics of the atmosphere, and can predict the patterns of a bridge or a roadway. Another unique feature is that IoT can support systems that work independently of human interventions and oversight and, on their own, become more efficient over time by embracing a fundamental algorithm. Figure 1 shows the rate of increase of Internet-enabled devices from inception and forecasted to the 2020 timeframe.

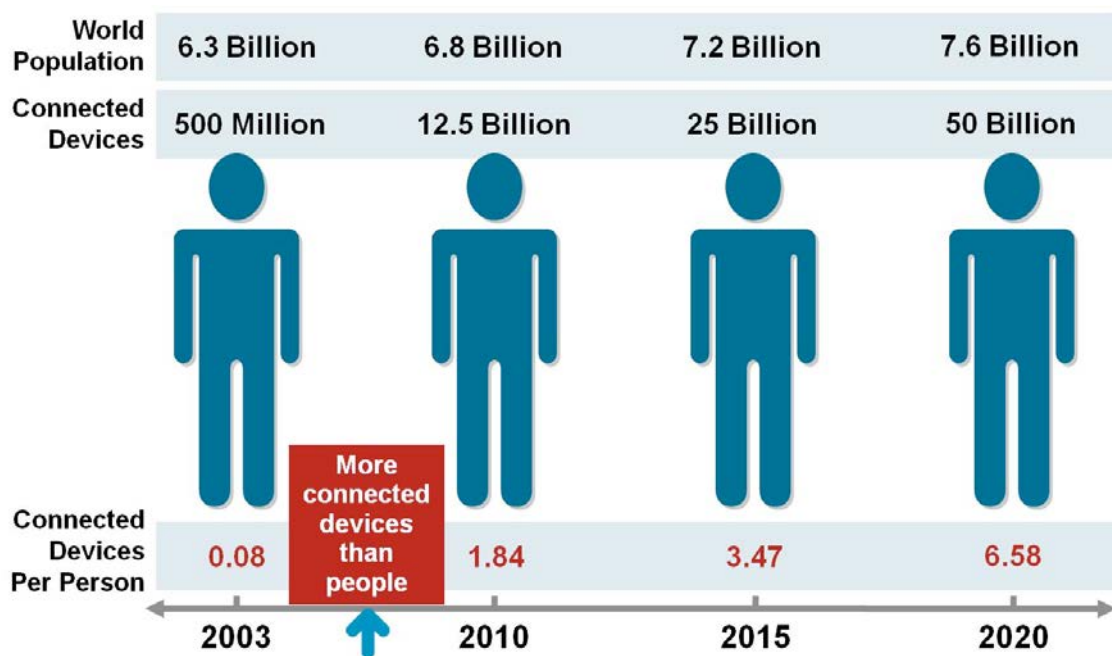


Figure 1. The IoT Was “Born” between 2008 and 2009. Source: Evans (2011, p. 3).

Despite the different benefits associated with the advancement in technology and the use of IoT, the technology has been highly vulnerable to a group of hackers who prey on any possible loopholes, particularly unprotected networks. According to Dinha (2018), in 2018, the attacks on IoT shot to 280%, because hackers were becoming more tech-savvy. This dramatic rise in hacking calls for immediate action to protect IoT systems from malicious users. In this evolving world of IoT, an extra layer of security is provided by DCs—which are efficient and cost-effective—and work impressively.

In summary, the IoT is still a technology in its early stages but is slowly developing to become a significant phenomenon in the world of technology. However, some of the shortcomings of this technology include the use of Low power and Lossy Networks (LLNs) that hinder the success configuration of security. This technology requires advanced security options that are available through the application of PKI systems. This paper seeks to establish the effectiveness of using PKI as a method of providing security, confidentiality, privacy, integrity, and authentication of communications.

A. PROBLEM STATEMENT

There are perhaps already billions of devices currently connected to critical systems and the Internet. This mass deployment of smart gadgets and devices results in security risks, which only grow with the number of deployed devices. Therefore, IoT security must be adequate, which involves the implementation of correct security development and smart device deployment. The task involves three vital elements that revolve around the establishment of trust: personal and data privacy, adherence to critical maintenance and standards, and core device security. These trust elements are crucial for the current threat landscape and for future system and products' life cycle challenges, which might inhibit the success of these frameworks. The IoT requires a security level that can deliver the much-needed encryption and authentication components that the IoT needs to ensure data security. Limited literature exists on this subject of security provision for IoT projects. Thus, immediate action needs to be taken to address this widespread challenge in information and communication technologies (ICTs). Any empirically generated and reliable findings could be highly instrumental both to scholars and to the practitioners.

B. PURPOSE STATEMENT

This research is design to, among other goals, to establish why PKI has been labeled one of the world's best critical security management systems underlying IoT technology which ensures the security of transactions and identities today. Consequently, users have complained that PKI does not offer a standardized, proven, scalable technology that processes and helps create a trusted environment for their IoT, or even manage the identities present in the IoT, both human and nonhuman. This thesis seeks to understand the impact of PKI on the IoT and whether it is significantly helpful. The thesis will explain in detail whether PKI can be a well-trusted ecosystem that can keep untrusted entities outside of the IoT networks. Additionally, the research will offer explanations about whether the PKI security platform eases the placement of IoT products into the market.

Lastly, this research will work to establish that PKI not only secures IoT devices but also helps people to engage securely in a world where individuals are nearly always engaged in a form of a connected computing environment. The study will also show how PKI makes businesses and people more connected and agile, which could have a profound impact on the way we work, play, and live. Lastly, it will examine some of the early misconceptions about PKI technology.

C. RESEARCH QUESTIONS

This study will be guided by the following research questions:

- What is the significance of PKI on the IoT?
- Can PKI solve the security, privacy, and authentication risks of the IoT objectives?

Having the above research question should permit the research to meet the obligations and requirements of the following research objectives:

- To investigate the significance of applying PKI on IoT
- To establish if PKI can solve IoT security, privacy, and authentication risks

D. POTENTIAL BENEFITS AND LIMITATIONS

This research will explore the potential expansion of PKI applications, as they could provide new “ultimate” security opportunities, especially for systems that rely primarily on the Internet. This research’s findings will, therefore, be fundamental in providing information on the significance of extra security measures in the IoT, such as the use of PKI. The findings will also inform research and policy about device connectivity and communication through the Internet.

Although this study is expected to generate practical measures in enhancing security in the IoT, there are known limitations. Factors such as the lack of access to a larger pool of firsthand information will significantly influence the study’s outcomes. Therefore, the research will rely on responses from surveys and interviews for the generation and analysis of data.

E. HYPOTHESIS

The key hypotheses in the study are:

- HO: PKI does not influence the privacy and security aspects of the IoT.
- HA: PKI positively influences the privacy and security aspects of the IoT.

Chapter I largely embarked on understanding the meaning of the key concepts discussed in the paper. Also, the chapter sets boundaries for the study by establishing the primary research questions and critical objectives. While IoT is a unique technology that offers both microscopic and telescopic solutions by creating links between people, physical objects, and machines, PKI is a particular type of cybersecurity that secures communication between multiple computers by creating, managing, distributing and revoking of DCs and public keys. This research study will investigate the significance of applying PKI on IoT as well as establish whether PKI can solve security, privacy, and authentication risks on IoT. The following section reviews relevant literature about the significance of PKI on IoT. It makes outstanding contributions to the understanding of the concepts and their applicability in the day-to-day running of organizations.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

A. EMERGENCE OF THE IOT

According to Miorandi, Sicari, DePellegrini, and Chalamtac (2012), before the IoT, individuals communicated with other individuals and with machines. For instance, if all the equipment belonging to a person was able to communicate, what kind of information would it be able to give? Objects that are IoT-enabled will provide information regarding the kind of conditions they are under as well as their environment with individuals, other machines, and software systems. This data can otherwise be shared in real-time or can be gathered and shared at intervals that are defined. Everything will possess digital connectivity and identity, which means one can track, identify, and communicate with objects.

According to Foote (2016), until recently, there was no notion of IoT, although there have been visions of machines communicating to each other since the early 1800s. Zou, Guo, Zeng, and Shi (2011) think communication between machines started with the development of the telegraph in the 1830s, followed by radio transmission in 1900. The two inventions formed a critical basis for the emergence and growth of the IoT. Foote (2016) claimed that the Internet is a critical aspect of IoT, begun in 1962 as part of the Defense Advanced Research Projects Agency. By 1969, it had grown to ARPANET, which later evolved into the modern Internet. It is important to note that while the IoT is currently considered cutting-edge technology in the IT industry, this technology is not based on new concepts.

Foote (2016) asserts that it was the British entrepreneur, Kevin Ashton, who laid the footing for what was going to develop into the IoT. He claimed that Ashton, who believed “the IoT had the potential to change the world”; from Ashton’s perspective, the concept of the IoT was “simple yet powerful.” Ashton is among the pioneers who brought IoT into being by creating a link between Radio-Frequency Identification (RFID) information and the Internet. He believed the IoT would offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications and

covers a verity of protocols, domains, and applications (Foote, 2016). In the IoT, the sensors embedded in devices are linked through wired and wireless networks. In 1999, Ashton's vision of RFID-based device connectivity differed drastically from the current IP-based IoT. For example, critical components of the underlying technologies required for IoT such as GSM, BlueTooth, Wi-Fi networking, NFC, and EnOcean, massive data storage for real-time sensor data, vast numbers of super-fast computers to process and analyze the data, and high-performance automated applications and advanced software systems to manage those applications were still in their infancy.

Notwithstanding the limitations of the time, Ashton's innovation and groundbreaking ideas played a pivotal role in the overall technological development of the IoT. In fact, according to Sundmaeker, Guillemin, and Friess (2010), the technological advancements that Ashton's vision needed have since been solved. Since 1999, interconnected devices have become prevalent and routine in our everyday lives. Silicon Valley tech giants like Google, Apple, Cisco, and Samsung are focusing their efforts on the production of IoT sensors and devices. For example, millions of devices with wireless connectivity capabilities have been invented, and over the years, the data coverage of mobile devices has improved exponentially, with most networks being able to offer broadband speeds. According to Stankovic (2014), many objects can now connect to the Internet. For instance, a recent addition to the IoT system connects smartphones to a doorbell, such that the ring sends signals when the doorbell is pressed, and offers an opportunity to speak and even see the individual on the smartphones' screen. Also significant is the 2011 development of Internet Protocol version 6 (IPv6)—a network layer protocol that is vital to IoT was launched publicly.

According to Weber (2011), the IoT is a technological system associated with our current devices and gadgets, or sensors that are attached to or within these items, which connect to the Internet with cables or wirelessly. Lopez (2013) indicates that the sensor will use numerous types of local area networks, for example, Wi-Fi, RFID, Near Field Communication (NFC), Zigbee, and Bluetooth. These sensors may also possess wide-area connectivity, for example, General Packet Radio Service (GPRS), Global System for Mobiles (GSM), Long-term evolution (LTE), and 3G.

The work of Gershenfeld et al. (2004) suggests that the early deployments and trials of the IoT networks started through the connection of industrial equipment. The IoT vision has expanded to the point of connecting everything from industrial tools to everyday objects, ranging from the utility meters of gas turbines to automobiles. It may also incorporate living things, for example, people, plants, and farm animals. In his work, Kumar (2016) discusses the example of the Cow Tracking Project conducted in Essex, which used information from tags used for radio positioning to check cows for sickness and track their behavior in herds. Wearable digital health and computing devices, such as the Fitbit and the Nike+ Fuel band, are excellent demonstrations of how people stay connected to the landscape of the IoT.

In short, anything a person possesses that has connectivity, and a sensor can participate in the connected ecosystem. Atzori, Iera, and Morabito (2010) believe the use of sensors to collect data on the physical equipment which is undergoing connection will contain either a single or more sensors. Each of these sensors will monitor a particular condition such as motion, vibration, temperature, and location. These sensors will, in the IoT, be linked together and with systems, which comprehend or present data from the data feeds of the sensors. These sensors will provide new data to individuals, as well as to the systems of companies.

B. THE EVOLUTION OF THE IOT

Before the Internet became the always-connected global phenomenon it is today, it underwent several radical changes. According to Chase (2013), the proliferation of the Internet began in the 1990s, and its impact was immense despite underutilization at the time. This underutilization, Chase believes, was because most people did not understand the global Internet's full capabilities and, it was limited in coverage and performance. Zhao (2014) thinks the Internet became a regular part of human life as a platform for things such as communication and a source of business and entertainment in the 2000s. However, we may not have moved beyond the antiquated methods of early communication, was it for the remarkable influence of a researcher working at CERN, the European Particle Physics Laboratory, in 1989. Tim Berners-Lee is credited with coming up with the concept of the

World Wide Web (WWW) and building the first web page in 1993 because he wanted a decentralized repository of information that was linked together and shareable with anyone who could connect to it (McPherson, 2009).

Later, seeing the value in what Berners-Lee and his team had created, CERN made the software for the WWW open-source, meaning anyone in the public domain could use it (without cost) and hopefully build on it (Berners-Lee, Cailliau, Luotonen, Nielsen, & Secret, 1994). National Center for Supercomputing Applications (NCSA) Mosaic, or simply Mosaic was developed at the University of Illinois Urbana-Champaign beginning in late 1992; it is the web browser credited with popularizing the WWW (Schatz, & Hardin, 1994). However, although Mosaic was groundbreaking, it wasn't until a group of former University of Illinois at Urbana-Champaign students left the UIUC facility to start Netscape that the web started to take off. It was the former students led by Marc Andreessen that created Netscape Navigator, the first web browser many people had ever used.

Moreover, according to the April 2009 survey conducted by the Pew Research Center's Internet & American Life Project, some "63% of adult Americans had broadband internet connections at home." (Horrigan, 2009, p. 9). More users liked broadband because it was relatively inexpensive, the connection stayed up even when not in use, and perhaps more important, the vast majority of broadband connections came into homes through the same connection used for cable TV, so users tended not to require a telephone line to connect (Horrigan, 2009).

Today, the Internet is an excellent feature of consumers, industry, and government, as it serves as a reliable and useful source of information. Today, connectivity among devices still requires a level of human interaction. However, the technology also promises invisible technology that will allow operations of the Internet and other resources with limited human interaction. Ning and Wang (2011) assert that the IoT of tomorrow is expected to be highly advanced, and it will have the capacity to handle human activities with minimal human interaction, as devices will be able to detect a signal and receive information analysis and take actions. However, in today's world, systems of technology with structures of data and protocols are quite complex. They are also limited in terms of

the level of security needed, and effectiveness. However, as time goes by, complexities will reduce.

Greengard (2015) argues that the development of IoT was the second wave of the digital revolution, whose beginning was marked by a widespread computer adoption in the 1970s and 1980s. Among the many prospects of technology, IoT is expected to introduce new products and services as well as outdo many current market options. During the introduction period, the technology was expected to bring about remarkable changes in many sectors of the economy and thus affect every aspect of human life, including voting practices, taking vacations, and taking meals in restaurants. Although it is not easy to tell what exactly would IoT turn the world to be, scholars have predicted that it will end up creating a more technology-centric world. Humanity will experience tremendous changes with the rise in technology use. Some changes will include living in automated homes, connecting to medical products and wellness from home, and drive vehicles on networked roads (Greengard, 2015).

Fettweis (2016) thinks as machine-to-machine connectivity continues to advance, more and more products will be fitted with web servers to allow the secure connection. He suggests that in the past, machine-to-machine connection systems were complicated to develop, but some companies still managed to develop them for their operations. Boualouache, Nouali, Moussaoui, and Derder (2015) claim that advancements in technology have allowed for more development in powerful processors whose applications have expanded. According to Chase (2013), powerful processors, coupled with their capacity to support high-level languages of programming and sophisticated operating systems, have opened up a path for IoT applications in an extensive array of devices.

Specifically, systems in homes, offices, and businesses are developing smart appliances capable of detecting and storing information. According to Chase, these systems can be connected to the Internet, and users can remotely manage and monitor the systems from wherever they are and include:

- Automated swimming pool systems
- Automatic lighting systems
- Automatic security systems

- Automatic sprinkler systems. (Chase, 2013, p. 5)

Despite these existing technologies, there is much inconsistency hindering the successful deployment of such technologies. Such inconsistencies are associated with the lack of proper coordination between different organizations. They are systems made up of different components, all made by the different organizations, and their establishment is based on a system of coordination among all the organizations (Chase, 2013). Lack of consistent communication layers coupled with differences in interfaces makes it very hard to establish cross-application usage. A successful system needs a simple way through which the programs run on the devices consistently, enabling them to respond to the other devices.

Uchihiro, Ishimatsu, and Inoue (2016) think the Internet is a vital element of the IoT. However, they also believe Internet technology has not always been open, and it has led to the development of new service needs such as messaging that the public got access to such a vast platform of connectivity. Before the development of the Internet, networks existed for the services of enterprises, but there was no form of sharing. Government systems also had their networks, and these systems are what evolved to become the Internet.

According to Chase (2013), the Internet grew from simple communication needs such as messaging to complex systems of movement of time-critical data and the media, which requires a system of power management. Gubbi, Buyya, Marusic, and Palaniswami (2013) addressed the issue of power management because devices require reliable sources of energy and, their portability will limit them to batteries. They maintained that power management needs to be very well thought-out because they have to be sustainable and energy-efficient. The devices also have to be developed with platforms that can allow connectivity between them, and this will necessitate the development of complex hardware systems that incorporate powerful chips as well as for as strong interfaces that can handle complex programs and apps to run the system (Chase, 2013).

Gubbi et al. (2012) argue that although the industry is still young, the evolution of the IoT has been rapid, and more devices are coming out each year. Gubbi et al. believe

the true potential of the IoT has not yet been realized, but the capabilities are vast, and the technology promises to grow even more. Deif and Gadallah (2017) anticipate that technological advancement will significantly change the lives of human beings across the world due to the application across almost all sectors of the economy. Accordingly, all the applications will be applied to advance human life's specific features, making the world safer and more efficient. Furthermore, businesses will significantly benefit from these technologies, as connectivity to systems of businesses will be made more accessible through the use of mobile devices. Businesses will become efficient and become more intelligent, thanks to a combination of services from smart equipment and efficient operations, which includes remote monitoring of internal systems (Deif & Gadallah, 2017).

C. UNDERSTANDING THE IOT

Chui, Loffler, and Roberts (2010) describe the IoT as technologies that network physical objects together, enabling near real-time information sharing between numerous disparate elements and systems to communicate their location, status, and other vital information to each other and a central system. Chui et al. (2010, p. 1) further describes the IoT as “sensors and actuators embedded in physical objects—from roadways to pacemakers—are linked through wired and wireless networks, often using the same Internet Protocol (IP) that connects the Internet. These networks churn out huge volumes of data that flow to computers for analysis.”

According to Lee and Lee (2015), the IoT is a system of interconnected physical objects that have technology embedded to enhance communication with the outside environment. Pal (2008) and Marburger (2011) say the 21st century has been characterized by a tremendous growth in technology, which has seen the world grow into a global market. Indeed, connectedness in today's world has become the norm, and people from around the globe are living in a connected life. Machine-to-machine connectivity is growing as a crucial aspect of the IoT. The IoT is a system that allows different smart devices to be connected and has the advantage of efficiency, energy conservation, and increased security. It is a technology that is advantageous to both individual consumers as well as enterprises.

However, Ratasuk, Vejlgard, Mangalvedhe, and Ghosh (2016) believe IoT is still in its early developmental stages, and the number of advances needed is quite immense. IoT provides a chance for the establishment of services capable of enhancing the lives of people in diverse segments of the economy. Tahir, Tahir, and McDonald-Maier (2018) believe that IoT is a technology capable of introducing a new way of life. They believe IoT is a system that will necessitate the development of global distribution systems because the services expected from this technology are also expected to attract demand on a global scale. Successful implementation of IoT will develop new commercial models because of high demand, which will transform the communication and smart device industry. According to Yang, Wang, Xie, and Zhang (2018), the system is expected to extend to a wide variety of sectors in the economy, including education, health, military, and many others.

Likewise, Ratasuk et al. (2016) believe that the digital ecosystem that circles about the highly progressive application development will also require reconfiguration to meet the necessities of a wide variety of gadgets and devices that are interconnected. It is a network system that will enable devices to communicate and network with each other independently of humans. It will significantly enhance the efficiency of and lead to the development of new revenue streams for organizations. One of its popular systems currently in existence is associated with the machine to machine connectivity, which is a less sophisticated aspect of the system that is gradually growing.

Furthermore, according to Zhang and Yu (2013), globalization and high consumerism are aspects expected to push the demands and supply of smart devices across the world. They argue that services from systems of the IoT will require specialized distribution systems that are consistent with global business systems and demand for this system, and technology is vast because of its global scale. The other aspects are associated with the need for coordination between vendors, Mobile operators, and manufacturers. Socioeconomic impacts on customers and the general public concerning the development of the system have been very positive. This is based on the ability of the system to create a connected life that can improve the lives of the people: how they live as well as the way they work.

Indeed, if the IoT is going to be successful as Olssen, Codd, and O'Neill (2004) argue, concerned parties must come together and find coordinated ways of meeting the needs of global consumers, while simultaneously providing them with positive and consistent customer experiences. Equally important, different aspects of business and management have to be well organized and coordinated. Partnerships and alliances have to be well-established to ensure that all players benefit from each other. Mobile operators have taken the lead in the provision of global services associated with the technology. However, the services they are currently providing are a glimpse of what economies expect to form the technology.

If the demands of many sectors of the economy are to be met, as Govinda and Saravanaguru (2016) suggest, extensive work is generally required to develop and implement IoT systems. Likewise, Yeh and Lin (2018) assert that new commercial models have to be established to satisfy the requirements of global dissemination and also global demands for centralized forms of services. Mobile networks will have higher demands from different devices. The IoT promises excellent technological advancements and high levels of productivity and success for individual consumers and enterprises.

According to Miorandi, Sicari, DePellegrini, and Chalamtac (2012), before the IoT, individuals used technology to communicate with other individuals and with machines. The IoT begs the question: If all the equipment belonging to a person was able to communicate, what kind of information would it be able to give? Objects that are IoT-enabled will provide information regarding the kind of conditions they are under as well as their environment with individuals, other machines, and software systems. This data can otherwise be shared in real-time or can be gathered and shared at intervals that are defined. Everything will possess digital connectivity and identity, which means one can track, which means one can track, identify, and communicate with objects.

D. POTENTIAL IOT OPPORTUNITIES

Innovations in the first significant benefit IoT has brought about include enhanced communication. Given the advancement of platforms transmitting messages to satisfy the necessities of the multifaceted systems of IoT, the movement of information will remain

extremely well-organized. New systems of communication, such as sensors and monitors, which will be put in place as part of the services of IoT, will enhance access to information from various aspects of human lives. All of these are systems that provide information that can improve people's lives. These include:

- Location information
- Automatic lighting systems
- Automated security systems
- Automated health systems and many others

According to Mandula, Parupalli, Murty, Magesh, and Lunagariya (2015), the other critical aspect of IoT is associated with enhanced control of systems as a result of automation. Automation means that IoT systems will be complicated, and one aspect is that they will be intelligent, meaning that they will require minimal human interaction. This is an aspect that will provide greater control, which will now be put on more careful and precise systems. Enhanced control is also possible, boosting the ability of people to control systems remotely. Chase (2013) argued that a connected world means that access to devices and information will be high, and people will have more control over many aspects of their lives. Businesses will have more control over systems in their organization, and life will be made easier thanks to automation.

The third benefit of the IoT, according to Dijkman, Sprenkels, Peeters, and Janssen (2015), is associated with cost reduction and increased efficiency. The systems of IoT will allow individuals and organizations to make actual measurements of systems rather than using estimates, and this will have an impact on cost. IoT systems can reduce system failures. Chase (2013) added that through the use of monitors and sensors, businesses and individuals could easily monitor their homes and businesses. With IoT, saving costs are manageable, and efficiency is enhanced. Figure 2 depicts the interconnectedness of the IoT.

Furthermore, Chui et al. list six diverse types of emerging IoT applications, which fall into two broad categories: first, information and analysis, and, second, automation and control:

Information and Analysis. As the new networks link data from products, company assets, or the operating environment, they will generate better information and analysis, which can significantly enhance decision-making. According to Chui et al., some organizations are starting to deploy these applications in targeted areas, while more radical and demanding uses are in the conceptual or experimental stages.

1. **Tracking Behavior.** As products are embedded with sensors, companies can track the movements of these products and theoretically monitor individual human interaction with them.
2. **Enhanced Situational Awareness.** Data from large numbers of sensors, deployed in infrastructure (such as roads and buildings) or to report on environmental conditions (including soil moisture, ocean currents, or weather), can give decision makers a heightened awareness of real-time events, particularly when the sensors are used with advanced display or visualization technologies.
3. **Senor Driven Decision Analytics.** The Internet of Things also can support longer-range, more complex human planning and decision making. The technology requirements-tremendous storage and computing resources linked with advanced software systems that generate a variety of graphical displays for analyzing data—rise accordingly. (2010, p. 5)

Automation and Control. Making information the premise for robotization and control implies changing over the information and subsequent analysis created through IoT into instructions that feedback through the network to actuators that, in turn, alter processes. Closing the circle from information to robotized applications can raise efficiency, as systems that alter consequently to complex circumstances make numerous human interventions superfluous (Chui et al., 2010).

1. **Process Optimization.** The Internet of Things is opening new frontiers for improving processes. Some industries, such as chemical production, are installing legions of sensors to bring much greater granularity to monitoring. These sensors feed data to computers, which in turn analyze them and then send signals to actuators that adjust processes—for example, by modifying ingredient mixtures, temperatures, or pressures. This improved instrumentation, multiplied hundreds of times during an entire process, allows for major reductions in waste, energy costs, and human intervention.
2. **Optimized Resource Consumption.** Networked sensors and automated feedback mechanisms can change usage patterns for scarce resources, including energy and water, often by enabling more dynamic pricing.

Utilities such as Enel in Italy and Pacific Gas and Electric (PG&E) in the United States, for example, are deploying “smart” meters that provide residential and industrial customers with visual displays showing energy usage and the real-time costs of providing it.

3. **Complex Autonomous Systems.** The most demanding use of the Internet of Things involves the rapid, real-time sensing of unpredictable conditions and instantaneous responses guided by automated systems. This kind of machine decision making mimics human reactions, though at vastly enhanced performance levels. The automobile industry, for instance, is stepping up the development of systems that can detect imminent collisions and take evasive action. (Chui et al., 2010, p. 5)

When considering the full spectrum of possibilities for the IoT, Singh (2018) argues the IoT is a very crucial tool in modern life and characterized by extensive use of the Internet in collecting, disseminating, and exchanging critical information. Moreover, due to its unique ability to create connections with anything that has sensors or software, the IoT has enabled people in this century to automate almost everything. The modern market is invested with new gadgets, which enable us to perform huge tasks by issuing a simple command to a machine. For instance, it has become possible to control electronics at home remotely from long distances.

Ratasuk et al. (2016) suggest that machine-to-machine connections are already in place and perform excellent work in people’s lives. A good example is an interconnection between computers and smartphones, as evidenced by Apple Inc.’s substantial investment in the machine-to-machine connection as an aspect of their service portfolio (Ratasuk et al., 2016). In the same way, the full evolution of machines into the IoT will require coordination between different vendors, devices, and appliances. Despite efforts by Samsung and Apple, no single company can produce such an advanced service; however, more and more mobile operators are developing machine-to-machine connections.

According to Ratasuk et al. (2016), some of the benefits of a connected life as developed by this new technology include; time productivity, energy efficiency, and increased connectivity. Implementation of IoT systems is expected to result in the establishment of new business opportunities and boost economic growth. Höller et al. (2014) believe the system involves a wide range of players, such as vendors and mobile operators. All of them will significantly benefit from the increased economic opportunities

associated with the new technology. It is a system that will create demand for new products and thus develop gaps to be filled by the creation of businesses and the development of new employment opportunities. According to Khan et al. (2012), smart devices are slowly enhancing economy proliferation as sophisticated technologies emerge. (Manyika et al., 2015) notes that their connection as a portion of the IoT is becoming a fundamental characteristic of different economy segments, such as utilities, automotive, communication, health, agriculture, transportation, and housing.

Also, Lee and Lee (2015) assert that the IoT is a technology associated with life-enhancing services. It has various features which set it apart as a significant advancement in technology. Furthermore, they also believe the IoT can increase people's quality of life by increasing the efficiency of various aspects of their lives, including reducing costs and increasing security. Specifically, energy efficiency reduces the costs of energy and other utilities, and connectivity allows people to monitor their houses and businesses remotely and thus help enhance security. Likewise, the IoT can also be used in cities for effective traffic management, efficiency in insurance management, such as through the use of pay as you drive.

In fact, the use of IoT systems in security and healthcare has been instrumental in enhancing service delivery in those sectors (Akhila et al., 2017). Additionally, Istepanian, Hu, Philip, and Sungoor (2011) believe the use of IoT has enhanced the monitoring of patients while at home, leaving space in hospitals for more severe cases. Indeed, multiple technology manufacturers have marketed devices consumer use, and also make it easy for doctors to monitor the vital signs in of patients and respond immediately. For instance, according to Chui et al. (2010, p. 1), "Pill-shaped microcameras [sic] already traverse the human digestive tract and send back thousands of images to pinpoint sources of illness." Multiple technology manufactures have marketed devices that make it easy for doctors to monitor the vital signs in patients and respond immediately. The following are descriptions of current, commercially available medical applications of IoT:

- **Current Health's Artificial Intelligence (AI).** FDA-approved wearable device that measures all vital signs (except blood pressure) in a local hospital setting and the patients' homes. The remote device measures a patient's pulse,

respiration, oxygen immersion, temperature, and mobility, and is most frequently utilized by patients with chronic obstructive pulmonary illness (COPD) and heart failure. It provides precise information concerning respiration and pulse and provides doctors with real-time updates concerning their patient's wellbeing, permitting them to handle complications expeditiously. The innovation utilizes machine learning to analyze the information it collects to distinguish risky changes in data. The company is using its technology to identify and analyze early warning signs for illnesses that rank among the foremost deadly in the U.S. (Carfagno, 2019).

- **VitalPatch.** VitalPatch, developed by VitalConnect, is a health monitoring device in the growing field of TeleHealth. This state-of-the-art biosensor accurately monitors eight physiological measurements continuously in real time. The device measures: Single-lead ECG, body temperature, heart rate, heart rate variability, respiratory rate, body posture, fall detection, and user activity (VitalConnect, n.d.).
- **Nymi.** Is a wristband that relies on authenticating identity by matching the overall shape of the user's heartwave (captured via an electrocardiogram sensor). Unlike other biotech authentication methods—like fingerprint scanning and iris-/facial-recognition tech— the system does not require the user to authenticate every time they want to unlock something so it uses the unique heartbeat to remain continuously logged in to IoT enabled devices so long as the wearer keeps the wristband on. This wearable technology is equipped with an accelerometer and gyroscope to enable user defined gesture control targeting of specific items (Nymi, n.d.).

According to Chen et al. (2017), today, the police are using IoT systems to monitor street cameras and enhance maintenance of law and order. Additionally, the application of IoT system has proved to be extremely fundamental in helping business operators to monitor consumer trends and respond to market demand changes on time (Lee & Lee, 2015). Because most businesses operate in a competitive environment, instant response to

market changes is a surefire way of avoiding losses and increasing sales and maximizing profits and revenues.

Additionally, according to Gupta, Patchava, and Menezes (2015) and Akhila et al. (2017), other applications in cities include energy management and security. They believe the health sector will also greatly benefit from features such as electronic health, useful in monitoring and communicating among different health practitioners. This has a far-reaching impact on improving the quality of health of individuals. As healthcare demands go high, the need for an efficient system becomes paramount, and connected smart devices provide an excellent opportunity for enhancing the provision of health services (Ruggeri & Briante, 2017; Prakashan et al., 2017). According to Tianbo (2012), the education system is also going to experience significant developments; smart devices allow for more personalized learning in classrooms that enable education systems to meet students' specific needs. Deng (2010) believes that smart devices enhance students' learning opportunities by increasing the efficiency of access to educational opportunities. Figure 2 illustrates the interconnectedness of the IoT.

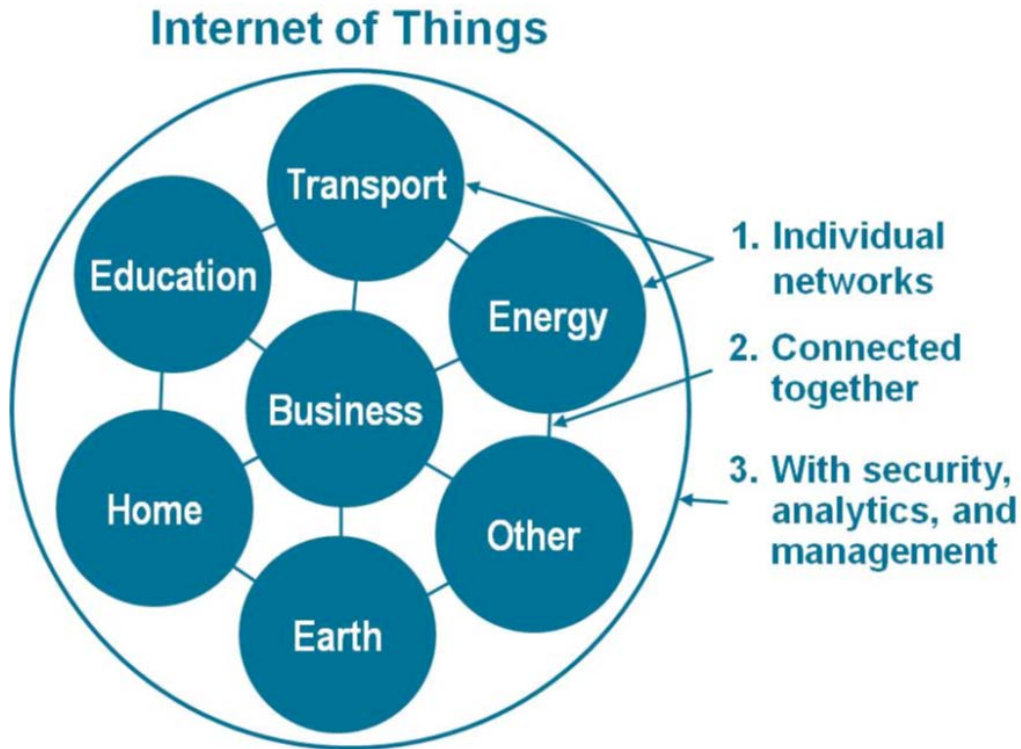


Figure 2. IoT Can Be Viewed as a Network of Networks. Source: Evans (2011, p. 4).

E. ISSUES PRESENTED BY THE IOT

1. Security Issues

Moreover, although it is virtually impossible to cover the complete scope of the issues that surround the IoT, all users need to be ensured regarding the resilience, security, reliability, and the stability of Internet services and applications. Globally, users should have complete trust in the Internet, the devices connected to it, and they are well secured when conducting online activities. Ukil, Sen, and Koilakonda (2011) affirm that the security of IoT is connected to users' complete trust in their environment. If people cannot trust or do not have faith in their connected devices, or that their information is safe from damage and misappropriation, then the resulting deficiency of faith leads to an unwillingness in using Internet services. Further, Roman, Zhou, & Lopez (2013) believe the outcomes of such a scenario could have worldwide implications for technical innovations, electronic commerce (e-commerce), free speech, and probably every aspect

of online activities. Therefore, as Weber (2011) indicates, ensuring the security of services, as well as products of the IoT, should be a top priority in this sector.

As more devices are progressively being linked to the Internet, new chances to exploit potential vulnerabilities in security grow. Cybercriminals use IoT devices that are poorly secured as entry points, allowing these individuals to cause devices to malfunction or be re-programmed. Devices that are poorly designed expose the data of users to theft through leaving streams of data unprotected. Together with the potential deficiencies in security designs, the mere increase in the nature and number of IoT devices tends to increase the chances of an attack. When combined with the highly interconnected nature of the IoT devices, all poorly secured and connected devices could potentially affect the resilience and security of the Internet, both locally and globally. For instance, Stankovic (2014) argued that television or refrigerator that is unprotected could be infected with malware that might send harmful spams to recipients across the world directly using the home Wi-Fi connection of the owner.

Sicari, Rizzardi, Grieco, and Coen-Porisini (2015) argue that our potential to continue in our day to day routines without the use of systems or devices which are Internet-enabled is bound to reduce in a hyper-connected world. On the contrary, it is relatively hard to buy devices that cannot link to the Internet since some vendors only make products that can connect to the Internet. As each day passes, we get more dependent and connected to Internet-enabled devices, and we require these devices to be safe while still understanding that there is no device that can be completely secure. They added that this rising level of dependency on Internet-connected devices and the services linked to the Internet that they interact with raises the chances for hackers to acquire access to these devices. This partly explains why the security associated with the use of IoT services and devices is a crucial discussion and should be treated as a critical issue. Firdous et al. noted that, for example, “in 2014, cybersecurity vendor Proofpoint had discovered a botnet comprising 100,000 consumer devices including an Internet-connected refrigerator sending 750,000 spam email messages to companies and individuals across the globe” (2017, p. 1).

2. Potential Threats Unique to IoT Devices

IoT endpoints tend to share the same security needs: a trusted identity, a device's identity, data secured at rest and motion, and verified applications. These needs translate to the signature, encryption, and authentication. Much reliance is placed on IoT DC elements, for example, switches, devices, sensors, data, applications, and control. Innumerable commercial systems, infrastructure, and operations are already being controlled through the Internet. This trend is only bound to increase as organizations continue to implement more devices to become more competitive.

One good example is the capability of a valve actuator remotely able to validate messages that it receives from the controllers, which are very important. The message, as well as messaging authentication, is a critical process in ensuring the validity of data to be applied to business decisions. The need for related controls and specific assurances has significantly increased for both consumer-driven and industrial IoT devices. Therefore, security is a crucial aspect of the IoT. An IoT PKI shows the importance of secure authentication and protected data at different endpoints. Digital certificates have become a popular solution for encryption, signing, and authentication (Hong, 2013). According to Chui et al., the facts are clear:

1. Communications technology is constantly evolving and even the most advanced sensor technologies have a finite operational life and significant requirements for physical and cybersecurity.
2. IoT needs massive numbers of deployed sensors and robust communications architecture in order to be successful. (2010, p. 2)

Likewise, there have been questions raised concerning security challenges posed by IoT devices. Most of these questions were in existence before IoT growth; their level of importance continues to increase due to the scale of IoT devices deployment. Some of the prominent questions are. Nachappa et al. (2018) remind us that when thinking about IoT devices, it is essential to comprehend that these devices' security can never be complete. It is important to conceptualize the security of IoT devices as a spectrum of vulnerabilities since the issue of IoT device security is not a debate of secure or insecure. This spectrum ranges from completely unsecured devices with zero security features to highly secured systems with several layers of security. Nachappa et al. (2018) suggest that as new threats

to security keep evolving, network operators and devices manufacturers continue to respond to these threats accordingly. The resilience and security of the IoT are a utility of how threats to security get managed and assessed. The security of devices is a utility of the threats that devices will be compromised, the damages likely caused by such compromises, and the resources and time needed to acquire particular security (Nachappa et al., 2018). Likewise, Schneier (2009) acknowledged if a user is unable to tolerate a high level of security threats such as the case of the traffic control system operator, or an individual implanted with a medical device that is Internet-enabled. That person may feel justified in spending many resources in ensuring the security of the device or system.

According to Stankovic (2014), numerous factors affect the process of mitigating calculations and assessing risks. These factors including the incorporation of the current security risks and future potential risks, the predicted economic as well as other costs of injury if the threats are figured out, and the expected costs required for risk mitigation. These types of tradeoffs in security are usually made from an organizational or personal user perspective. Despite this, the interrelatedness of devices on the IoT needs vital consideration as part of an ecosystem of the larger IoT. The connectivity of the IoT devices that is networked implies that security choices made about IoT devices locally can have impacts on other devices globally. Developers of smart objects for the IoT have the responsibility of making sure that their devices do not let anyone get exposed to potential harm. Regarding economics, lack of device security in the IoT tends to have negative impacts on the devices involved and the individuals who might be forced to incur some costs. IoT devices are usually different from traditional computing devices and thus have different security challenges.

According to Nachappa et al. (2018), Data Confidentiality, Access Control, and Authentication are all important considerations. For instance, they wondered what the primary function of encrypting data with regards to IoT is. Is using robust access control and authentication technologies, and secure encryption in the IoT devices enough solution to prevent hijacking and eavesdropping attacks of streams of data produced by these devices?

Which authentication and encryption technologies can be adapted for IoT, and how can these technologies be implemented within the constraints of IoT devices such as processing speed, cost, and size? What foreseeable issues of management need to be addressed due to the scale of IoT cryptography? Are issues about the management of the crypto-key life cycle and the period expected during which any particular algorithms expected to stay safe being addressed?

Although IoT systems make the prospect of everyday tasks more expedient and enable decisions to be based on numerous sources of information, and manage limited resources more proficiently, businesses and ordinary users benefitting from IoT-enabled products and services must be aware of the likelihood that each of these locations and devices represents a mark for criminals and is vulnerable to malicious attacks. Some of the unique IoT challenges and vulnerabilities include:

- According to Zhang et al. (2014), many IoT devices such as consumer items and sensors are usually designed for deployment at a huge scale that involves orders of magnitudes beyond those that traditional devices can handle. This makes the potential number of interconnected links in these devices to be unprecedented. Additionally, most of these devices can develop connections and communicate together on their own dynamically and unpredictably.
- The IoT and its connected underlying and supportive ICTs may be vulnerable to malicious code. The deployment of malicious code may cause IoT equipment to malfunction or shut down altogether. The propagation of malicious code, including Trojan horse, worms, viruses, and rootkits, is substantial and will continue to grow as malicious code developers combine and integrate autonomous smart viruses and multi-stage viruses.
- Modeling, Simulation, Data Mining. Many IoT deployments consist of collections of devices that are identical or nearly identical. This collection homogeneity increases the potential outcomes associated with vulnerabilities caused by security issues as a result of the number of devices, which have the same traits (Heer et al., 2011). For instance, a vulnerability in the

communication protocol of a single company's brand of light bulbs, which are Internet-enabled, may extend to every model and make of gadgets and devices that utilize the same protocol or uses the same or key manufacturing characteristics. Consequently, the progressions in modelling and simulation technology will enable bad actors to identify critical nodes, paths, and their susceptibilities (Heer et al., 2011).

- Internet Protocols are the bedrock for communications, routing, and addressing of data over the Internet. Moreover, Internet Protocol Version 4 (IPv4) was the basis for most of the legacy Internet infrastructure and associated applications. However, because IPv4 did not have sufficient capacity to meet the growing number of Internet devices, a new protocol was developed. Although Internet Protocol Version 6 (IPv6) increases the number of addresses, it did not eradicate the weaknesses associated with IPv4; in fact, IPv6 left some IPv4 problem sets mostly unresolved, and introduced its own set of vulnerabilities and challenges.
- IoT devices are deployed with a service life that is anticipated more years than is linked with high-tech tools. These devices may additionally go through deployment in situations that make it hard to reconfigure or upgrade them, or they may live longer than the companies that manufactured them, leaving them orphaned without a way of acquiring long-term support. Circumstances such as these show that these security strategies, which are adequate during employment, may not be enough for the complete lifespan of the device as risks to security, continue to evolve. This tends to create vulnerabilities that also tend to persist for a long time. This is different from traditional systems, which are often upgraded with OS updates throughout the devices' life cycle to address threats to security. The management of devices in the IoT is a crucial security challenge (Weber, 2011).
- IoT devices are designed intentionally lacking the ability to be upgraded, or the procedure followed by upgrading may be impractical or cumbersome.

These devices are often not susceptible to the upgrade process since it presents inconveniences to the owners, leaving them vulnerable to cybersecurity threats (Roman et al., 2013).

- A significant number of IoT devices operate in a way that the owner has almost no sight of the internal workings of the device or the exact data streams they produce. This tends to create vulnerabilities in security when a user believes that their device is carrying out particular functions. In truth, it might carry out unwanted functions or gather more information than the user intends. The function of a device may also change without the knowledge of a user when an update is provided by the manufacturer, which leaves users vulnerable to the changes that may be initiated by the maker (Mahmoud et al., 2015).
- Several IoT devices are bound to undergo deployment in areas where security is impossible or difficult to achieve. Thus, any unsecured device connected to the IoT that uses open, unsecured, exposed servers, or Internet services protocols could be at risk. For example, researchers at the 2014 BlackHat conference successfully demonstrated that smart TV technology has the same attack vectors as a smartphone. Furthermore, they proved smart TVs were at risk for a wide range of attacks, including man-in-the-middle attacks, sniffed network traffic, commandeered TV programs and captured TV screenshots and logged keys, and stolen personal and financial information. The hackers do not need to gain physical or direct access to IoT devices. Therefore, features of anti-tampering, as well as other technologies, will have to be regarded to maintain security (Sicato et al., 2019).
- Some IoT devices are manufactured to be embedded in the surrounding, where an owner is unable to realize the devices' operating status actively. Devices may also lack a clear way of alerting an owner when there is a security issue, making it hard for the owner to know there is a security breach in their IoT device. This increases chances for a security breach to persist

without being noticed and corrected by a user if even mitigation and correction is practical or possible. A user may also be unaware of a sensor's existence in their surroundings, therefore, potentially enabling a breach in security to persist long without being detected (Jing et al., 2014).

Figure 3 depicts IoT security challenges.



Figure 3. IoT Security Challenges. Source: Nachappa et al. (2018, p. 2).

All of these questions are a representation of the wide-ranging considerations of security in connection with IoT. Wong, Locasto, and Keromytis (2005) noted that it is essential to note that when a device is connected to the Internet, it becomes part of the Internet. This means that appropriate and effective solutions for security can be acquired if only those involved with the device can apply a Collaborative Security Approach. This model has proven to be a practical approach in governments, public authorities, and industries to secure cyberspace, the Internet, and the IoT.

F. PRIVACY ISSUES IN THE IOT

It is important to note that the IoT varies significantly from the traditional Internet. With the IoT, devices are fixed with sensors for monitoring various factors and collecting information (Lu, 2014). As explained by Lu (2014), many IoT devices used today as part of the IoT are mostly associated with aspects of low power and lossy networks. These are significantly limited with aspects of processing power, memory, and energy. According to Reddy et al. (2018), many of these devices are prone to loss of data and are incapable of handling complex security and privacy protocols. However, they are still deployed and are currently used as part of the systems of the IoT despite such significant risks to the security and privacy of the customers. With the IoT, everything around us, in the form of the smart devices, will be linked to a grid. The need to be connected is tremendous; however, there needs to be adequate security and privacy measures that the networks need to provide for information movement between the devices to be secure. Not all aspects of the network, especially the ones used by end-users, will be secure, and this will provide an opportunity for unauthorized access to private information.

According to Lu (2014), bigger networks are not safe because the risk of the security threat may lead to the loss of crucial information or destruction of essential protocols. Lu explains that low power and lossy networks (which are networks that provide power to the smart devices of today) provide security and privacy challenges because they are non-interoperable. The differences in the interfaces for movement of information and implementation of standard systems of communication. This also hinders their capacity to have adequate security and privacy because of the existence of restrictions on access as well as implementation. Interoperability is a notable aspect of ICTs. It allows systems and products to work together without any advanced effort on the part of consumers. It is a significant limit on the smart devices of today because they lack a common platform. Lu argues that a lack of interoperability hinders the implementation of standard privacy and security goals when it comes to security and privacy. Some of the features of low power and lossy networks put the security of such networks at risk. Better knowledge and comprehension of how these systems work can significantly help promote better security.

Wong, Locasto, and Keromytis (2005) tackle the issue of security of sensitive information; they believe that a significant problem in the joining of devices in the IoT is the movement of user sensitive information. The devices will need to have sensors and other aspects of collecting information and then use networks to move the information to other devices. Devices of the systems of the IoT have now begun to be functional, and many have reached end-users. Research shows that there are approximately 20 billion devices in use across the world, and in a couple of years, the number could be roughly 50 billion devices (Lu, 2014). The high rate of increase in these devices is based on their capabilities to influence people's lives.

In securing IoT, the initial step when utilizing PKI innovation is individual onboarding devices that are associated safely to an IoT application (Scheirer et al., 2013). At that point, provisioning of PKI Certificates happens. The PKI Certificates demonstrate the related devices' identities to the IoT application. Now and again, there are particular entryways or devices which may require more confirmation, for example, password and username credentials.

The most serious issue is; the IoT landscape is inconceivably extending in ways that make the assignment off on loading and guaranteeing the provisioning of every device unmanageable and intensely tedious (Hong, 2013). It likewise increases the danger of human mistakes, which may make a chance for genuine flaws in security because of the expansion in the volume of devices. Despite this tedious work, every device requires its own particular PKI Certificate that is extraordinary. Likewise, the PKI innovation needs to effectively deal with the certificates at the size of the IoT, for instance, revoking certificates as required by policy.

Lu (2014) believes in comprehending the risks better they pose concerning security and privacy; an analysis of their life cycle will explore some of their limitations. These limitations could prove risky, as described. According to Lu (2014), the main phases of their life cycle include manufacturing, commissioning, which involves the process of installation, and lastly is operation. Lu believes the manufacturing phase contains minimal risks, and are a result of people in the organizations that may be untrustworthy. One of the security risks of this phase is the cloning of the device. When the device is cloned, it may

be then sold, but at a lower price, however, this is not very risky. On the other hand, access to the devices during this phase may alter the software by implementing harmful features or establishing backdoor systems. When sold to the public, people may fall prey to unauthorized access.

Lu (2014) describes the next phase as the installation or commissioning phase, which is associated with providing the devices with their identities. It entails the installation of software, security features, and other aspects that make up the devices. During this phase, untrustworthy people may make substitutions on the installations and add faulty or insecure systems. The other risk associated with this phase is getting access to secret keys. With such keys, the networks through which the devices communicate may get compromised. Lu believes the installation phase is risky because it is where the devices' identity is implemented and the phase where eavesdropping (backdoors) may be laid down by untrustworthy people. People may lay bugs or software capable of collecting private information once they begin to use the devices. Another aspect of the phase is the substitution of the systems with faulty or insecure ones.

According to Lu (2014), the last phase is the operation phase; this is the phase associated with the use of the devices, and it is the phase where the devices are highly prone to security and privacy threats. Eavesdropping also takes place in this stage whereby people use systems that can intercept communications with other people or with other devices. Active routing attacks are another risk that is mostly associated with hacking, which provides access to crucial or private information that hackers may steal or destroy because of malice. Hacking is the leading risk during operation and occurs when unauthorized people find routes to access the devices, and once in the system, they may have some level or full control over the devices (Lu, 2014). Another risk is associated with denial of services. Sometimes unauthorized access develops a middle man in the system, and when this happens, the person can deny certain services the devices were meant to provide. Denial of service may also hinder the devices from performing a crucial task such as booting and may become great inconveniences to the users.

Desai, Sheth, and Anantharam (2014) claim that how the systems of devices are used in the IoT are structured to influence the security aspects of the devices. Centralized

systems provide an advanced level of safety. The management of devices and keys in centralized architectures provide higher security measures but, at the equivalent period, provide a point in the architecture that is distinct for security failure. They believe another aspect is associated with the synchronization of the devices for security. However, these devices are usually based on low power and lossy networks, meaning that they always need to conserve their energies because of limitations of power. As a result, they sleep from time to time, and this complicates the processes of authentication when it comes to security synchronization.

Desai et al. (2014) believe that the other factors are bootstrapping, and as explained previously, those are limited by factors of interoperability. They also claim that the process of authenticating nodes is very complex and lacks proper security. Developing secure connections is very difficult and thus provides a significant challenge for the connection of devices with one another. They suggest that the computation problem and the need for conservation of energy provide significant challenges for the technology.

Desai et al. (2014) argue that the lack of interoperability creates significant computational limits among different devices because of the privatization of a standard protocol of operation. They add that the inability of these devices to develop a secure connection with one another puts them under a high-security threat since the connections provide loopholes for unauthorized access. Computational limits during authentication make it very hard for the devices to connect securely. Lack of interoperability, which limits devices from working with others, hinders success in establishing a secure connection with one another (Reddy et al., 2018). Security issues occur at both aspects of the system's network as well as aspects of its physical structure. Two of the threats that IoT systems face are:

a. *Access Control*

Gusmeroli, Piccione, and Rotondi (2012) believe that access control provides preventive measures that ensure that nodes within the network are not compromised by unauthorized access. They add that Access Control is connected with the utilization of a wide range of measures developed for the need of limiting access either physically or

virtually to computer resources. Concerning using devices within the IoT, having many nodes that operate as a fragment of a structure puts the network at significant risk. With access controls, users of a system that are authorized are granted access and given privileges of using various aspects of the system. Unlike authentication, which only varies users trying to access the network, access control is what gives the right to access. Restriction of access can only be lifted once the client or server is authenticated and is authorized. Some of the common aspects of access control include login details and locks. The lack of stable access control may lead to significant security risks within a system.

Lu (2014) asserts that a lack of reliable access control may limit a system's capacity to restrict access by unauthorized users. In this case, the system can be easily compromised. He argues that all devices within the IoT need to have robust access control that can handle any form of access threats. According to Lu, one of the greatest threats associated with access control is piggybacking, which involves a legitimate user of the systems holding the doorway into the network for an intruder to access. In this case, the legitimate users provide credentials that allow the doorway of the network to open, and once it has the intruder follows through. Extra validation of access is crucial.

b. Availability

The second security threat is associated with the availability of information. For the successful operation of the IoT systems, information has to be readily available for devices when they need to access them. According to Chapman and Bell (2018), non-availability is a threat that is very significant for the system, primarily because most of the devices used are based on low power and lossy networks, which results in considerable limitations in terms of performance and energy conservation. They try to conserve their energy through initiating sleep mode, and when this happens to access to information is limited because the aspects of synchronization for authentication and authorization is hindered. Chapman and Bell (2018) also assert that availability is directly related to the concept of interoperability, which is associated with hardware and software conflicts between different devices within the same system of the IoT. Interoperability creates conflict

brought about by differences in user interfaces and hardware devices, which are attributed to the development of devices by different companies.

According to Chapman and Bell (2018), availability is a security threat also brought about by a lack of software upgrades, because if current ones are obsolete and cannot meet the needs of the network, it will fall short in accessing available information. This is problematic, as the IoT relies significantly on the availability of information from the different devices within the same network. Lu (2018) asserts that the existence of bottlenecks caused by both hardware and software problems limits the systems' access to information from the devices, and, for the devices to work efficiently, information has to flow smoothly and communicate without any shortcomings. Loss of data can cause unavailability, and malicious activities, such as a denial of service, also limit the availability of information and thus limit the success of the system.

G. INSECURITY IN THE IOT

According to Barcena and Wueest (2015), the issues of security that may affect the IoT are generally well known within the IT industry. However, although these questions existed before the development of IoT, the global integration of sensors and ICTs does not come without intrinsic security risks; therefore, the questions raised regarding security challenges presented by the IoT increment in importance due to the scale of the arrangement of IoT devices.

Part of what drives the high demand for the IoT is enticing the ability to access connected versions of almost all devices. Barcena and Wueest (2015) note that despite the vast amount of information concerning security threats, many users of the IoT fail to ensure the security of their devices, and many suffer from unauthorized access. Many dangers occur in such systems, and all could prove risky for the application of new technology. Reddy, G., Rama Mohan, and Reddy (2018) suggest that although security measures such as authenticating and encrypting data, are extensively used as effective measures of security control, they are widely disregarded and neglected because of the limited understanding of the way they operate. In other words, the rate of deployment of these

devices is swift, but the level of security awareness is still low. It is paramount that people have a full understanding of security threats that their home devices possess.

The IoT has created a large surface for attackers to exploit, as the aspect of connecting many devices to a network is bound to slip at one point or another, and the many risks are devastating when they occur. Since the IoT is mostly related to the use of smart wireless devices, and as the devices are remotely connected, from time to time, there will be authentication. As asserted by Barcena and Wueest (2015), some of the main threats are based on pure personal factors: a good example is weak passwords as access controls for devices. As simple as it sounds, having weak passwords may cost people considerably because a hacker may gain access to vast amounts of private information; weak passwords make a system easy to crack. As a result, many manufacturers try to encourage users of the devices to establish strong passwords or change them regularly. However, this can be problematic because the security measures needed for such processes are usually long, making it hard for users to implement them.

The IoT is slowly finding its way at home and based on current trends, and more devices can connect to the networks of this system. Barcena and Wueest state that some of the devices used to connect are usually for automation of certain aspects of the home, such as lighting, security, and energy management. Some of the devices include:

- Smart thermostats
- Smart locks
- Smart light bulbs
- Smart smoke detectors
- Smart energy management devices
- Smart hubs
- Security alarms
- Surveillance IP cameras
- Entertainment systems (smart TV, TV set-top boxes, etc.)
- Broadband routers. (Barcena & Wueest, 2015, p. 7)

Kamaludin, Mahdi, and Abawajy (2018) believe the advanced nature of the technology, specifically automation, will soon run most people's lives. Smart home devices are famous and popular around the world, and soon they will be in almost every home. These devices use mobile applications for the processes of monitoring or web

portals that give them access to the network. Sometimes they can be connected to cloud-based services for which users may use to monitor their functions and various systems at home.

Another essential technology currently popular is the use of a home network (Kamaludin et al., 2018). Home networks have become very popular because they create local networks that can route broadband and provide Internet access at home. By the simple use of a Wi-Fi connection, devices can quickly and easily get connected to the Internet, and are simple representations of home networks that connect different devices. Barcena and Wueest (2015) observed that the network connects several devices to the local network, making it possible to communicate with one another. A central router is then used to provide the network with Internet access.

In such a topology, safety is vital, and the dangers of illegal entry to the network are many. The central router provides some essential firewall services that try to protect the users of the network from threats. As Kolbe, Kubler, Robert, Le Traon and, Zaslavsky (2017) point out, the establishment and development of the IoT mean that more and more devices will find their way into homes, and they will all be connected to the same network for effective communication with one another. There are many categories of devices that find themselves in this system, yet there is no single security protocol to meet their needs (Barcena & Wueest 2015). This, therefore, means that as the number of devices increases at home, the capacity of the structure to deliver security for their operation reduces.

As Misra, Goswami, Taneja, and Mukherjee (2016) point out, there are two main categories of devices used as part of the IoT at home. One of the categories includes devices that use existing network technologies such as Wi-Fi and Ethernet, including TVs and laptops. The other category is based on devices that use a different form of network technology, including sensors. The varied aspects of connectivity of devices, especially at home, are based on the fact that there lacks a single defined protocol of connecting these devices and is a clear indication of the aspect of non-interoperability. According to Barcena and Wueest, devices use different communication methods, and some of the methods include the use of:

- Power lines
- Bluetooth
- Radio frequencies
- ZigBee
- Z-wave, among others. (2015, p. 7)

Misra et al. (2016) point out that currently, power line, Zigbee, and Z-wave are the protocols standard in the automation of many home devices today. Sometimes devices require the combined use of methods; for example, the use of power line and radio frequency is standard in many devices. Smart devices are commonly associated with the use of ZigBee and Z-wave connectivity with Z-wave amounting to more than sixty percent of network use. In most cases, the devices are connected to a central hub which may be connected wirelessly or connected via a cable. The central hub connects the devices to the network, and the network can be accessed remotely through web portals. One central aspect of this connectivity is the need for a standard protocol of connectivity to increase communication efficiency and access to information.

According to Santofimia et al., most devices currently operate through the use of regular Wi-Fi for effective communication, and smart hubs that form the central point of connection for devices provide an excellent surface of attacks for networks. Physical and virtual attacks are all following aspects of security threats for such home connections when there are limited restrictions or limited security measures implemented. Physical attacks may occur when smart devices are accessed physically and reconfigured by intruders or friends and family. Physical attacks are also linked to the utilization of second-hand IoT devices, where someone purchases a device whose security has already been compromised (Santofimia et al., 2018).

As devices are deployed, Barcena and Wueest (2015) have drawn attention to the fact that supply chains also provide platforms for initiating physical threats; for example, lacing software updates with Trojans that carry malicious software. Stajano (2002) believes that physical access to devices gives people the ability to configure the devices in manners that best suit their needs. Once they have control over the devices, they can access the network they operate on, steal information, destroy it, or deny service, which can be very problematic. Reconfiguration by an intruder may lead to the resetting of the devices, and

the establishment of new passwords, allowing intruders to establish their passwords, gain control of the devices. Likewise, Computer-generated assaults happen when invaders get unauthorized entry to the network through a direct connection that occurs through the use of Wi-Fi or Ethernet.

In this growing era of technology, where companies continuously struggle to improve their operations through the deployment of digital technologies, IoT initiatives are the backbone of such efforts. Increased volumes of data are generated and collected daily from the swiftly growing rate of usage for IoT devices. The cloud as well has played a critical role in the provision of IoT solutions for future consumption. However, in the collection and analysis of data to make business decisions, it is essential to have trust in the devices used. If organizations want to ensure the continued safety and security of IoT deployments, they must adopt time-tested security techniques to ensure their IoT systems are fully secured. One such useful time-tested security technique is PKI.

According to Coetzee and Eksteen (2011), the planet would have more IoT devices than human beings. Thus, all companies wishing to be part of this global interconnectedness should endeavor to put security measures in their private networks by contacting companies that provide PKI services and having their network secured.

Web-users play a significant role in the implementation of PKI. One of the responsibilities includes keeping the browser up to date by updating the software from time to time. The users also have to watch out for certain activities within the browsers, such as making sure that the position written down in the bar is the one intended to ensure that the protocol being used is the correct one. In most cases, the HTTPS is best to ensure that the connection is secured, to take keen note of pop-up windows, and be able to understand how to authenticate certificates (Guida et al., 2004). Users have to be very keen when using the Internet, especially ensuring they use browser tools and plugins to limit the activities of new websites.

The Open Web Application, Security Project's (OWASP) list of Top Ten IoT vulnerabilities, sums up most of the concerns and attack vectors surrounding this category of devices:

- Insecure web interface
- Insufficient authentication/authorization
- Insecure network services
- Insecure mobile interface
- Insufficient security configurability
- Insecure software/firmware
- Poor physical security. (Barcena & Wueest, 2015, p. 5)

H. PKI: A STRONG SECURITY FOUNDATION

Dener, Watkins, and Dorotinsky (2011, p. 121) describe PKI as “a suite of hardware, software, people, policies and procedures needed to create, manage, distribute, use, store, and revoke public-key certificates in order to provide “trust” for secure electronic communications and transactions in open environments. For each user, the user identity, the public key, their binding, validity conditions, and other attributes are made unforgeable in digital certificates issued by the CA.” Also, Asfar (2015, p. 5) describes PKI as an infrastructure made up of Certificate Authorities, Registration Authorities, Certificate Repositories, and Digital Certificates that “provides a secure environment for online transactions, confidential email, and e-commerce by authenticating the identity of the entities (the sender and the receiver), and maintaining the data integrity.” Furthermore, according to Lopez (2013), PKI as a security structure that is trusted and comprises of programming, equipment, individuals, strategies, and approaches which are expected to oversee safely, create, store, revoke, and disperse trusted DCs and guarantee the administration of open key encryption.

In the modern world of technology, the globalization of IT has created an international network of producers, suppliers, and consumers. The application of PKI on IoT devices cuts across industries, from payment structures, smart metering to automotive. PKI services have been used in the authentication of employees and devices in different companies. Indeed, critical data may involve very different information ranging from eID services, including the production of passports to the management of digital rights in the entertainment industry. Globalization has had a noteworthy impact on the enhancement of international systems. It as well has led to the development of banking and business

systems that operate over the Internet, resulting in the development of distribution systems that are highly diverse and simplifies the management of devices and applications work.

The need for PKI security services has mainly been brought about due to the continued rise of e-commerce business transactions, including electronic banking, two systems that deal with very sensitive and private customer information. Consequently, the problem of how to protect the open network environment and the underlying infrastructure of IT systems is of significant concern. To this end, IT subject matter experts (SMEs) banded together. They came up with the innovative idea of PKI, which can address the security requirements of in-transit and at-rest data. It also facilitates access to protocol and the verification of proper availability hence ensuring full coverage of system and data integrity, confidentiality, and availability.

The PKI environment is vast, with different moving parts that work together for success (Hong, 2013). Consequently, PKI has become the cornerstone for many IT infrastructures in ensuring enhancing non-repudiation, authenticity, integrity, and authenticity of critical and sensitive data. The existing PKI infrastructure of vetting identity, which is accomplished by publicly audited and trusted CAs, provides all the essential foundations for IoT organizations' authentication (Rea, 2015). PKI credentials offer proof that the organization's identity, devices, and domains were established properly because public keys are bound cryptographically to such devices. On-demand issuance, as well as abilities of pre-vetting such as DigiCert's PKI for IoT, perform and enable real-time verification or one-time verification to complete the assurance of identity, which is required by IoT systems and projects. PKI can provide unique value and core competency, which enables trusted connections in networked devices, smart devices and infrastructure, and cloud services. This authentication component is the one that is gravely required by IoT for security, and it is what PKI ably offers.

Housley and Polk (2001) describe how the flow of data over networks is kept safe from unauthorized access that enables the flow of sensitive data, for instance, online banking information or personal information about people conducting transactions over the Internet. This system enhances the procedure of encryption, which then guarantees confidentiality and privacy by safeguarding the identities of the collaborating parties is

well known and therefore increasing the level of security; the use of PKI is usually due to the need for increased security (Casola et al., 2007).

1. Uses of PKI

Dener et al. describe the uses of PKI as:

solutions provide public keys and bindings to user identities which are used for encryption and/or sender authentication of e-mail messages, documents, users' access to applications, secure communication, and mobile signatures (mobile signatures are electronic signatures that are created using a mobile device and rely on signature or certification services in a location-independent telecom environment. (2011, p. 123)

Furthermore, according to Guida et al. (2004), PKI enables a secure broadcast of crucial data, and its solutions greatly simplify the end-user devices and applications the way and simplify the management of devices and applications work. This secure transmission would protect it from unscrupulous players even though the source of data was compromised. Furthermore, Internet security professionals have long regarded PKI Infrastructure and the use of DCs as their security backbone. Boldyreva, Fischlin, Palacio, and Warinschi (2007) believe that PKI delivers the most essential and necessary tools of privacy in communication processes inherently through authentication and encryption.

The unique role of PKI in the account of identity and data safekeeping, and its capability to usher the secure flow of data transversely through networks, make it as the best solution for Internet service providers, including the IoT. PKI performs its role by ensuring that there is appropriate data authentication, mutual trust, and security. Moreover, PKI ensures the integrity of information obtained from sensors. Most of the PKI solution manufacturers are strategically positioned to solve the security requirements of the ever-increasing IoT society. Commercial PKI providers can offer particular security elements, scalable platforms, and trust anchors that are needed to secure IoT devices effectively.

The use of PKI systems is also a great source of new revenue streams for businesses with a good comprehension of how the system works (Zhang & Yu, 2013). High levels of business growth, which is characteristic of digital businesses, bring with them strengths and weaknesses. However, a more effectual business environment brings with it

shortcomings associated with vulnerabilities and gaps within the systems. Identity Management Access systems are used to manage identities within networks and used by the organization for electronic identity management (Zhang & Yu, 2013). These systems provide the frameworks that businesses use to facilitate this management, where digital businesses use user identities for authentication. It empowers establishments to preserve decent accounts of the people they deal with and gives them proper accountability whenever they are audited. This is usually part of the policies and procedures of the business, and their operations are based on the guidelines of the policies in terms of whether the identities comply with the policies of the business. This is a crucial aspect of security for businesses, as well as compliance with the business' policies.

The management of access to information is paramount to any business because of mismanagement results in threats of unauthorized access, which may include the destruction of data due to malicious intention, the demand for particular information, and also the denial of service. However, aspects of Identity and Access Management (IAM) are insufficient to provide enough security for organizations' information (Zhang & Yu, 2013). Digital businesses have significantly evolved, and aspects of the IoT have become very complicated. Hence, the simple management of identities carried by the services of IAM is insufficient, and that is why more security measures are needed. The world of the IoT is reflected by the great need to manage both people that are responsible for the networks as well as the gadgets and devices connected to an IoT system. They are devices that are not always connected because of power inefficiencies, so more security measures are required.

According to Thompson, Essiari, and Mudumbai (2003), PKI tends to explore the legal factors as well as the operational factors of the network of a system. These operational factors may include rules, policies, and procedures that govern the infrastructure's operations. These hereditary factors may include factors of warranties and jurisdiction that usually guide the infrastructure. Furthermore, PKI's security level is much higher than the security level provided by ordinary username and password combinations. Because the identities of people communicating in any given network are well established and known when using PKI, a higher level of accountability is created, which is vital in improving the security of any given system or network.

PKI enables the basic security services for such varied systems as:

- SSL, IPsec and HTTPS for communication and transactional security
- S/MIME and PGP for email security
- SET for value exchange
- Identrus for B2B. (Weise, 2001, p. 3)

In addition, some important benefits that PKI and its use of public key cryptography offers for e-commerce and other organizations includes:

- Reduces transactional processing expenses
- Reduces and compartmentalizes risk
- Enhances efficiency and performance of systems and networks
- Reduces the complexity of security systems with binary symmetrical methods. (Weise, 2001, p. 3)

According to Weise, many other similar solutions rely on the fundamentals of public key cryptography such as:

- Student IDs on college campuses
- Voting
- Anonymous value exchange
- Transit ticketing
- Identification (passports and drivers licenses)
- Notarization (contract, emails, etc.)
- Software distribution
- Symmetric key management. (2001, p.3)

In summary, as Weise (2001, p.4) points out, “A PKI does not serve a particular business function; rather, a PKI provides a foundation for other security services. The primary function of a PKI is to allow the distribution and use of public keys and certificates with security and integrity.” Although a well-planned PKI can address challenges that are inherent in the e-commerce world, Weise, remind us that there are additional challenges to consider when deciding upon a PKI solution because,

PKI is not by itself an authentication, authorization, auditing, privacy, or integrity mechanism. . . a PKI does not infer trust by itself, but requires the establishment of a trust base, on which the PKI can rely. This requirement means that the basis of trust must be established on a personal, business, or other level, before it can be accepted by the PKI. (2001, p. 4)

2. Challenges of PKI

How an organization identifies and authenticates a customer or entity remotely the first time is principally important when entities are engaged in high-value transactions that carries significant legal or financial consequences. Conversely, if there is little risk to issue certificates to entities needing less robust methods of authentication. To summarize, PKI can support business venture into e-commerce, but stakeholders must first identify and evaluate business requirements for the different security mechanisms that a PKI can enable.

3. Defining Business Needs

The lesson here is that different businesses have different PKI needs. For example, if a business is a world-renowned news outlet like the New York Times, or Amazon selling products or services over the Internet, implementing a PKI to enable data integrity becomes one of the primary concerns and is then inarguably a cost-effective expenditure of resources. Therefore, according to Weise, the following must be accounted for when planning a PKI because data modification (i.e., posting inaccurate news or tampering with e-commerce transactions) without authorization may have severe repercussions:

- Integrity for the posted prices
- Identification and authentication for a potentially large population of customers
- Confidentiality of customer and transaction information
- Non-repudiation for supporting dispute resolution. (Weise, 2001, p. 4)

Implementing a PKI to enable these various security mechanisms can provide an online merchant with a cost effective approach to risk management. Other considerations for defining business requirements of a PKI include:

- Careful planning—Internet-based e-commerce business solutions are often complex, as are the PKI solutions necessary to support them. Take the time to perform a detailed evaluation of your business and technical environments before taking steps to implement a PKI.
- Interoperability—Does your current business model require interoperability? With whom? For what purpose? If your PKI requires interoperability, you should determine which of the different standards and protocols you must adhere. ... Because of the competing standards and protocols and the various interpretations that different vendors have

of these, it is critical that organizations determine their interoperability needs.

- Determining a PKI system and vendor—There are different PKI and cryptographic systems from competing vendors. Several different protocols, certificate formats, and platforms exist. Some investigation is needed to decide which PKI and vendor is the best for your particular business enterprise. Often a standards compliant solution from one vendor will not integrate with that of another vendor. This may cause problems if you consider a multi-vendor PKI solution.
- Performance and capacity—In situations where large amounts of data must be enciphered for confidentiality, public key cryptography may not be suitable because the cryptographic algorithms perform at relatively slow speeds. Symmetric or secret key cryptography is typically used for these applications... A PKI can be established for the distribution of the symmetric or secret keys that are subsequently used for the encipherment of data. Public keys and public key certificates can also be significantly larger than symmetric keys and this can affect how they are stored. (Weise, 2001, p. 5)

I. LOGICAL COMPONENTS OF A PKI

The following section briefly discusses the framework of a classic PKI, and how the different apparatuses work together.

1. PKI Framework

Different logical components comprise a PKI. As noted previously, a PKI is a framework of people, processes, policies, protocols, hardware, and software used to generate, manage, store, deploy, and revoke public key certificates. Nash, Duane, and Joseph (2001) claim that a PKI works best with the help of some components which function in unison. However, these components are further divided into two main aspects, which include the validation of the data and ownership of the public keys and the certification process. The most important aspect of the infrastructure is the certification process since it brings all the operations of the public keys in the system together. According to Nash et al. (2001), some of the critical components are a registration authority, a distribution system, and a CA.

The CA is mainly trusted with identifying individuals using the system, and it also issues certificates. Adams and Lloyd (2007) remind us that digital information about

individuals operating within a given system is usually contained in these certificates. On the other hand, the registration authority links people with the certificate by passing on digital certificate requests. It operates as the certificate's authority subordinate. The distribution system is involved with the storage of public keys and certificates as well as the flow of information in a system. PKIs also work through the use of protocols, which include the generation of keys and certificates, the generation of digital signatures, the validation of certificates and keys, and the revocation of certificates.

In short, PKI is a security framework that is most trusted but comes with challenges. Alrawais, Alhothaily, Cheng, Hu, and Yu (2018) believe that PKE and DCs are two critical elements of network security and operate as significant factors in PKIs. Public key enabling is the process of configuring systems and applications to use certificates issued by the PKIs for authentication, digital signature, and encryption. Each product type including web servers, domain controllers, network appliances, thin clients, must be configured correctly.

2. Trust Models

Although Trust models are important to the successful implementation of a PKI, a technical/ in-depth analysis of the various models is beyond the scope of this paper. Suffice to say that the following are the more common/better known examples of trust models:

- Hierarchical
- Distributed (Web of Trust)
- Direct (Peer to Peer)
- Cross Certification (Chokhani, 2003).

3. PKI Security Services

a. Integrity

Many viable systems, infrastructure, and operations are now being controlled through the Internet. This trend is only bound to increase as organizations continue to implement more devices to become more competitive. Managing data, which involves

movement, storage, and manipulation of the data, requires a high degree of data integrity to ensure the trustworthiness and security of the information. Data integrity ensures that information within a system is recorded as it is exactly intended for the system and that the same process applies during retrieval. Data integrity ensures consistency of information and, therefore, reduces data loss and corruption, while ensuring that there are no changes in the information, which may occur unintentionally. Integrity ensures data trustworthiness and is associated with keeping standards of consistency, which ensure that data cannot be altered in any way (Lu, 2014). Integrity involves establishing measures that ensure that people uphold trust and avoid unauthorized access to information.

Integrity also explores various aspects of ethical considerations. For example, accessing information after receiving permission is critical, as it gives a person full rights over data accessibility. However, maintaining trust is difficult, given the temptation of hackers to sell data at a high price. People also try to access data illegally because of malicious intent, which leads to significant risks (Lu, 2014). Thus, the need for related controls and specific assurances has significantly increased for both consumer-driven and industrial IoT devices. In the final analysis, Integrity is guaranteed as long as the CA's signature on the digital certificate can be verified.

b. Authentication

According to Yao, Han, Du, and Zhou (2013), authentication is associated with the processes of verification that occurs when one or more devices want to route information to one another. Porambage, Schmitt, Kumar, Gurtov, and Ylianttila (2014) claim that authentication verifies the source of data being routed and helps validate who is trying to access information. The security of the authentication process is considered a threat in the IoT, because this is a system that is usually highly automated, occurring with minimal human interactions. Therefore, it may provide a pathway for unauthorized access to the network, which would put the information being conveyed by the network at considerable risk of being intercepted.

Besides, according to Lu (2014), authentication occurs in tandem with other activities, such as authorization and encryption of information. It is a practice that collects

information about users and allows a device to prove the intent of the client or the server attempting to access network information. The process of verification and authentication is straightforward and transparent to end-users because the entire process only takes a few milliseconds.

There are many ways of authenticating, and in an automated system such as the ones used in systems of the IoT, the use of DCs is very effective in the process of authentication. By using digital certificates, the identity of the entity can be verified. These are certificates with details of the client, used to validate the authenticity of the requests made for information and access to a network. However, authentication does not dictate client or server activities, but instead, verifies their identities and makes sure they are valid before offering access.

c. Confidentiality

Confidentiality, a service that is equivalent to privacy, can create significant security risks for a system. Weise (2001, p. 6) states, “Confidentiality means ensuring that the secrecy and privacy of data are provided with cryptographic encryption mechanisms.” Lu (2014) claims that confidentiality concentrates on the features of privacy, and ensures that information does not reach those who may have no authority or right to access, and restricts contact to only authorized parties. He asserts that establishing policies and systems of confidentiality is very important for a system and that confidentiality of information can be categorized into levels, grounded on the degree of impairment once information is in the hands of the wrong people. Lu believes one of the best methods of enhancing the aspect of confidentiality is training. Creating a consciousness around upholding the privacy of information is vital according to Corbò, Foglietta, Palazzo, and Panzieri (2018); in the IoT systems, confidentiality is paramount.

d. Non-repudiation

Scheirer et al. (2010) remind readers that although non-repudiation, confidentiality/privacy, integrity, and authenticity have long been the pillars of trust, the way trust operates today is significantly different. In today’s global society, individuals tend to transact with other individuals from around the world whom they have not met and

may never meet. These transactions may, in fact, not even be between one individual and another; they may instead be between an individual and a machine, or just between machines. For example electronic wire transfer, automatic teller machines, insurance claims processing, electronic filing of tax forms, and e-commerce.

As Chodos, Reiniger, and Bruch (2019) point out, non-repudiation in a traditional environment is provided by handwritten signatures, sometimes after being witnessed and notarized by third parties. Digital signatures in electronic environments present the same trust element. Any place where transactions are made, there needs to be an establishment of trust. In the end, the signature on the certificate guarantees that only the owner has the private key associated with the public key in the certificate. In today's world, trust relies on PKI, and this involves three things:

- Technology
- Methodology
- The infrastructure used to perform the transaction. (Chodos et al., 2019, p. 22)

J. PKI PARTICIPANTS

According to Chokhani, Ford, Sabett, Merrill, and Wu (2003), the success of PKI depends on how it is implemented in a system, and its effectiveness depends on the parties responsible for its use within a system. In short, a PKI is “is a collection of servers used to create and manage public keys and digital certificates. It creates digital certificates which bind public keys to entities, stores them securely and revokes them when required.” (Afshar, 2015, p. 5). Moreover, Cooper et al. (2008) believe PKI is straightforward and depends on the provision of trusted certificates between the parties carrying out the transactions. If one possesses a certificate that they trust, then that person trusts them.

1. Subscribers

Examples of subscribers who receive certificates from a CA include employees of an organization with its own CA, banking or brokerage customers, organizations hosting e-commerce sites, organizations participating in a business-to-business exchange, and

members of the public receiving certificates from a CA issuing certificates to the public at large (Chokhani et al., 2003).

2. Relying Parties

Examples of relying parties includes: employees of an organization having its own CA who receive digitally signed e-mails from other employees, persons buying goods and services from e-commerce sites, organizations participating in a business-to-business exchange who receive bids or orders from other participating organizations, and individuals and organizations doing business with subscribers who have received their certificates from a CA issuing certificates to the public. Relying parties may or may not also be subscribers within a given PKI (Chokhani et al., 2003).

3. Registration Authority (RA)

PKI works best with the assistance of components that work in harmony, argue Nash, Duane, and Joseph (2001). Registration authorities, i.e., the entities that establish enrollment strategies for end-user certificate candidates, perform identification and verification of certificate applicants, start or pass along revocation demands for certificates, and approve applications for reestablishment or re-keying certificates. Subordinate organizations inside a larger organization can act as RAs for the CA serving the entire organization, but RAs may moreover be external to the CA (Chokhani et al., 2003). In general, the RA operates as the CA's subordinate, and it links people with the certificate by passing on digital certificate's requests (Asfar, 2015). In any case, these components are further divided into two main aspects, which include the validation of the data and proprietorship of the public keys, and the method of certification. As examined already, the foremost aspect and the foundation of the infrastructure is the certification process, since it brings all the operations of the public keys within the infrastructure together. Furthermore, according to Weise:

A Registration Authority (RA) is an optional, but common component of a PKI, used to perform some of the administrative tasks that a CA would normally undertake. Most importantly, an RA is delegated, with the CA's explicit permission, the authority to perform tasks on behalf of the CA. (2001, p. 14)

4. Certification Authority (CA)

The sources of trust are referred to as CAs, which are entities configured with trust anchors. In short, a CA “confirms the identity of the entity by issuing a digital certificate that binds the identity with the public key of that entity.” Afshar (2015, p. 6). Indeed, CAs, (trusted third party) is inarguably one of the most important entities in a PKI. An end entity is any user or imamate object that requires a digital certificate to identify them. The end entity usually must have the capacity to generate a public/private key pair and some means of securely storing and using the private key (Weise, 2001).

It is important to note that although considered an entity, by definition, a CA is not an end entity because the CA is trusted with identifying individuals using the system, and it also issues certificates with implementing secure authentication of systems, users, and devices. Asfar (2015) reminds us that digital information about individuals operating within a given system is usually contained in these certificates. Therefore, the process of linking public keys with identities of entities is developed via a process of issuance and registration of certificate by a CA, and judging by the level of guarantee of the networking, this can be conducted under the supervision of a human or through an automated process (Kumari et al., 2017).

Rea (2015) describes the CA as an organization that is associated with the creation, issuing, and revocation of DCs within a network. The certificates that CAs provide to customers are usually chained to roots that are trusted and embedded within browsers, but it also scrutinizes and audits third parties. The CA also verifies ownership information of the keys, as well as the control of the keys to be used in communication. It is also responsible for the verification of the information in the certificate and thus operates by authenticating owners of the certificates. It delegates the use of certificates concerning the security or business aspects and embeds roots in applications to establish secure connections with them and their use. To summarize, by signing both the key and the information about the owner, the CA certifies that the information is correct, that the public key belongs to the entity, and more importantly, the entity can be trusted (Schneier, 1996). Functions of the CA are:

- Issuing certificates
- Maintain and issue Certificate Revocation Lists (CRLs)
- Publish its certificates and CRLs
- Maintain status information of certificate expiration dates. (Weise, 2001, p. 6)

According to Schneier, Key Management includes (Key generation, transferring keys, key distribution, key verification, key usage, updating keys, storing keys, backing up keys, revocation of keys, and destruction of keys) is “the hardest part of cryptography.” (1996, p. 169). And, although an in-depth analysis of the key management life cycle is beyond the scope of this paper, suffice to say that the security of any cryptographic algorithm rests in the key. Moreover, according to Schneier (1996, p. 170), “If you are using a cryptographically weak process to generate keys, then your whole system is weak.” In short, once the keys are generated (random keys are best), the keys are transferred to the CA. The CA will then create certificates for the keys, which are then installed on the server of the system to enable secure web pages.

As an aside, it is essential to note that browsers provide a point of access to the Internet and therefore play a significant role in the implementation of PKI. They are responsible for specifying requirements for CA inclusions in their root store. Applicants for certification have to use the browser, which then scrutinizes their application against a criterion which is usually already published in the system. The process of browser updates is critical because it is associated with the removal or inclusion of trusted roots. It also sometimes allows the users it trusts to manage their roots within the system manually. The browser also takes part in the reception of audits made by the CA on roots, and it does so to ensure that the roots still comply with the stem; otherwise, it will be forced to remove them from the system (Rea, 2015).

CAs may be organized in a hierarchy in which an organization’s CA issues certificates to CAs operated by subordinate organizations, such as a department, division, or department inside a bigger organization. Figure 4 illustrates the CA hierarchy and. Figure 5 shows the CA certificates installed on the author’s Internet Explorer.

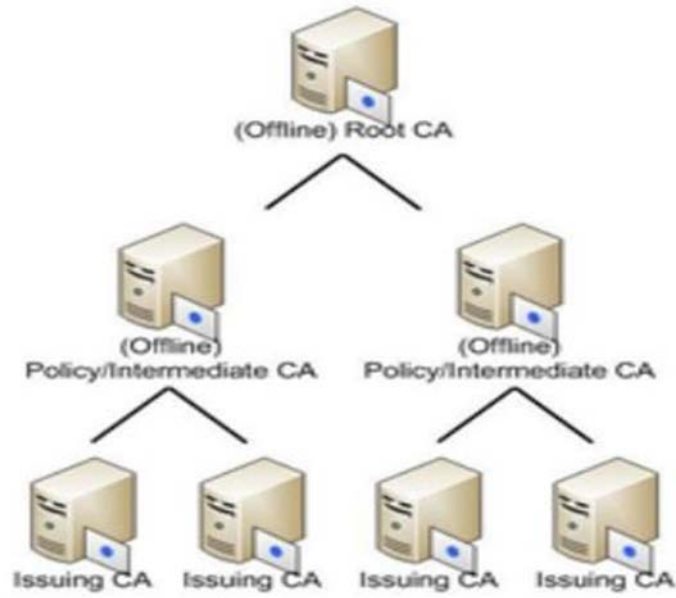


Figure 4. CA Hierarchy. Source: Afshar (2015, p. 7).

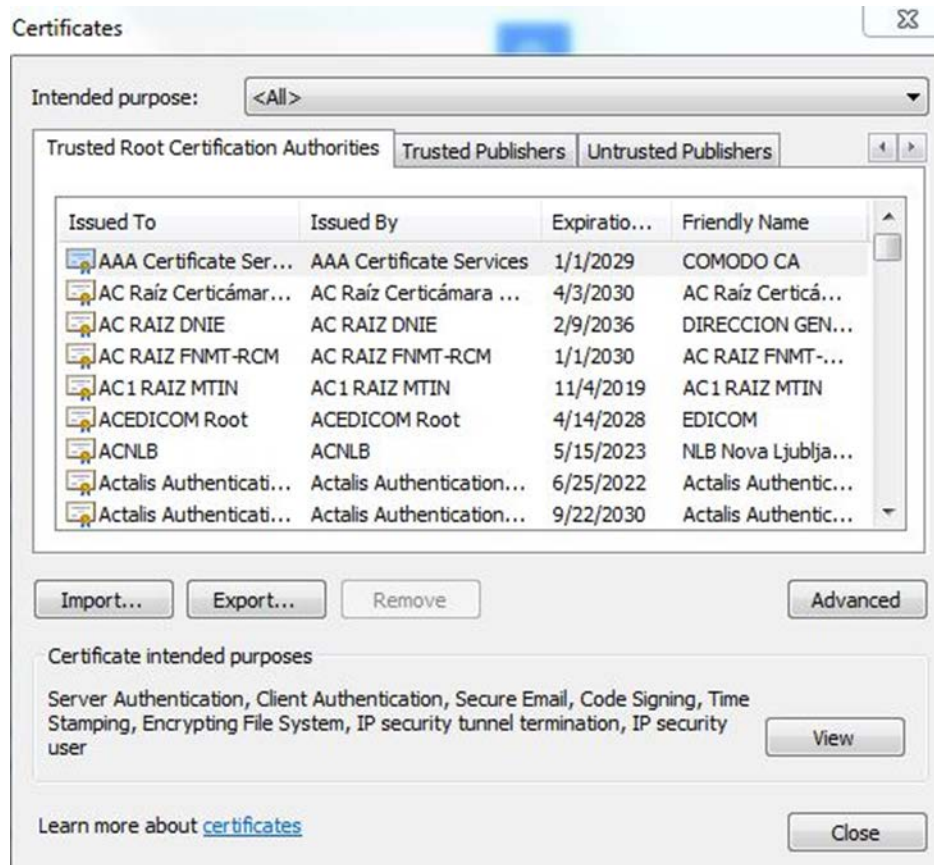


Figure 5. CA Certificates Installed on the Author's Web Browser

a. *Certificate Policy (CP)*

When a CA issues a certificate, it states a relying party that a specific public key is bound to the identity and other attributes of a specific entity; the certificate subject is more often than not the subscriber. Thus, from the viewpoint of a PKI, it is crucial to create some policy guidelines/rules which are to order compliance with specific algorithm capabilities. Hence certificate policy (CP) plays a critical part in a PKI. The X.509 standard defines a CP as “a named set of rules that indicates the applicability of a certificate to a particular community and class of application with common security requirements.” In short, A CP “sets forth the mandatory requirements and criteria imposed by the PKI concerning the various topics. In other words, the purpose of the CP is to establish mandatory requirements that each entity in a PKI must do (Chokhani et al., 2003). The following extension fields in an X.509 certificate are used to support CPs):

- Certificate Policies extension;
- Policy Mappings extension; and
- Policy Constraints extension. (Chokhani et al., 2003, p. 11)

b. *Certificate Practice Statement (CPS)*

The DSG and PAG define the term certification practice statement as: “A statement of the practices which a certification authority employs in issuing certificates.” (Chokhani et al., 2003, p.14). CPSs are detailed and describe the tenants, which must be followed by a CA in the life cycle of certificates. CPSs are crucial because of the applicability of how the CA manages keys over the entire life cycle, which includes services such as publication, revocation, and renewal, and re-keying capabilities. Rekeying has been defined as the process of installing a brand-new set of keys using a similar subject for each new certificate. Renewing refers to the process of using the same keys with a new certificate and similar subject; however, it is not rare for the certificates of IoT devices to never get replaced (Chokhani et al., 2003). In the DSG, the ABA expands the definition of a CSP with the following comments:

A certification practice statement may take the form of a declaration by the certification authority of the details of its trustworthy system and the practices it employs in its operations and in support of issuance of a

certificate This form of CPS is the most common type, and can vary in length and level of detail. (Chokhani et al., 2003, p. 14)

One needs to remember that some PKIs may not need to create a comprehensive and detailed CPSs. For example, applications that pose only negligible risks if compromised may only require low levels of assurances of trustworthiness of its services; in such a scenario, the entities establishing a PKI may opt to write or have CAs use a subscriber agreement. As mentioned previously, the ability to communicate securely and ensure integrity, authenticity, and confidentiality of information is a real and urgent problem. Consequently, since a detailed CPS may contain sensitive details of its system, the CA may elect not to publish a detailed CPS in such a PKI. Instead, the CA may opt to publish just an abstract or summary of the CPS that contains only those provisions from the CPS that the CA considers relevant to the PKI participants. Relevant information includes the responsibilities of the parties or the stages of the certificate life cycle (Chokhani et al., 2003). In summary, according to Weise, each PKI implementation should reflect the following in a CP statement:

- Purpose of the PKI
- Specific business requirements the PKI addresses through:
- Security architecture
- Associated trust model and threat profile
- Specific security services the PKI supports. (Weise, 2001, p. 19)

The following specification should be considered for inclusion in a CP or CPS:

- Training, operational, installation, and user manuals (which may contain operational requirements)
- Standards documents that apply to particular aspects of the PKI (such as standards specifying the level of protection offered by any hardware tokens used in the PKI or standards applicable to the site construction)
- Key Management Plans
- Human resource guides and employment manuals (which may describe some aspects of personnel security practices), and
- E-mail policies (which may discuss subscriber and relying party responsibilities, as well as the implications of key management, if applicable). (Chokhani et al., 2003, p. 19)

5. PKI Hardware Security Modules (HSM)

HSMs are also known as Tamper Resistant Security Modules or (TRSMs), and because of their reliance in the financial services industry are another primary component of a CA. Built-in HSMs are highly effective in protecting and improving the private keys that are linked to all CAs. Scheirer, Bishop, and Boulton (2010) claim that PKI is currently the best way to ensure trust and HSM are the main ways to ensure trust in a PKI. They believe transacting without trust in the digital world is practically impossible, and to ensure trust, there is the need for assurance that displays:

- The transaction can be proven to have occurred
- There is confidentiality/privacy breach
- The intended transaction is the one that took place
- The entities performing the transactions are who they purport to be.

Transactions which are being carried out currently all depend on trust and trust relies on PKI and PKI relies on security modules. Security modules have to validate, store, and issue keys in protected environments. A security module can be either one of two types:

- Software Security Module (SSM)
- Hardware Security Module (HSM)

The main contrast between the two is that HSM is a computer specifically designed and dedicated to functioning in a security role. At the same time, SSM is a program that operates on a general-purpose computer (Rea, 2015). All the organizations which use HSMs to secure their PKI use it across the entire architecture of the company's PKI. NIST tries to make sure that cryptographic modules for CAs, OCSP, and Key Recovery Servers responders are modules of hardware that have been validating as meeting level 2 or 3 or higher of FIPS 140.

a. *The Function of Security Modules*

Security modules tend to provide PKIs with technological services and said modules generate keys. When systems like funds transfer systems request certificates to display to another bank that it is trustworthy enough to complete a wire transfer, the security module becomes the device that generates the private/public key for the certificate (Cooper et al., 2008). When the second bank receives the certificate, the bank uses a private key cryptography and security module operation to check the certificate and confirm whether the certificate is trustworthy. Security modules are typically utilized to find out whether or whether not it came from a trusted source that remains uncompromised. Security modules generate two keys by use of public-key encryption techniques. These keys possess mathematical relationships in such a way that a message with one key can only go through decryption by using the other (Cooper et al., 2008). Security modules carry out the following when signing messages with digital signature:

- Analyze message digests, which are fixed lengths of binary fields, by use of hash generator algorithms
- Carry out the encryption of the digest by use of the senders' private keys, combined in the signature are the names of the algorithm associated with hashing and the key which is public of the sender that is appended to the enciphered digest
- Carry out the encryption of the entire message (the signature and the message itself) by use of combined public and secret key cryptography (Rea, 2015).

The security module of the receiver carries out decryption of the key, which is clandestine using the private key of the receiver and decrypts the rest using the key, which is covert.

- The digest undergoes decryption through the public key of the sender
- Hashing is a one-way process; therefore, the message digest gets re-evaluated through the same hashing algorithm that the sender used

- The created digests from the above steps are compared; if they are similar, then this proves the authenticity of the signature (Rea, 2015).

The digital signature provides another layer of assurance of integrity. Any changes to the message will cause the digests not to match; it provides extra authentication because only the key holder can sign the message. The keys then must be generated eventually, stored, and put to use in a very secure manner (Rea, 2015).

b. Advantages of Hardware Security Modules

- Security Modules for hardware provide physical separation for key material and cryptographic operations.
- The hardware and software of HSMs are dedicated to specifically to providing cryptographic operations; it can furthermore be enhanced precisely for that determination.
- Hardware Security Modules also conduct cryptographic operations very fast and with more elevated assurance than their software counterparts.
- Hardware Security Modules have hardware that is specifically designed and dedicated to ensuring the generation of random numbers. And thus, can generate numbers with greater entropy than would be expected provided the hardware was not designed specifically for that purpose.
- Hardware Security Modules are devices for standard-compliant computing. The Federal Information Processing Standard (FIPS) 140–2A is a good example. FIPS 140–2A is a U.S. standard that covers the assurance and implementation of security mechanisms like tamper protection and algorithms (Lesjak, Hein, & Winter, 2015).

6. Public Key Certificates

In this continually changing universe of IoT, an additional layer of security is given by DCs, which are productive as well as practical. PKI is a security structure that is trusted

and comprises of programming, equipment, individuals, strategies, and approaches that are expected to oversee safely, create, store, revoke, and disperse trusted DCs and guarantee the administration of public-key encryption (Lopez, 2013). Ellison and Schneier (2000) assert that public-key encryption, along with DCs, has emerged as two ground-breaking technologies crucial for maintaining the security of networks; they work hand-in-hand and secure PKI. DCs are developed and used electronically and tend to cooperate by proving and providing the ownership of public keys. These certificates contain a wide range of information, which may range from the public key owner's identity to the owner's digital signature (Adams & Lloyd, 2007). These DCs operate in networks as passports. They can certify public keys ownership and thus create high levels of accountability, which can then be utilized to confirm the actual management of information.

One advantage of these DCs is that, just like passports, they cannot be forged. DCs help validates the identities of the people using the networks. They are electronic documents that comprise of information in relation to the proprietor of the key that is public; it helps demonstrate the owners' identity and marks the final aspects of the public key. DCs also have the capacity to transfer information into a centralized system that can guarantee better management of information for electronic businesses and online banking (Adams & Lloyd, 2007). DCs provides the signature of the sender and validates their identities. It is a great resource that improves accountability and, at the same time, provides network restrictions to unauthorized people.

DCs are applied to secure connected devices, for instance, printers, fax machines, servers, and routers for many years (Boldyreva et al., 2007). The propagation of smart devices has led to the emergence of IoT to be very complicated. One of the things that differentiate IoT from outdated networked structures is the level of diversity in the connected devices. Nevertheless, the similar layers located in traditionally connected ecosystems make PKI one of the best solutions for securing the Internet (Guida et al., 2004).

The capabilities of DCs have to be pre-defined carefully to make sure every certificate is in correct alignment with the policies and that they meet all the requirements of use, including subject name, object identifier (OID), period, and validity (Scheirer et al.,

2010). The nature of a high number of IoT devices insists that they get disconnected, and this nature disconnection can hinder the process of issuing new certificates. Therefore, it is crucial to make sure that all subscribers acquire the correct certificates on their first time, mainly because one does not get a second chance to install the right certificate on the previously disconnected devices.

According to Weise (2001, p. 13), “The most widely used format for DCs are those based on the IETF X.509 standards.” The degree of improvement of the utilization of DCs is developing fundamentally, and numerous innovators comprehend the immense value that these certificates give as far as authentication, integrity, and confidentiality in connection with information, devices, and identities that are in close association with the IoT. Organizations spend too much time and money in setting up enterprise PKI. However, this does not mean that this is ideal for IoT. For instance, X.509 certificates are not the only ones used to authenticate devices, users, or data encryption. Other options can be used when selecting authorization and authentication protocols and mechanisms. Latvakoski et al. (2014) drew attention to the fact that, for example, OAuth and OpenID and other technologies to be used for transport other than Hypertext Transfer Protocol (HTTP), which may include Constrained Application Protocol (CoAP) and MQ Telemetry Transport (MQTT). Nonetheless, the number of individuals who thoroughly understand PKI’s full importance in the IoT is not as much as expected. In summary, DCs are practical tools in today’s complex networks that require significant security levels.

7. Certificate Extensions

Certificate extensions give extra data inside a certificate and permit them to be custom fitted for the specific needs of an organization. It is vital to note that certificate extensions can influence the interoperability of certificates if a relying party does not recognize the structure or substance of the certificate extension. The sorts of data that will be found in a certificate extension incorporate policy, usage, revocation, and naming data, which give specific points of interest individual to an organization’s PKI (Weise, 2001).

8. Certificate Depositories (CDs)

Similar to a RA, a certificate depository is also optional however, it is arguably an important component of a PKI. According to Weise:

When the directory is controlled by the CA or RA, the certificate distribution process is greatly simplified. Rather than trying to distribute every certificate to a unique point, the CA simply updates the directory. A critical factor is that only the CA must have the authority to update or modify the directory, but the directory must be publicly readable. (2001, p. 14)

K. PKI FUNCTIONS

The following are four basic processes which are common to all PKIs:

1. Public Key Cryptography

One of the earliest forms of cryptography in ancient Egypt was used by priests substituting texts (Adams & Lloyd, 2007). Since then, new aspects of this feature date after World War II. In short, cryptography refers to using keys and encryption algorithms/ciphers for encryption and decryption of data; ciphers or algorithms are mathematical functions or formulas (Weise, 2001). It is imperative for IT pros (as well as regular users to have more than a fundamental understanding of the concepts of public-key cryptography, and its significance in the IoT. Public keys are associated with the field of cryptography, which is different from the traditional symmetrical key, which is also used in cryptography for security purposes (Adams & Lloyd, 2007).

a. Key Strength

The key strength is a critical calculation in cryptography. An insufficiently strong key will degenerate indeed the best-designed PKI. The level of the cryptographic quality of any key depends on its use, but in common, the following applies (Weise, 2001).

- Keys must be replaced before the time feasible to determine them through cryptanalysis to prevent potential compromise.
- A key must be replaced by a new key within the time feasible to perform a successful dictionary or brute force attack on the old key.

- A key must not be used to ensure the security or integrity of data where it is feasible to determine that key in a period less than the useful life of that data. (Weise, 2001, p. 16)

b. Encryption and Digital Signatures

The processes of encryption, coupled with the applications of DCs, are effective in the delivery of privacy as well as the verification of identities within a network. Encryption of data involves encoding the information in a manner that cannot be understood by anyone other than the intended receiver of the information. Corbò et al. (2018) believe the use of public keys is paramount in encryption of information within a network. This is because the keys provide rights of access to the information and enable an authorized person to be able to decode the information using the keys. Encryption is connected to the progression of transforming a message so that an addressee can read it and understand its meaning. Encryption involves various aspects that include the creation of one-time keys that are used for symmetric keys. This is important for sending long messages because the use of symmetric keys saves time as compared to asymmetric keys, which are much slower than symmetric (Goyal et al., 2006). It is also associated with the encryption process, which will take place by use of the symmetric key and involves the transformation of the information using the key.

This paper focuses on RSA because of its widespread use in e-commerce, and according to Schneier, of all the public-key algorithms, RSA, named after the three inventors (Ron Rivest, Adi Shamir, and Leonard Adleman) works for encryption and digital signatures and is the most popular public-key cryptographic system. Schneier asserts that RSA is not only the “de facto standard in much of the world,” but he also describes RSA as “by far the easiest to understand and implement. ... and gets its security from the difficulty of factoring large numbers.” (1996, p. 466). Additionally, Weise describes RSA as:

A public key cryptographic algorithm that is based on the hard mathematical problem of factoring composite number. . . The basic cryptographic feature of RSA is that it allows the encryption of clear text data with one key but decryption with the other. This basic cryptographic feature is what provides RSA its asymmetry. (2001, p. 15)

In brief, RSA encryption is the creation of ciphertext by one entity utilizing another entity's public key to perform the encryption. This process is critical since it permits numerous entities to send one entity encrypted messages without the need to trade secret/private cryptographic keys. In terms of digital signatures, according to Weise,

RSA digital signatures work in an inverse fashion from encryption. Digital signatures are generated by performing the encryption of some cleartext using one's own private key. This encryption allows one entity to send a message to many other entities that may then authenticate that message, without the need to first exchange secret or private cryptographic keys. The recipient simply decrypts the message with the originator's public key. (2001, p. 15)

2. Hash Functions

Another viewpoint of security incorporates hashing, which is a function of the digital certificate related to the development of a digest, which may be a representation of the complete message. Schneier (1996, p. 429) summarize the process as "A one-way hash function, $H(M)$, operates on an arbitrary-length pre-image message, M . It returns a fixed-length hash value, h . $h=H(M)$, where h is of the length m ." Hashing guarantees that all aspects of the message are recorded as it is transmitted to the intended recipient, making the message secure and changes are rapidly recognized and detected. Hashing adds to the system the digest, which provides an additional security guarantee by guaranteeing the message moves unaltered. As described above, aspects of authentication can limit the speed of information; with hashing, speed is increased as compared to the other methods that incorporate encryption (Messerges et al., 2002).

In IoT, systems speed is fundamental if the systems are anticipated to be convenient and reliable for the movement of data between devices. The digest is more often than not an encryption of the message, but it is done in an interesting way that makes it smaller than the actual message, meaning that it'll be simpler to move within the network (Messerges et al., 2002). The digest also utilizes the use of digital signatures. The evaluation of the digest ensures that the message is unaltered as it travels through a network, and the digest also maintains what is termed message integrity," which enhances trust within a network. According to Weise,

Given its general acceptance and incorporation in cryptographic standards, SHA-1 is a good example of a hash function. The purpose of SHA-1 is to provide a non-secret key-based hash. It is widely used in public key cryptography, especially in conjunction with RSA, where public key-based authentication mechanisms are required. (2001, p. 17)

3. Symmetric Key Encryption

Symmetric encryption algorithms such as data encryption standard (DES), Triple-DES, advanced encryption standard (AES), and International Data Encryption Algorithm (IDEA) supplement public key cryptographic frameworks and are utilized to perform encipherment of data for confidentiality. Of note, symmetric keys still play a noteworthy part in PKI execution despite the reality that they offer fewer benefits than asymmetric keys. The elemental characteristics of symmetric cryptographic frameworks utilized with PKI are that the symmetric keys are more often than not indistinguishable and are utilized for both encryption and unscrambling. In any case, because of this symmetry, the keys must be kept secret and shared only between two parties (Schneier, 1996). Figure 6 outlines the functionality of the Symmetric encryption algorithm process.

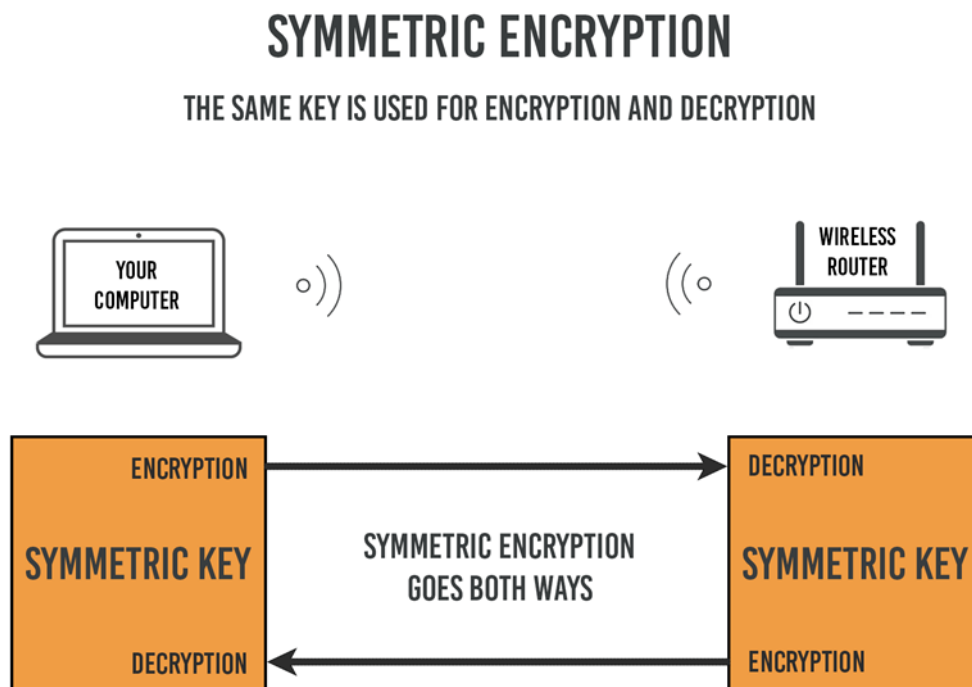


Figure 6. Symmetric Encryption. Source: TipTopSecurity (2017).

4. Asymmetric Key Encryption

In a PKI environment, both Symmetric and Asymmetric encryption are utilized. However, it is widely acknowledged that asymmetric encryption is more beneficial over Symmetric encryption and is typically used in digital certification and key management (Rea, 2015). PKI is a system that uses Asymmetric encryption (also known as public-key cryptography) and works in an unfathomably distinctive way. Conceptually, unlike Symmetric Encryption, Asymmetric Encryption includes the use of a cryptographic key pair to encrypt and decrypt data. Although a thorough analysis of the technical details of the cryptographic calculation utilized to create the keys is beyond the scope of this paper, nevertheless, it is imperative to note that the keys are mathematically connected, the public key is utilized to encrypt/scramble, and the private key utilized to decrypt/unscramble. Moreover, ordinarily, both the public and private keys are computed together at the same time, within the same mathematical process. This implies they are unequivocally related, scientifically talking. Hence, the keys can be utilized to encrypt/decrypt the same data, and also explains why public and private keys from diverse key-pairs would not work together.

To summarize, the encryption/decryption process is essentially a one-way process; meaning, when one of the keys (either public or private) is used to encrypt some data, only the other key can be used to decrypt the data. It does not matter who else has the public key since it is useless once the information has been encrypted. It can as it was be decrypted only with the private key, which is stored in a secure location. .Figure 7 shows a basic Asymmetric encryption operation. In this example, the public key encryption is used first to establish the connection, which is then replaced with symmetric encryption for the duration of the session.

ASYMMETRIC ENCRYPTION

DIFFERENT, BUT MATHEMATICALLY RELATED KEYS ARE USED FOR ENCRYPTION AND DECRYPTION

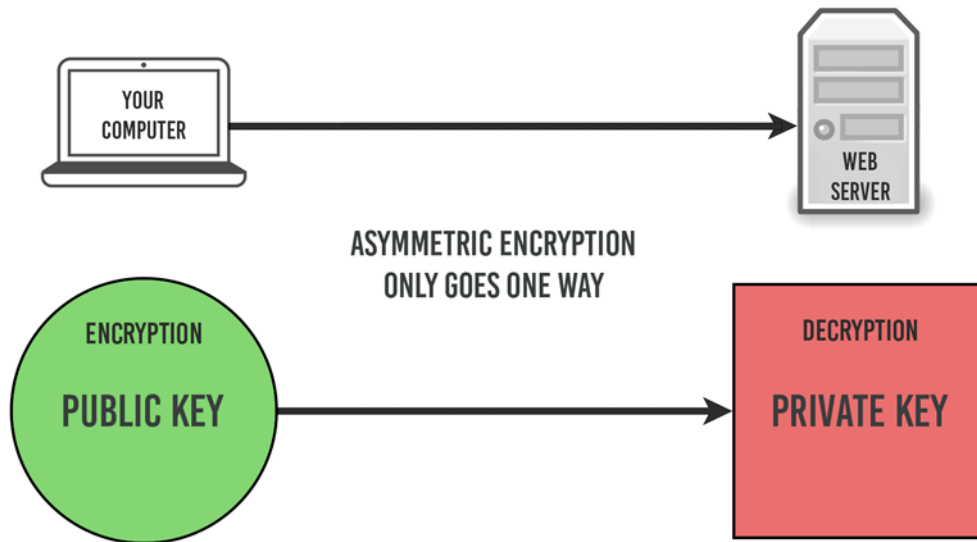


Figure 7. Asymmetric Encryption. Source: TipTopSecurity (2017).

5. Key Separation

The concept of key separation is that keys being utilized for particularly defined functions (i.e., encryption or decryption). This separation of duties makes a difference to isolate any misuse that will happen from the compromise of a cryptographic key and to dodge individual cryptographic assaults moreover. This partition is alluded to as compartmentalization of risk. In a well-designed PKI, to sanction a suitable level of risk compartmentalization, unique key sets ought to be utilized for encryption and digital signature generation (Weise, 2001).

2. Certificate Issuance

As mentioned previously, one of the primary functions of the CA is certificate issuance, which is the process of binding a public key to an entities including individuals, business organization, or to some other data.

3. Certificate Validation

Certificate validation is the process of guaranteeing the trust relationship or binding relationships exists and that a certificate is still valid for specific operations. However, the period taken for a certificate to be regarded as valid may uncover the quality and strength of the utilized algorithm. For short-term certificates, a more robust algorithm is fundamental, and a weaker one may just do the work. Certificates that require a longer time tend to require roughly 250 bits of strength (Kumari et al., 2017). Most organizations and companies select to utilize a National Institute of Standards and Technology (NIST)-proven minimum standard of cryptography; a set of guidelines are published by NIST, which help in distinguishing the leading choices. Elliptic Curve Cryptography (ECC) is among the most excellent ways to obtain higher security levels in an environment that's low-powered. This, in any case, depends on the capabilities of the cryptography.

4. Certificate Revocation

As the title propose, certificate revocation cancels an already issued certificate and either distribute the cancellation to a CRL or empowers an Online Certificate Status Protocol (OCSP). In fact, according to Dener et al. (2011, p. 122), “a Validation Authority, or Directory: Confirms whether a specific certificate produced by this CA is still valid or not (e.g., lost or compromised private keys, or change of information contained).” When the planning procedure is devoted, indeed, a big CRL does not need to be clumsy. For a vast CRL, one has to make contemplations such as configurations of the most current CRL extension within the certificates provided. When one uses an overhauled CRL, they can disperse as it were the changes to the base CRL. This helps in minimizing network update and load times and helps keep the list of revocation more current (Scheirer et al., 2010).

An OCSP gives clients with server approaches instead of pushing a list of canceled certificates, which empowers one to discover out on the off chance that a certificate is canceled. This will empower some aspect of consistency and predictability within the revocation activity without the need to exchange the total base within the newest CRL point of distribution. The issue is that the OCSP approach is more of a baggage balancing attempt and things adjusting endeavor. Since this can be a client-server utility containing a crypto

operation implanted to each authentication check, guaranteeing that the server is appropriately measured to sign the fundamental sums of reaction is fundamental. OCSP has the penchant for being hindered down by morning smart cards, which utilize OCSP legitimacy checking since of an undersized server (Kumari et al., 2017).

Another great practice is OCSP stapling. This process empowers the certificate presented to add or 'staple' time-stamped OCSP response reaction signed by the CA to the TLS handshake. This could dispense with the got to contact the CA, whereas the requester of the certificate can depend on the affirmation that's unquestionable from the CA straightforwardly. Stapling further helps decrease the issue of privacy that's connected to pattern checking of utilization and does this in a more successful way from a network traffic activity point of view. One must arrange for denial of certificates if required carefully. For the arrangement of an IoT, one ought to arrange for larger CRLs and guarantee the CRL focuses of distribution or the CDPs resolvable all around by use of ubiquitous protocols like file transfer protocol (FTP) or hypertext transfer protocol (HTTP). At that point, one ought to utilize OCSP to shape and control the traffic of network revocation (Hong, 2013).

L. PUBLIC KEY CERTIFICATE BINDING

1. Entity Authentication

Entity authentication, confirmation, and enrollment can be a severe issue. This depends on the risks of an organization and is reflected in their CA. In case an adequate level of validation does not happen amid the original identification and authentication of an entity, any ensuing reliance on the qualifications and certificates issued to that character might be suspect. In case there is a small negative result to the issuance and use of a certificate, for illustration, leasing motion pictures from a video store, there may be as it were a straightforward entity authentication process. Alternately, the issuance of a certificate for use by a visa office may be more robust if that is a nation's, to begin with, line of defense against cyberterrorists. As a fundamental matter, in case an organization is endeavoring to reproduce an existing manual method that requires identity validation, for illustration, to open a reserve funds account at a bank, they ought to imitate the same

process they utilize nowadays. The method may be computerized or manual, but the credentials required and the due constancy processes are the same (Weise, 2001).

2. Certificate Generation

To generate a certificate, the CA performs the following steps

1. Acquire a public key from the end entity
2. Verify the identity of the end entity
3. Determine the attributes needed for this certificate, if any
4. Format the certificate
5. Digitally sign the certificate data. (Weise, 2001, p. 19)

3. Acquiring the Public Key

Depending on the value proposition and commerce dangers related with the issuance of a public key certificate, the CA may take vital measures when getting the specified recognizable proof and certificate data. For example, the CA may permit it to be sent electronically, or utilize more modern means such as utilizing fortified/bonded messengers (Weise, 2001).

4. Verifying the Identify of the End Entity

Once more, depending on the value proposition and commerce dangers and the sum of dependence on the public key certificates, the CA may take basic measures to confirm the end entity. For example, they may essentially take the entity's word that they are who they say they are, or the CA may established more exacting measures, such as a detailed due diligence process as the business proposition merits. In any case, the most imperative figure within the authoritative handle is to guarantee that an entity's identity is verified unambiguously (Weise, 2001).

5. Formatting the Certificate

Before the certificate is signed by the CA, all information to be set into the certificate is collected, organized, and formatted. The particular information and format of a public key certificate can change depending on desires of the PKI (Weise, 2001).

6. Signing the Certificate

At long last, the certificate is carefully signed with the private key of the CA utilized for signing certificates. Once signed, it can be dispersed and/or distributed utilizing distinctive vehicles (Weise, 2001). Figure 8 delineates the structure of a X.509 Computerized Certificate.

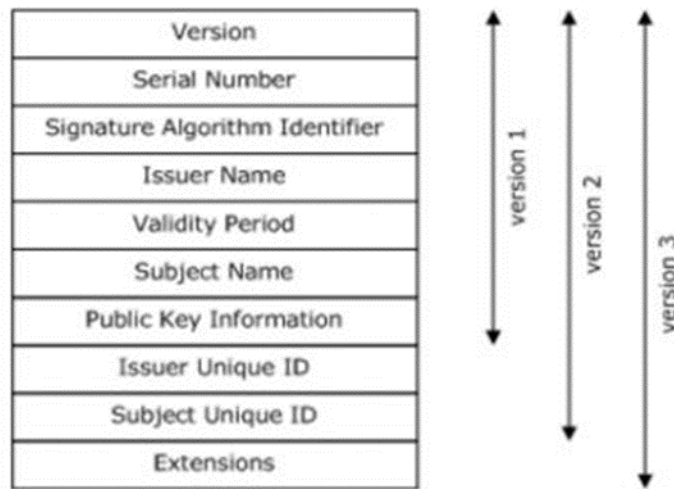


Figure 8. Structure of a X.509 Digital Certificate. Source: Afshar (2015, p. 11).

M. PKI'S FLEXIBLE DEPLOYMENT

PKI is highly implementable, free to adopt, and has an open standard and can be extended and customized. This makes it the obvious choice for organizations aiming to add their system's connectivity, smart devices, and services. All IoT devices are different regarding their implementation and utilization. However, PKI provides numerous flexible deployment options to cater to the critical encryption and authentication abilities of unique devices. The network connectivity availability, the internal memory of a device, the computational power, the regular updates, and maintenance are among the crucial factors which impact IoT devices' deployment (Housley, 2004). The platform flexibility, availability, and performance vary significantly throughout different CAs. Of course, when selecting a PKI, organizations can select between acquiring standalone PKI frameworks

for in-house deployment and outsourcing an integrated PKI platform (Dener et al., 2011). Several of these differences include:

- OIDs, custom profiles, and usage fields
- Longer and shorter certificates validity periods
- Subject fields for custom certificates
- Stronger cryptographic algorithms and hashes
- Certificates algorithms and hashes that are direct-to-root chained
- Increased availability of spreading of amenities globally and systems
- Trusted revocation options and roots that are flexible
- Certificates that are scalable up to millions as well as billions (Chokhani et al. 2003).

Also, several protocols of certificate management are in existence as a fragment of a safety device distribution procedure and enrollment:

- Enterprise Application Programming Interface (API)
- Enrollment over Secure Transport (EST)
- Simple Certificate Enrollment Protocol (SCEP)
- Certificate Management over CMS (Chokhani et al., 2003)

The security given by PKI enables an assortment of approaches to deployment, which makes PKI one of the foremost adaptable and appropriate arrangements for IoT security; it can be efficiently executed during the process of device manufacturing or moreover be remotely conveyed amid a client's initial setup (Housley, 2004). Figure 9 delineates the essential components required to set up a PKI.

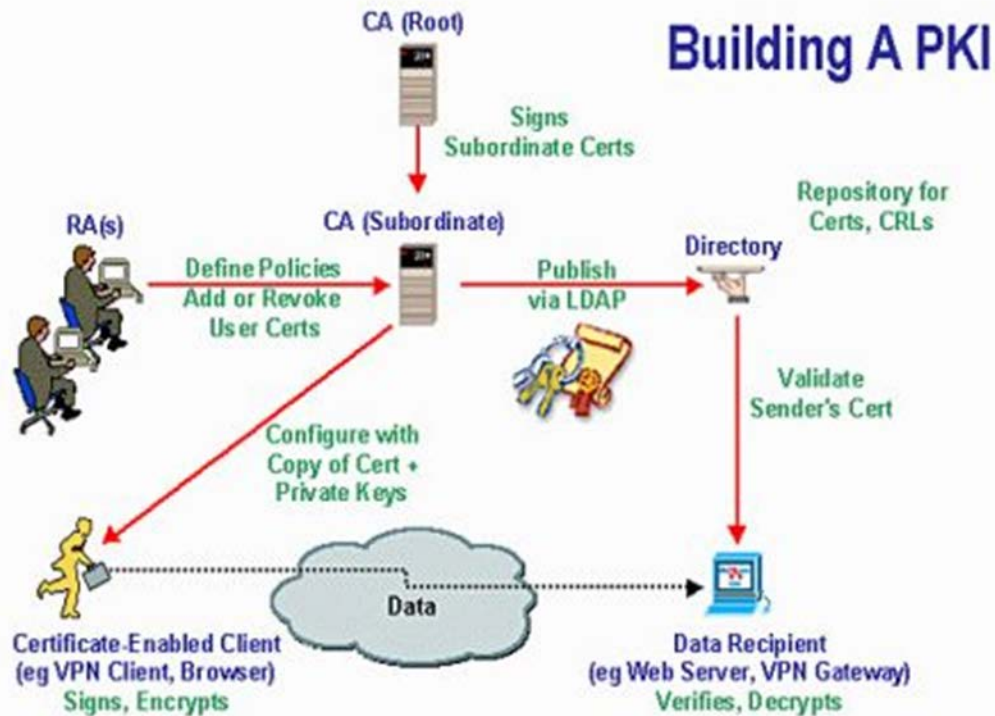


Figure 9. PKI Components. Source: Afshar (2015, p. 6).

N. AN EXAMPLE OF A PKI IN ACTION

The following example, provided by Weiss (2001), is public-key cryptography for both confidentiality and integrity. The reason for this case is to demonstrate how public-key cryptography instruments can be utilized in a PKI. In this case, both parties, Alice and Bob, share a common trust point; that is, they both utilize the same CA to have their certificates signed. Thus, they do not have to assess a chain of trust to decide the validity of any other CA. Precursor Steps:

1. Alice and Bob each generate a public/private key pair.
2. Alice and Bob each provide their public keys, name, and descriptive information to an RA.
3. The RA validates their credentials and forwards the certificate requests to the CA.
4. The CA generates a certificate for Alice and Bob's public keys by formatting their public keys and other information, and then signs the certificate with the CA's private keys.
5. The results of this operation are that Alice and Bob each have a public/private key pair and a public key certificate. (Weise, 2001, p. 22)

Alice and Bob each generate a secret symmetric key. Presently, Alice and Bob each have a public/private key combination, a computerized key certificate issued by a common trusted third party (i.e., the CA), and a mystery symmetric key. Assume presently that Alice wishes to send Bob a few bits of information he will depend upon and hence requires an assurance of integrity; that is, the substance of the message cannot be changed. Alice and Bob moreover need the confirmation of confidentiality and need no other parties to be able to see that data. A contract for merchandise and administrations where parties concur upon cost, time, and value exchange could be a great illustration of such a process (Weise, 2001). Figure 10 illustrates Alice sending data that needs confidentiality and integrity to Bob, using a digital signature (steps 1–5).

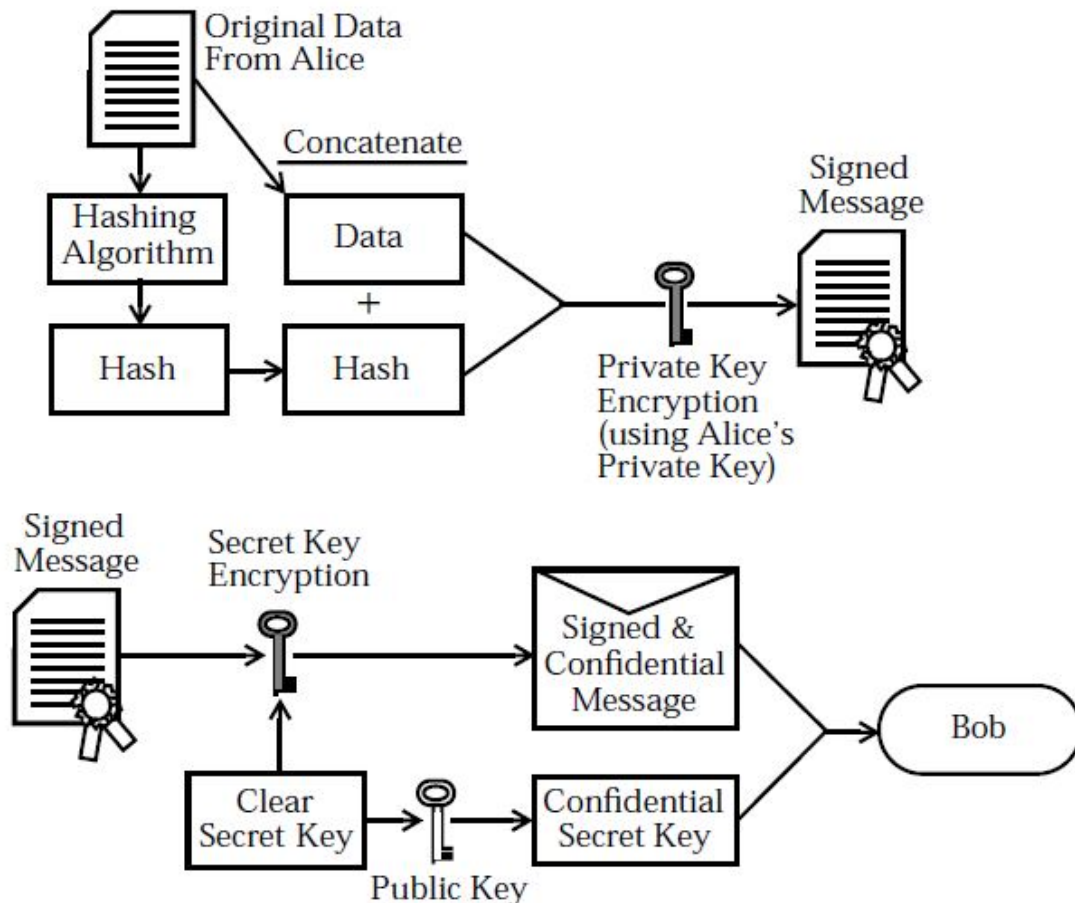


Figure 10. Overview of Using a Digital Signature. Source: Weise (2001, p. 25).

Afterwards, Alice takes the message, formats it in accordance with the convention rules she and Bob have concurred to and after that hashes the message. The hash gives a unique value for the message and will afterward be utilized by Bob to test the legitimacy and integrity of the message (Weise, 2001). Figure 11 outlines Bob unscrambling the information and comparing hashes (steps 6–10), Figure 12 illustrates the process to issue DCs, and Figure 13 outlines the working of DCs.

1. Alice takes the message in question, formats it according to the protocol rules she and Bob have agreed to and then hashes the message. The hash provides a unique value for the message and will later be used by Bob to test the validity and integrity of the message.
2. Alice concatenates the message and the hash and then signs (i.e., encrypts) these with her private key. This signing provides message integrity because Bob is assured that only Alice could have generated the signature because only Alice has access to the private key used to sign the message. Note that anyone with access to Alice's public key can recover the signed message and so, we have only established message integrity at this point, but not confidentiality.
3. Because Alice and Bob would like to keep the message confidential, Alice encrypts the signed message and hash with her secret symmetric key. This key is only shared between Alice and Bob and no one else. Note that enabling confidentiality can be implemented through various techniques and protocols. In this example, a symmetric key is used because it can be more efficient than using a public key for encrypting lengthy messages such as the purchase order here.
4. Alice must provide Bob with her secret symmetric key to enable Bob to decrypt the message encrypted with that key. Alice signs (i.e., encrypts) her secret symmetric key using Bob's public key. For this example, we assume Alice obtained Bob's public key previously. This generates what is known as a digital envelope and which only Bob can recover (i.e., decrypt) because only Bob has access to the private key that is needed to recover the digital envelope. Remember, what is done with one key of a pair can only be undone with the other key of the pair. This provides confidentiality over the transmission of Alice's secret symmetric key to Bob.
5. Alice forwards to Bob the original message and the hash that are both encrypted with her secret symmetric key and the digital envelope containing the secret key encrypted with Bob's public key. (Weise, 2001, p. 23)

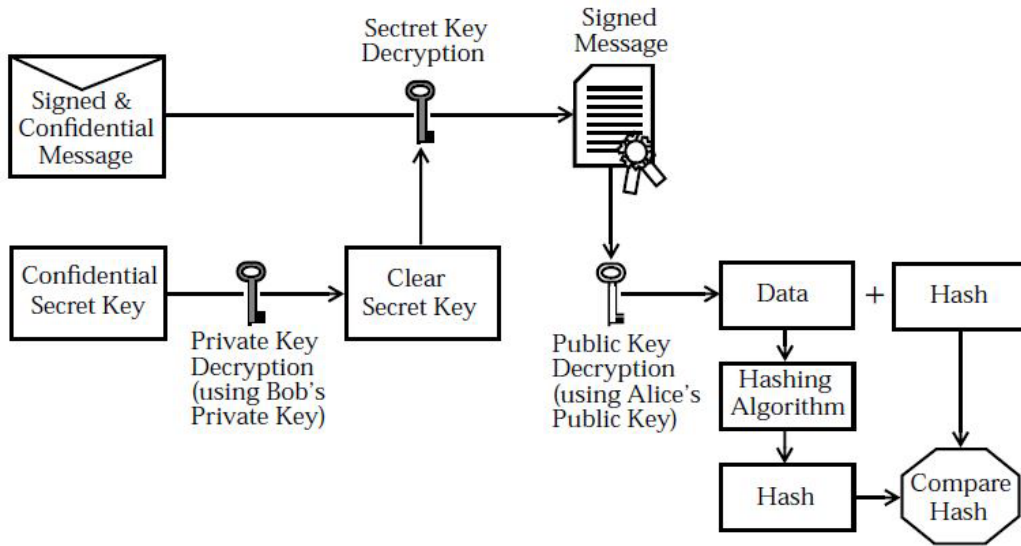


Figure 11. Overview of the Decryption and Hash Comparison Process.
Source: Weise (2001, p. 26).

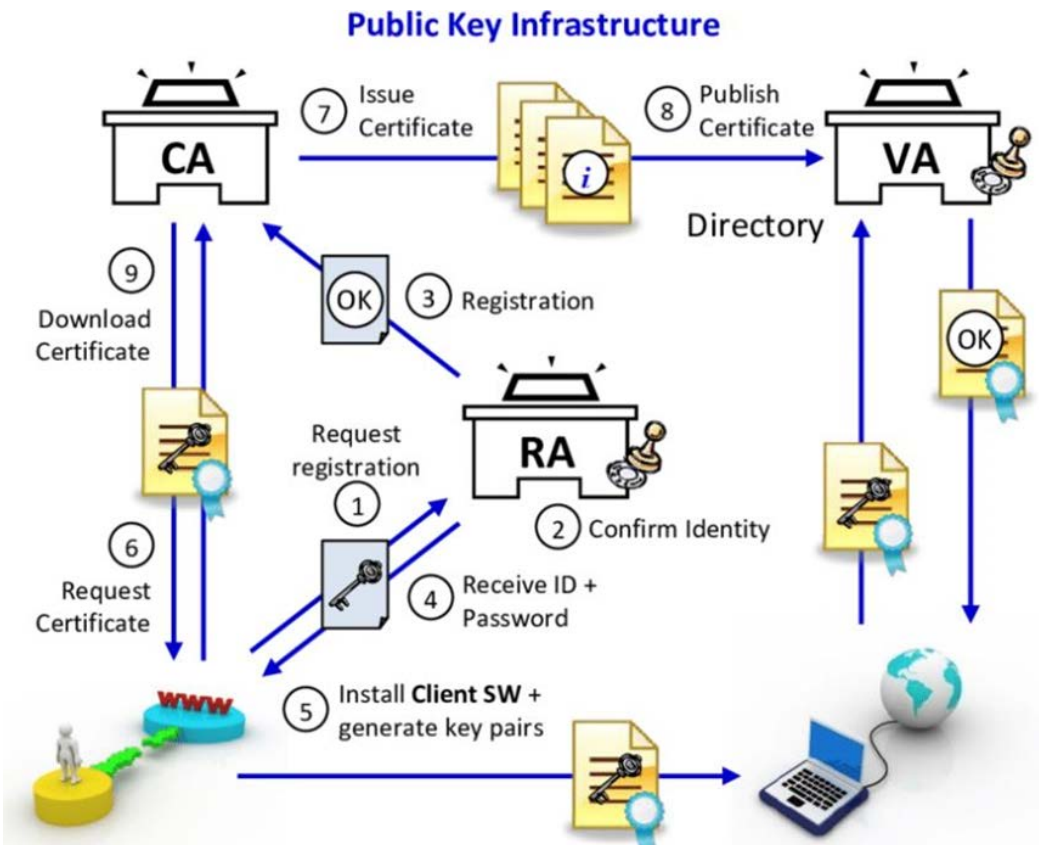


Figure 12. PKI Process to Issue Digital Certificates. Source:
Dener et al. (2011, p. 122).

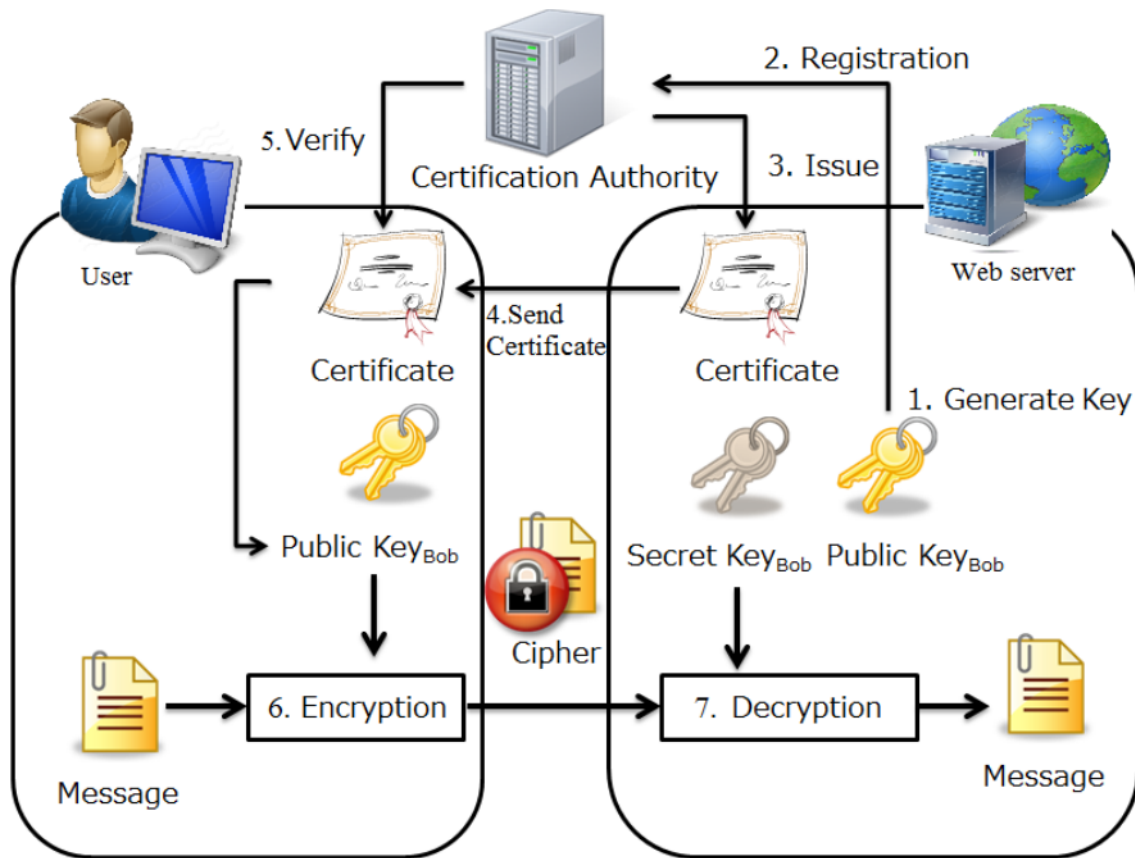


Figure 13. Working of Digital Certificates. Source: Afshar (2015, p. 14).

When talking about PKI, assurance signifies the level of certainty that the system or an individual that the identity of a certificate belongs to the device in question. Guaranteeing the assurance of a wide range of devices is not a straightforward assignment; hence, it is pivotal to ensure that mitigation plans are developed and executed. The framework of the IoT works by combining millions of various gadgets that share standard information. Hence, it is no shock that dangers tend to be higher for IoT frameworks than for ventures. As a result of the higher IoT risk, the environment of PKI, which should provide trusted certificates all through the framework, licenses cautious security planning to create beyond any doubt there is a defined assurance level for authentication of devices. It is not an option to characterize the levels of assurance required for complex frameworks of IoT. Organizations need to characterize the correct amount of assurances in order to let the depending parties be able to understand why the certificate is trusted, conjointly to

comprehend the tasks the device is expected to accomplish and not finish (Adams & Lloyd, 2007).

O. PKI FOR MOBILE, CLOUD AND IOT

The advancement in the development of PKI services has made it easy for many organizations to access the services of PKI, and thus DCs, which offer great opportunities for reducing significant security vulnerabilities offered by mobile devices (Rao et al., 2012). With DCs and other security aspects of PKI, the burden aspect with technological aspects of security is minimized, and at the same time, the experience that users get is highly improved. Today, many organizations are trying to find ways to leverage mobile devices and systems of IoT to establish new business opportunities. There is a great value that results from the systems of IoT, and this is associated with the development of new business opportunities and enhanced communication (Zhang & Yu, 2013).

Successful, large-scale deployment of IoT will likely be affected by cloud computing, mobile innovations, and any associated potential vulnerabilities. Consequently, cloud computing will apply a more remarkable impact on system security since most large-scale information centers are planned to utilize different locales with the same IT items and computer program setups over scattered areas. Cloud computing is portrayed as a decentralized network model for empowering on-demand access to a shared pool of computing control that separates computing assignments among all the computers without a central computer or server. For example, expansive information centers, such as those possessed by Amazon, will make opportunities to exploit critical infrastructure vulnerabilities exceptionally appealing to cybercriminals (Rao et al., 2012). Consequently, complex operations and assets are required for a complex framework of security; DCs offer the best source of security, and that is the main reason that PKI is fundamental as a security solution for mobile cloud and other important aspects of the IoT (Rao et al., 2012).

Cloud-based services have grown as a solution for access to resources such as expensive software and storage facilities (Rao et al., 2012). The rise of digital business has led organizations to push technological boundaries that have created enormous demands

for cloud technologies. These advancements have led to the deployment of better PKIs that combine important aspects of trust and technology to ensure that information is protected.

In relation to mobile technology, it is evident that soon, computers will be replaced by mobile devices as the primary devices for computational purposes (Rao et al., 2012). The spread of mobile technology has grown so fast that the organization has forgotten how dangerous mobility can have on the security and privacy of a network. Old security measures associated with the username and their corresponding passwords have become insufficient in providing security for these devices. In this case, PKI is a system that has proven to be effective in the management of security and can be effectively implemented in mobile devices to provide security and privacy solutions. Today, mobile operating systems apply the use of DCs as factors to enhance the security of these devices.

The IoT has critical differences from enterprise PKIs regarding the life cycle planning of the certificate. Managing, planning and implementation of a typical enterprise certificate for PKI life cycle can at times be made simple the way it has been done before for the same instances, and it is restricted to the renewal, retrieval, and cancellation of certificate issuance (Scheirer et al., 2010). Many commercial trust models' elements can be dealt with using the mechanisms which are the default. However, the management issues of certificate life cycle for the IoT provide challenges based on different touchpoints and events such as:

- Device manufacturer—the creation of security repository
- Device delivery—complete manufacturing of a device
- Device maintenance—here operational cycles such as renewal and rekeying take place
- Retirement—identity is revoked or removed
- Device design—certificate planning and content
- Integration—pair identity with a particular device

- Device deployment—device undergoes the production phase (Scheirer, 2010).

P. PKI AVAILABILITY AND SCALABILITY

Millions of certificates are issued by IoT PKIs for small things such as valves, sensors, applications, and circuit boards (Adams & Lloyd, 2007). While the inability of an enterprise PKI to offer a new certificate only affects a small subset of less critical operational functions, a similar event on IoT PKI leads to the disabling of the entire assembly line. For example, researchers compared the inability of five employees to access the Wi-Fi connection in a meeting room with losing \$1 million in revenue for every two hours of manufacturing time that is interrupted (Adams & Lloyd, 2007).

A PKI has huge scaling impacts and can successfully service an IoT system. All the components of an IoT should be tailored to manage and issue a particular degree of certification that is several times the average size of the largest known enterprise PKI. The components have to be available per minute or per second rates of enrollment, which far exceeds the enrollment keys for enterprise PKIs. Other than being scalable, IoT PKIs also have to be available.

- **Certificate Authority Considerations**—being able to scale out from the standpoint of certificate issuance implies that clustered logical CAs can be developed and be able to answer API requests for new enrollments. Thus, the failure of a single node means that another one takes control to ensure the CRL signature is still able to occur. This ensures availability and scalability.
- **Server scaling**—the enrollment of certificate has to be able to keep up with the pace of high amounts of requests. When handling a CA that has hundreds of millions of certificates that are subordinate, choices regarding the management of this number of requests need to be made. A critical point to note is whether or not the certificates should be put into documentation. If this is the case, how will this be done, and where will they live? Alternatively, the process of enrollment could be automated without necessarily having to store the certificates in the CA database. The certification enrollment process can

also be sped up and automated by interfaces to the systems of other businesses (Adams & Lloyd, 2007).

Q. POTENTIAL PKI AND IOT CHALLENGES

Whereas IoT can supply benefits, the danger to components, devices, and IT systems and foundation is expanding as the IoT grows. The colossal volume of multifaceted information being transmitted depends broadly on different Web innovations and a robust wireless communications foundation. PKI that is required by the IoT is a sharp contrast from a basic Enterprise PKI. Consequently, in order to achieve a level of integration and cooperative vitality, IoT communications hardware utilized in transmission, collection, and lodging of information (e.g., servers, sensors, smaller than expected processors, information capacity gadgets) must be secured. Agreeing with Jeevitha (2017), most devices that are utilized within the transmission, collection, and housing of sensitive/ delicate, exclusive, or individual data, will transverse cloud services and decoded systems with diverse security prerequisites and security levels even though a few of these gadgets will be blocked off physically. In contrast, others may be savvy sufficient to imitate and, in this way, get access to the assets of IoT frameworks. The following are some challenges that can assist organizations in planning for certificate policies where the PKI environment will eventually be based.

1. Physical Security

- How to ably secure devices from physical tampering

2. Device Integrity

- How to make sure the devices used to communicate with the system of IoT are the right ones and not imposters.
- How to make certain the participants of the IoT system are genuine

3. Data Security

- How to make sure that data is and does not get manipulated

- How to guarantee the safekeeping of the data consumed and produced by the system.

To summarize, Chapter II embarked on a literature review that was meant to generate critical insights to enhance the understanding of PKI and IoT. Among the key areas analyzed was the understanding of the emergence and evolution of the IoT and its impact in the modern era. IoT has experienced much growth and acceptance since the 1930s, fueled by the massive growth. However, the growth in IoT has posed significant challenges to Internet security, as evidenced by increased cybercrime. Other causes of insecurity include insecure deployments that consist of collections of devices that are identical or nearly identical. This collection homogeneity increases the potential outcomes associated with vulnerabilities caused by security issues as a result of the number of devices with similar trials. As a result, PKI was developed as a special protection tool to address IoT security challenges. PKI's emergence and function have also been discussed and other DCs that have been used alongside PKI. Data insecurity and various types of threats to the security of the IoT have been discussed in detail to set a transparent background that shows the need for a more complex and advanced source of security for Internet-based systems.

To understand the effectiveness of using PKI as a protection tool, Chapter III describes the methodology that will be used to collect primary data that will be analyzed to test the major hypothesis. The chapter will describe three key methods; interviews, questionnaires, and case studies that will be used to collect data from the target audience. The primary target for the study will be companies that have already adopted PKI as a means to protect their Internet-based systems.

III. METHODOLOGY AND FINDINGS

A. METHODOLOGY

In Chapter III, the methodology used in the data evaluation and data collection is explained briefly. It describes the techniques, data target population, collection, sampling, data processing, and data analysis. Additionally, this section also briefly presents the limitations and problems which were experienced through data collection.

The research study used both aspects of qualitative and quantitative methods; hence it utilized a mixed-methods approach to collect useful data for the study. This is an approach that incorporates both aspects of qualitative and quantitative research and was beneficial because it created a better understanding of the phenomenon under study (Tashakkori & Teddlie, 2010). It helped break down the topic of study into facets that were easy to explore. The research method explores the aspects of the development of synergies in research and uses the strength of each of the research methods to find and develop successful results (Creswell & Clark, 2017). This research, therefore, conglomerates the assortment and examination progression of both qualitative and quantitative data.

Mixed-Method—the mixed methods research design is dependent on the ability to provide alternative designs of collecting and analyzing information, thus proved very significant in conducting thorough research (Creswell & Clark, 2017). It is also responsible for the high levels of communication during research that promotes more success in data collection, and this was evident in the smooth running of the research. It is integrative and leads to the visualization of the designs, therefore, offering a better perspective and understanding of the research (Tashakkori & Teddlie, 2010). Well-designed mixed methods are characterized by aspects of substantially integrated data, the collection of a broader range of data from both quantitative and qualitative methods. Johnson, Onwuegbuzie, and Turner (2007) argued that mixed methods are among the three fundamental paradigms, that is, qualitative research, quantitative research, and mixed methods.

Moreover, blended strategies enhance the perspective of the research by broadening the scope of the research because it offers more investigative approaches and utilizes way better strategies of information collection (Tashakkori & Teddlie, 2010). Blended strategies can moreover, permit analysts to utilize subjective information to investigate the discoveries of quantitative information. This happens when the strategies are carried out successively, meaning that one builds straightforwardly on the other. Blended strategies moreover, give an all-encompassing approach competent in reaching more respondents and, thus, help gather more information. The blended strategies plan received different apparatuses of information collection that included the use of:

Surveys—surveys contained both closed and open-ended questions were deployed to IT technology specialists and mobile operators at companies that deal with network security. The researcher leveraged her access to active duty IT sailors and DoD Civilians, and also leveraged her membership in professional credentialing organizations to reach a broader group of IT subject matter experts. The respondents were required to respond to a series of questions that were designed to collect essential data on the data security measures used by these companies. The primary objective of the data collection was to gauge the respondents' attitudes and beliefs regarding the efficacy of PKI's adoption and application on the IoT.

Interviews—a different set of companies was selected for the interviews. For each company, interviews were conducted with the top management comprising of 10 senior staff members. The interviews collected data about the strategies utilized in these companies to ensure that their data is safe from malware. Also, the interviews sought to establish whether these companies were aware of and utilized PKI services to secure their company data.

B. FINDINGS

This paper seeks to establish the effectiveness of using PKI on IoT devices as a protective measure. While PKI certificates have been frequently used by organizations as a means to protect their IoT devices, the advancement of the technology underlying IoT-enabled. From the data obtained from the research and literature review, it is evident that the role of PKI on IoT cannot be underestimated. Furthermore, an emerging body of research indicates an increase in the reliance and applicability of PKI as a vital enterprise asset and a root of trust. A root of trust is vital because, an IT supply chain includes all information, systems, people, processes, facilities, and communication and shipment channels involved in the specification, creation, sales, distribution, delivery, servicing, maintenance decommissioning, and disposal of IT products to their purchasers' or acquirer's (Adams et al., 2000).

1. Survey Respondent Demographics

- The primary target population for this study was mid-level and senior management of companies that have already embraced PKI services as a means to protect their devices.
- The target population worked for organizations that possess a lot of regulatory compliance requirements to protect their data, for information security, and for privacy.
- While surveys were administered to the companies' IT specialists to collect data regarding their experiences with PKI, interviews were conducted using personnel from five companies. Five companies were network administrators, with an average of 60-person start-ups, one company was a CIO of \$80 million, and the other four companies were Internet-based with their worth ranging between \$45 and \$60 million.

Only five survey questions are included in this section; we list five for concision and analysis purposes. See the Appendix for the full list.

1. What is the IoT, and is the IoT relevant in today's world?
2. What are some of the known issues which affect the implementation and development of IoT, and which the correct framework to solve the issues?
3. What is PKI, and how does it work?
4. What are some of the common challenges affecting the use of PKI?
5. Is PKI the solution to solve the security, privacy, and authentication risks of the IoT objectives?

The following problems were specific challenges encountered during this research:

- Non-response bias: the following survey results are founded on a particular example of survey yields. Surveys were sent to a sample of Internet security and IT practitioners in different locations; there is always the chance that those who did not participate possess different beliefs from those who participated in the survey.
- Sampling frame bias: the exactness of the outcomes of the investigation depends on the degree to which the sampling frames are representative of the people who have claim to have IT or IT security skills.
- Self-reported results: the quality of the research is dependent on the integrity of responses that are confidentially acquired from the respondents.

2. Analysis of Survey Responses

The research confirmed that PKI might be a useful tool in improving secure communication between bunches of interconnected devices or computing hubs. Organizational communication is made secure from access from noxious people by ensuring that only the respective individuals have access to the decryption key. Be that as it may, this scheme is confronted by the challenge of conveying its public key so as the

receiver of the message is sure that it is from its exact origin. To guarantee the authenticity of the message, a reliable and trustworthy third party should be included to ensure the integrity and authenticity of the public key. A PKI comes in to serve this reason; however, in any case, selecting a suitable vendor for PKI and PKI deployment requires a thorough investigation, and business preparation and planning to actualize the PKI innovation. Entities must begin with an understanding of their security needs as this will be vital to dodge the challenges identified in a previous section of this paper. Figure 14 shows the number of respondents who knew the answers to the open-ended questions listed in the Appendix. It is important to note that when the analyst says knew the answers, she is referring to survey respondents that knew the textbook definition for the distinctive terms and expressions.

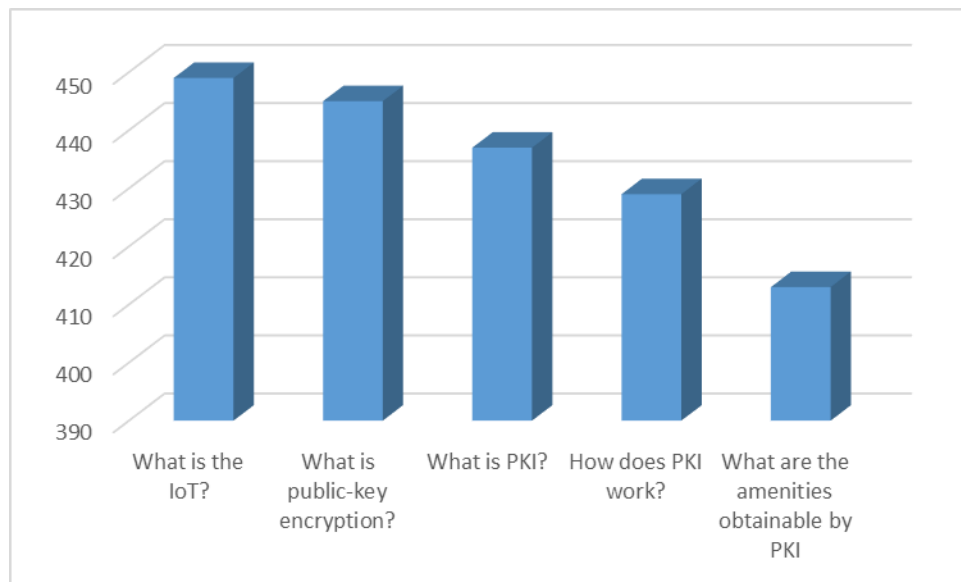


Figure 14. Accurate Response Rate for Open-Ended Survey Questions

Question? What are some of the common challenges affecting the use of PKI?

According to the data, one of the essential challenges influencing the utilization of PKI is caused by necessities of industry compliance on the choice of PKI deployment strategy. When the respondents were inquired to distinguish the common challenges influencing their decision to utilize PKI, almost 48% (215/449) of respondents said that the greatest issue is external standards and mandates. .

An additional key takeaway is that the PKI's certificate revocation function lacks clear ownership; almost 55 percent (247/449) survey respondents think certificate revocation status checks are handled by the OSCP, followed by 45 percent (202/449) of the respondents who claimed that most organizations they know off use automated CRLs. Figure 15 is a breakdown of survey respondent's response.

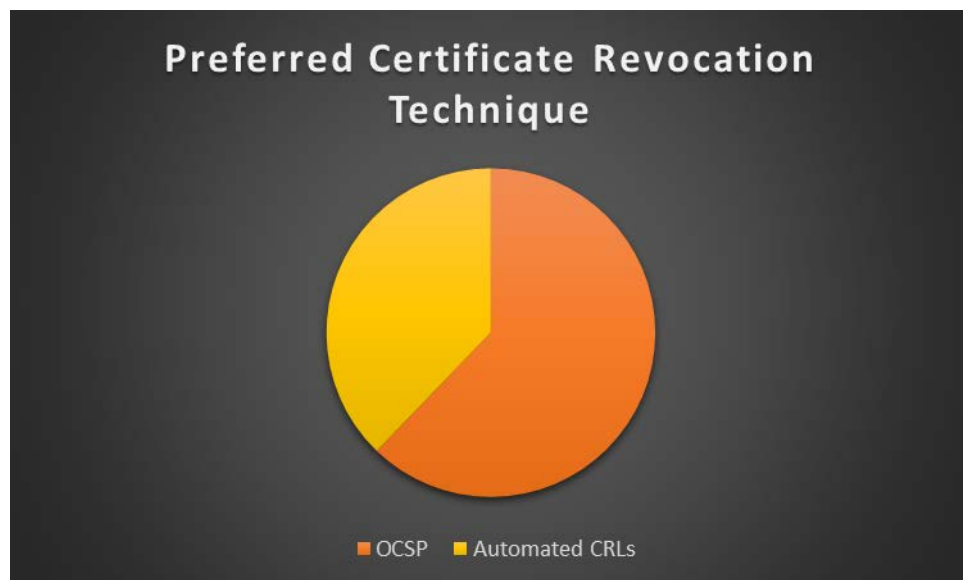


Figure 15. Technique Best Suited for Revocation of Digital Certificates

Question: What are some of the known issues which affect the implementation and development of IoT, and which the correct framework to solve the issues?

Figure 16 shows FIPS 140 is followed closely by the Common Criteria for Information Technology Security Evaluation (Common Criteria), which is supported 66.5 percent (299/449), and 33.5 percent (150/449) respectively.

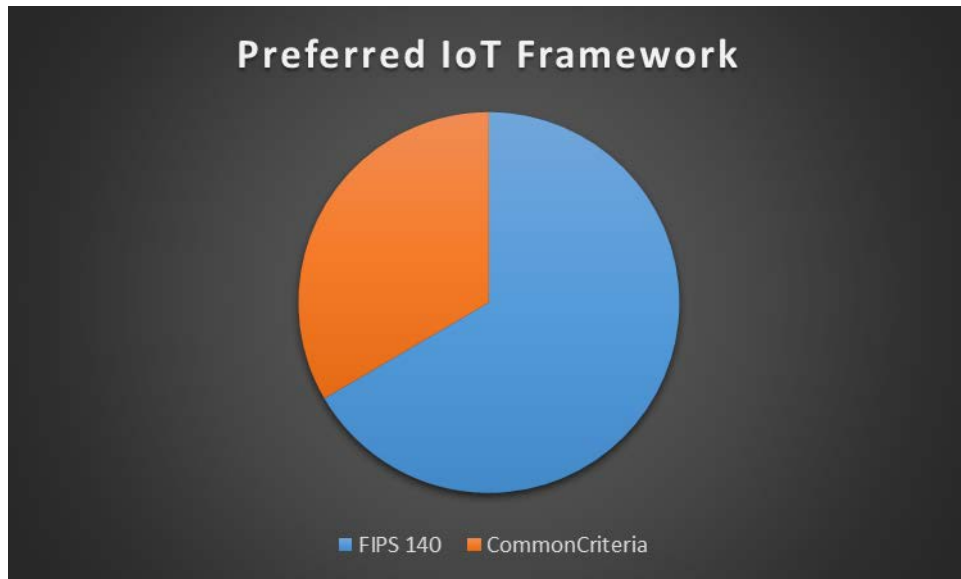


Figure 16. Preferred Framework to Solve IoT Security Risks

Question: Can PKI solve the security, privacy, and authentication risks of the IoT objectives?

By an overwhelming margin, 85.7% (385/449) agree that the development of PKI is significant, is practical and useful for IoT, and PKI can solve the security, privacy, and authentication risks of the IoT objectives. However, it also shows that 14.3% (64/449) do not think PKI is 100% effective—meaning, they believe PKI is one of several essential components of an overall defense-in-depth security strategy on which other applications, systems, and security components are built to solve the security, privacy, and authentication risks of the IoT objectives. Figure 16 shows the breakdown of the total response rate of 89.8% (449/500).

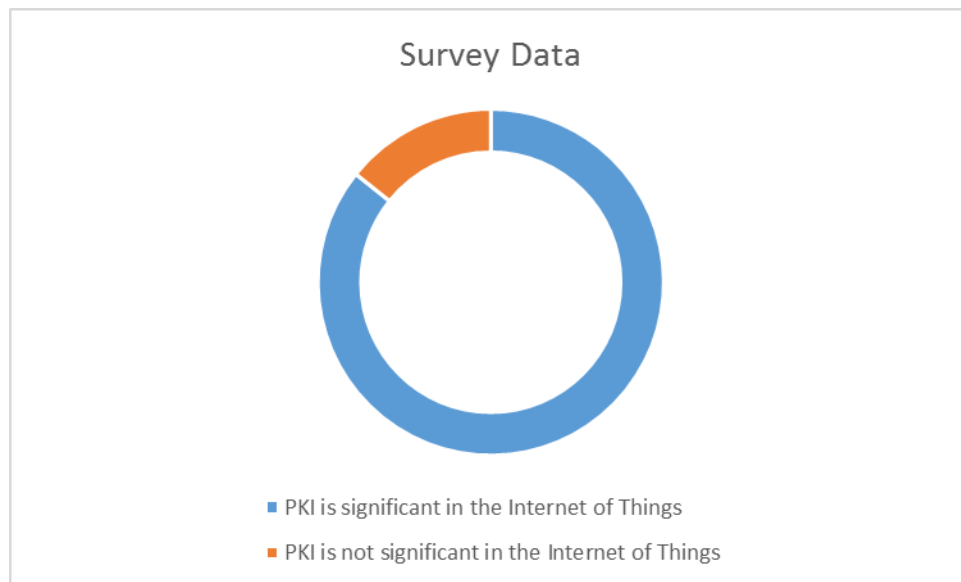


Figure 17. PKI is effective for the IoT

3. Analysis of Interview Responses

Question: Can PKI solve the security, privacy, and authentication risks of the IoT objectives?

The results obtained from the interviews indicate that many company officials had high trust in the effectiveness of PKI to offer protection to IoT devices. However, although PKI has been identified as one of the most effective and practical techniques that can provide reliable security and authentication for the IoT, not everyone interviewed was convinced that PKI alone could solve the security, privacy and, authentication risks of the IoT. The researcher discovered that 78% (78/100) of the interviewees think that PKI is a practical, useful, and effective way to provide protection and security from malware and other insecurity issues associated with the IoT. Figure 18 depicts the breakdown of personnel interviewed.

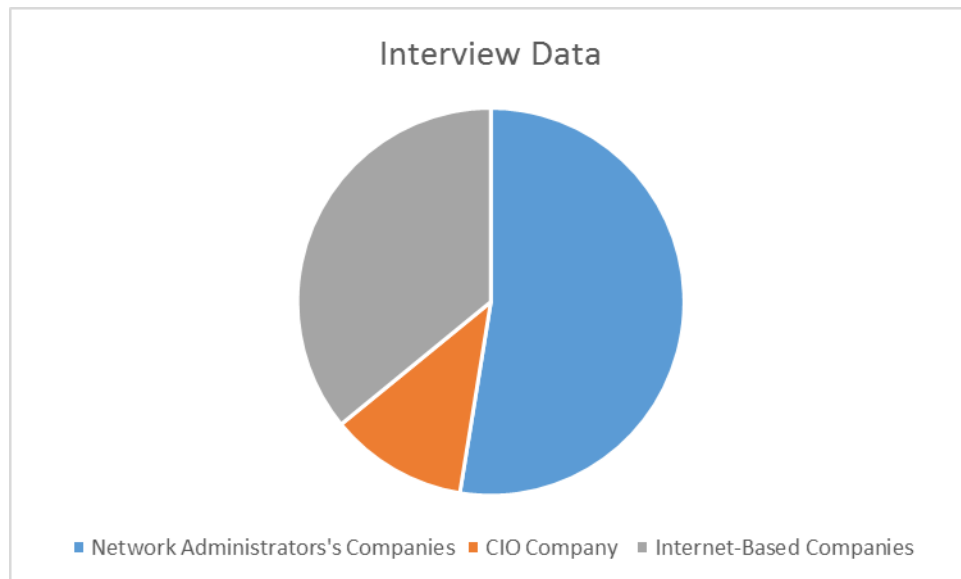


Figure 18. PKI is effective on the IoT

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

The growth and complexity of systems have brought a relative advancement in hackers' and system malware producers' knowledge, thus generating a strong desire for complex and more advanced security systems. As indicated by this study, it is delineated that PKI is the key to taking care of the security and protection issues of the IoT. The decision to use PKI on IoT needs a prior understanding of the disparate endpoints that are crucial in connecting an entire circle of industrial resolution or consumer products. According to Wayne Harris, a PKI consultant, in the pursuit of widespread adoption, organizations should plan PKI for devices that are low powered and use digital certificates to meet the requirements for the average IoT sensor or device (Housley, 2004).

According to researchers and scholars, PKI can be viably utilized to improve the authentication, non-repudiation, confidentiality, and integrity of devices. This is often accomplished by the melding of Symmetric and Asymmetric cryptographic techniques that are upheld by the application of a straightforward and effectively overseen foundation rather than complex different security frameworks. Compared with frameworks that are as it was based on symmetric cryptography, PKI is more progressed and offers scalable IoT protection services.

While it is acknowledged that the current growth and advancement in technology have brought tremendous changes in the traditional methods of providing security to IoT devices, likewise, the growth and complexity of the systems have also brought a relative advancement in the knowledge of professional hackers and script kiddies thus, generating a strong desire for complex and more advanced security systems. One renowned system of providing security for IoT devices is the PKI; however, effective implementation of PKI depends on the efforts of several parties; the operations of CAs, site administrators, browsers, and users should collaborate to offer maximum security options for a network. The implementation process is complex and can be quickly jeopardized by a single player's actions, which demonstrates that technology alone cannot develop trust and security within

a system. How the policies and strategies greatly influence the impact, it will have on the security and privacy of a system.

When conducting the research, the researcher found a podcast by Jeremy Rowley, Executive VP of Emerging Markets at DigiCert, who talked about automating PKI for IoT platform and building scalable solutions for the IoT platform. According to Rowley (2017), many IoT devices get employed on the Internet, for instance, connected watches, connected vehicles, and many other things. The issue is that most of these devices tend not to deploy security. Therefore, they are subject to attacks. For example, in 2015, there were attacks on various devices, such as medical devices and cars. Rea (2015) reminded us that in 2016, there were incidences when one could take over an insulin pump and change a person's dosage causing harm to the patient using the insulin pump.

Rowley (2017) stated that the question at hand for Internet professionals was how to ensure the security of IoT devices. Rowley claimed that they had found a way to provide the automation of DCs as well as other credentials in a way that was not expensive, and that can be scaled to the millions of devices that require security. He added that at DigiCert, they carry this out using standard protocols like EST or SCEP. They also had created their software, the DigiCert Auto-Provisioning Platform. This platform manages the complete life cycle of certificates without any human intervention.

Rowley (2017) pointed out that among the challenges faced was in carrying out all the activities that needed doing. Therefore, they built a robust system that could scale the amount required for billions (Rea, 2015). Organizations that are using the platform include automotive companies, healthcare companies, smart home initiatives, and industrial companies. These are organizations looking to ensure the security of their vital infrastructure against attacks. Many of the devices being secured are already deployed, and they usually end up possessing a secure environment for computing where one can put their credentials. According to Rowley, there are smart gadgets as well as devices available that may not possess their platform, but they are working hand in hand with the systems to improve methods to ensure the security of those devices. However, with new, smart devices, manufacturers and engineers are encouraged to develop security into the structures during design.

Among the challenges they faced when ensuring the security of IoT devices was that some people firmly believe that PKI is traditional. Rowley (2017) explained that one wishes to deploy on a low-powered device when one has a digital X509 certificate, which is usually large and bulky. He added that at DigiCert, they had been working hard to develop how they can accomplish the accommodation and that they had established certificate profiles, which would be as small as 80 bytes, and that can be applied to low powered devices. This enables them to present a scale of devices that possibly will not routinely be able to see safety cost-effectively. They endeavor to allow security on any device they can because their goal at DigiCert is to ensure the Internet is secure (Rea, 2015). They would like to ensure they provide certificates everywhere to ensure the protection of end-users and the aligned parties when carrying out transactions with their devices.

At DigiCert, one of the areas that they are pretty keen on is the transportation department as well as on vehicles. In vehicles, there are sensors which get deployed to monitor oil and tire pressure as well as the deployment of airbags. All of these are in communication with the central system. Thus, each of these sensors tends to provide information necessary for the functioning of a car. Attackers and malware are targeting these systems and altering the data coming to them to control the vehicle and give them directions.

At DigiCert, they are providing the sensors with certificates as well as panels of control to provide substantiation to the regulator panel from the instruments to ensure the sensor knows it is part of the car (Rea, 2015). They are aiming at encrypting the communication to prevent the information from being accessed by an attacker. They are providing related services to this, and thus when using their products, people can provide robust IoT platforms which will be able to stand the test of time by application of strong crypto so supply verification services, which allows one to know when an instrument is linking, the person connecting to the apparatus to encrypt the message occurring through the device, as well as to provide the communication with integrity. There is no chance anyone would want another person to manipulate their equipment and have it malfunctioning or carrying out things that they did not intend it to do.

Another automated security that DigiCert trusts in and believes that people should concentrate on is PKI (Rea, 2015). At DigiCert, they have been working on numerous tools that will be able to encrypt sites fully and provide authentication and identity services. Rowley (2017) adds that at DigiCert, they have been working together with manufacturers and developers to develop new ways to ensure IP protection. This will help prevent other manufacturers from being able to duplicate any same device and sell them. DigiCert has found that they can deploy credentials in ways that ensure the duplicate devices cannot be manufactured and used on any network.

Companies that provide these duplicate devices lobby since they can acquire additional revenue as the black market does not undermine them. The means of IP protection they have developed at DigiCert helps protect their IP from being taken and duplicates being made, as well as the provision of customers with safety, which ensures their structures are trustworthy and safe (Rea, 2015). Rowley (2017) firmly believes that automation is becoming a crucial part of all security facets. He is content to be there and believes that if companies want to develop their IoT devices safety, they first have to execute a susceptibility test and make sure they know the type of data going through their devices, where the data goes, how the data is encrypted, and which other devices are in communication with their own devices. Once companies can do this, they can come up with a way to economically secure their devices and systems and figure out the level of technology and encryption required to protect their users. They also need to involve security professionals such as DigiCert to assess the security requirements and to find out how to protect and encrypt devices.

This thesis tried to prove that PKI is a successful security measure and an effective mitigation strategy for implementing IoT systems. According to Weise (2001), the IoT has extraordinary promise; however, business, policy, and technical challenges must be handled before these frameworks are embraced more broadly.

Adopters will need to demonstrate that the modern sensor-driven commerce models create superior value, and is an excellent return on investment (ROI). IT group and government controllers ought to think about rules on data privacy and information security, especially for employments that touch on sensitive consumer data. Legal risk frameworks

for the appalling choices of robotized and automated frameworks will have to be built up by governments, companies, and risk analysts, in consort with insurers.

Additionally, on the innovation side, the cost of sensors and actuators must drop to levels that will energize the broader widespread use of IoT. IoT technologies and the benchmarks and standards that back them must advance to the point where information can stream openly among sensors, computers, and actuators. Computer software programs required to aggregate and analyze information and graphic display techniques must make strides to the point where gigantic volumes of information can be ingested by human decision-makers or synthesized to directly mechanized, automated systems more suitably (Weise, 2001).

Inside companies, considerable changes in information patterns will have implications for organizational structures, as well as how choices are made, operations are overseen, and processes are conceived. For example, product development will have to reflect more noteworthy conceivable outcomes for capturing and analyzing data. Companies can start taking steps presently to position themselves for these changes by utilizing modern innovations to optimize commerce processes in which conventional approaches have not brought palatable returns. Energy utilization effectiveness and process optimization are great early targets. Tests with the emerging technologies ought to be conducted in development labs and in small-scale pilot trials, and established companies can look for organizations with imaginative innovation providers making Internet-of-Things capabilities for target industries (Weise, 2001).

To summarize, this work briefly highlighted essential differences between an IoT, PKI, and an enterprise PKI, and took a look at the current state of the security of the IoT. Security, incorporation with existing technology, and indeterminate returns on investment have been identified as the three most significant obstacles to a higher rate of IoT adoption in the enterprise. Consequently, the related risk factors and the dissimilar management, deployment, and design considerations for PKI for the IoT applications will be discussed in this section. Moreover, this section seeks to establish the imperative necessity to guarantee secure communications in IoT systems, and affirm that PKI is the correct technological solution for encrypting and authenticating device communication.

B. RECOMMENDATIONS

Chui et al. (2010) predict that advances in wireless networking technology and the greater standardization of communications protocols is leading to the widespread adoption of IoT by organizations and individuals. However, they also caution that wide-scale deployment and implementation of these technologies is unlikely to occur before the 2025 timeframe, even though connected everyday objects and sensor networks deliver significant benefits and value to the economy and significant efficiency to business entities. Businesses can lower costs and boost corporate profits because IoT technologies streamline commercial logistics and industrial automation that reduce labor. Connected everyday objects and sensor networks are common in workplaces, public places, and households.

According to OECD (2016), this aggregated data can drive innovation, research, and marketing, as well as optimize the services generated. And, although IoT holds the promise to substantially contribute to further economic growth and social prosperity, the degree of adoption and ability to reap its benefits will largely depend on the capacity of governments to create adequate policy and regulatory frameworks in key areas including telecommunications, security, privacy and consumer policy (OECD, 2016). Securing an IoT infrastructure requires robust security methodologies. These strategies require one to secure their information within the cloud, ensure the secure provision of devices and guarantee data integrity when executing over the Internet. The security methodologies can be created and executed through the compelling interest of several players included within the development, manufacturing, deployment, and operation of IoT-enabled components and devices.

Nachappa, Aparna, and Somanna (2018) addressed the issue. They wondered what the function of operational and technical standards for the deployment and development of secure IoT devices is, how can one effectively measure and identify the characteristics of IoT devices security, how can one measure the efficiency of IoT security countermeasures and initiatives and, how can one ensure the best security practices are implemented. Also, Nachappa et al. (2018) address the issue of 'Cost vs. security trade-offs.' They examined questions such as: What is the process used by stakeholders to make decisions that are cost-beneficial with regards to the IoT devices? How can one accurately assess and quantify the

risks to security? What motivates device manufacturers and engineers to accept additional costs of product design to ensure that devices are safe and accept responsibility for the results of negative externalities caused by their security choices? How will usability and functionality incompatibilities get reconciled with security? How can one ensure that the solutions for IoT security provide opportunities for IoT innovation, economic, and social growth? (Nachappa et al., 2018).

To summarize, the first impactful message from this investigation is, there are ways to more extensive adoption of IoT. Be that as it may, the way incorporates a few crucial tasks that must be embraced by the different partners and stakeholders. An adequacy evaluation must be started to identify gaps and decide potential moderation methodologies for each issue set recognized in this thesis. To assess the viability of IoT, IoT partners ought to reexamine and distinguish enhancements and efficiencies that can be created and showcased to improve the security of IoT-enabled gadgets. Consumers, businesses, and specialized partners and other stakeholders must work in tandem and leverage their area of expertise to accomplish a future state of building and maintaining a successful IoT. The key to IoT success tend to fall along two principal axes:

1. Business Enablement

Business stakeholders possess the analytic requirements prerequisites of their items. Therefore, they should define processes for conducting analytic activities and after that collapsing those results back into operational decision-making processes. Businesses out to construct forms that make best utilize of the IoT portfolio (Holsapple et al., 2014).

2. Technical Enablement

Specialized partners like technical stakeholders possess the capacity to, secure supporting apparatuses, architect and sustain solutions, and construct analytic capability. Consequently, specialized partners need to build a campaign of learning that reintegrates the messages from investigate research investigations, analyses, and lessons learned to construct a validated, verified, and steady engineering solutions to serve the particular security-related needs of the worldwide IoT community (Holsapple et al., 2014).

3. Recommendations for IoT Stakeholders

Similar to how the Internet and versatile mobile communications was embraced broadly, so as well can the IoT. Be that as it may, if the public and business stakeholders believe the risks outweigh perceived benefits, at that point the IoT might lose its current momentum, and perhaps never reach its full potential. Therefore, the following subsections provides brief descriptions of IoT stakeholders, and also offers suggestions for how IoT security collaboration and shared responsibility can be encouraged and addressed. The recommendations in this section are based on the researchers 26 year work history in the core disciplines of IT security, and her knowledge gained through her credentials as a Certified Information Systems Security Professional (CISSP), Information Systems Security Manager (ISSM), and Information Technology Infrastructure Library (ITIL) v3 Expert level.

a. IoT Solution Developers

Engineers more often than not center in the development of solution for the IoT. These engineers may be a Systems Integrator or conceivably be members of an in-house side that specializes in the activity. The solution developer is bound to create components of the IoT solution from scratch as well as integrate a few open-source or off-the-shelf components. They may too adopt solutions that are pre-configured with minor adjustments. The first part is figuring out the action of Solution developers is figuring out whether the solution provider that is outsourced can be trusted. Then, it is vital to ensure that there's understanding of how the IoT-enabled components is developed, how device activation, reactivation, recalls, updates, support and maintenance documentation occurs.

Martín-Ruíz, Fernández-Aller, Portillo, Malagón, and Barrio (2018) addresses the question: Do IoT devices need to be designed for upgradeability and maintainability with their extended service life to adapt them to the changing threats to security? New parameter settings and software have the potential of being installed in fielded IoT devices by a centralized system of security management if all devices possessed integrated device management agents. Do there exist IoT devices that are low-risk thus do not require such kinds of features?

Nachappa et al. (2018) also addresses this concept, for example: What sets are best for practice for developers and engineers to use to design IoT devices to make them safer? How do lessons learned from the IoT security problems get understood and conveyed to communities of development to enhance future devices? What are educational and training resources provided to teach developers and engineers more secure designs of IoT? Proposals for IoT developers/designers incorporates the following:

- Use PKI because PKI is regarded as the best technology available to guarantee data safety, identities, and messages across open networks. Developers also need to comprehend that PKI does not only implement the technology, it also helps in establishing trust, which means it defines the procedure and processes for every entity in the PKI and communicates the acknowledgment and responsibilities of liabilities of every object in the system.
- When the IoT device attributes are vital to the local trust configuration, it is essential to make certain PKI procedures that can cater to changes in attributes. For instance, this may incorporate the development of Attribute Authority (AA) architectures of trust, and methods are not leaving out CA architectures of trust and procedures.
- The CAs ought to enable trust of AA service providers, while AAs ought to follow the same developed processes for trusting CAs, and policy for AAs to work under needs to be developed (this incorporates management policies and attribute release). An AA may publish a statement of practice that will demonstrate how they tend to meet policy requirements, including security controls and operational controls.
- The CAs may verify (by use of an audit) that the AA is working by the policies established and the published practices. The CA may provide identity certificates to the AA to be used to ensure attribute assertions are made. The App community trusts this signer of proclamation through being provided a midway that links to a community core (Hong, 2013).

- The AA tends to follow the policies published to manage and make assertions enrolled devices. When the attributes of devices change, the local AA issues attribute statements that are updated regarding the device. If the Attribute Authority misbehaves, the CA can revoke the assertion signer, now de-authorizing it from the system.
- Follow the appropriate technique of secure software development- developing secure software needs ground-up security thinking, from the beginning of the project to its implementation stage, testing stage, and deployment. The decisions of tools, platforms, languages are all affected by the technique chosen.
- Choose the source of software carefully- open-source software allows developing solutions quickly. When choosing which open-source software to choose, it is essential to consider the level of activity of the communities where each of the open-source components belongs. An active society makes sure that software is reinforced and that any present problems are exposed and appropriately addressed.
- Integrated carefully- many security flaws of software are present at the boundary of APIs and libraries. Functionality, which possibly will not be needed for the new distribution, may be available through an API layer. To ensure complete security, one needs to ensure they check all components' interfaces that are being integrated for flaws in security.
- Develop hardware safely- the deployment of IoT usually needs equipment to be deployed in locations that are insecure, for instance, in unsupervised locales or public areas. In such circumstances, it is essential to ensure that the deployment of hardware is near tamper-proof since many attackers tend to use these situations as entry or egress points.
- Ensure the safety of authentication keys during rollout; all the devices need device IDs and associated authentication keys generated by cloud services.

These keys need to be kept safe physically during and after deployment. If any key gets compromised, this can be used by malicious devices to mask themselves as actual devices.

- Follow the appropriate technique of secure software development- developing secure software needs ground-up security thinking, from the beginning of the project to its implementation stage, testing stage, and deployment. The decisions of tools, platforms, languages are all affected by the technique chosen.
- Choose the open-source software carefully- open source software gives an opportunity to develop solutions quickly. When one is deciding which open-source software to choose, it is essential to consider the level of activity of the communities where each of the open-source components belongs. A society that is active makes sure that software is reinforced and that any present problems are exposed and appropriately addressed.
- Integrated carefully- many security flaws of software are present at the boundary of APIs and libraries. Functionality, which possibly will not be needed for the recent distribution, may be available through an API layer. To ensure complete security, one needs to ensure they check all components' interfaces that are being integrated for flaws in security.

b. IoT Hardware Manufacturers

Because manufacturers could unintentionally be vectors for malicious code that infect and destroy IoT-enabled objects, the issue must be addressed. Nachappa et al. (2018) addresses the question: Are device manufacturers supposed to be penalized for the sale of hardware and software with unknown or known security flaws? How might consumer protection and product liability laws be extended or adapted to cover all negative IoT externalities, and can this function in a cross-border surrounding? Would regulation be able to keep up with the pace and be efficient enough in the evolving IoT technology and changing threats to security? Manufacturers of the IoT hardware that gets deployed, the

integrators that assemble hardware from different manufacturers, or the suppliers that provide the hardware for IoT deployment.

- Scope hardware to the least requirements- the design of equipment needs to include the least number of features required for the operation of hardware. One way is through incorporating Universal Serial Bus (USB) ports. These added features can assist in opening the device for attack vectors that are to be avoided.
- Comprehend the security mechanisms that are to be embedded and whether or not Trusted Platform Modules (TPM) are to be used. Finding out whether or not the device will be regarded as a protected environment and whether the capability to specify a trust model before the deployment of the device is a choice form as part of the crucial things to be considered
- Make hardware secure from tampering- there need to be built-in mechanisms that will detect any physical tampering, for instance, the opening of the cover of devices or remove parts of a device. These interfere indications that can form a fragment of the stream of data that gets uploaded to the cloud.
- Build secure hardware- it necessary to ensure the building of security features, for instance, secure encrypted storage. These features assist in making devices safer and help in protecting the overall IoT.
- Make upgrades safer- the manufacturer of devices with secure upgrade paths allows the device to be reliable during and after they receive their updates

c. IoT Solutions Marketers/Deployers

Once an IoT resolution has been established, it necessitates undergoing deployment in the field; hardware, and deployment of solutions for hardware devices. Consequently, it is imperative to address the issue of tech obsolesce because sensors and communications devices must be standardized, maintained, and replaced/upgraded repeatedly. So, which is the correct path to follow with IoT devices that are obsolete as security challenges alter and

the Internet evolve; Do IoT devices require built-in “end of life” features of expiration that disable them? Requirements like these tend to force old devices that are not interoperable out of service and replace them with ones that are more interoperable and secure. They argued that these and other considerations would undoubtedly cause challenges in the open marketplace (Fu & Wenyan, 2018).

d. *IoT Solution Operators*

After the implementation of the IoT solution, long-term monitoring, maintenance, upgrades, and are required, these operations are performed by skilled teams comprising of IT specialists, maintenance teams, domain specialists, and hardware operators who consistently monitor the environment to detect threats.

- Ensure the operating system of devices and their drivers are upgraded to their latest versions is a significant undertaking. This helps in providing security for IoT devices and keeping them protected from malicious attacks.
- Installing the latest anti-malware and antivirus capabilities to their system if it permits them; up-to-date anti-malware and antivirus definitions makes a huge difference and help mitigate external threats.
- Ensure protection of cloud credentials. The credentials for cloud authentication used for operating and configuring IoT distribution are probably the easiest ways to acquire entree and concession an IoT system. It is crucial to protect these credentials through changing passwords often and avoiding the use of these credentials on machines that are public-facing.
- Conduct frequent system audits because frequent auditing can be the first line of defense against detecting security breaches. Most systems come with built-in event logging and are generally user friendly.
- Security attacks against IoT infrastructure that are launched when bad actors gain physical access are typically the most severe. So, ensure the physical safety of the IoT-enabled devices and infrastructure- are usually the worst

attacks on security. One of the critical safety practices against malicious attacks is through ensuring the security of USB ports as well as other physical points of access.

C. CONCLUSION

This paper sought to investigate the extent to which PKI can be useful in providing security to IoT devices by conducting in-depth research and by the use of primary data. In general, the findings of this study about the effectiveness of PKI agree with many prior studies. Adams and Lloyd (2003) argued that PKI's judicious deployment gives certain fundamental advantages to an organization, including some potential for significant savings in costs. Indeed, as argued by Loshin, Cobb, Brayton, Finneman, Turajski, & Wiltsey, S. (2018), without PKI, sensitive information can still be encrypted, confidentiality, and exchanged between two entities, but there would be no assurance of the identity of the other party. Any form of sensitive data exchanged over the Internet is reliant on the PKI for enabling the use of public key cryptography the PKI enables the authenticated exchange of public keys.

Rouse's contention affirms that PKI is currently the best strategy for ensuring the safety of the IoT for several reasons; it is useful, reliable, affordable, and effective. Indeed, increased public demand coupled with even more significant technological advances could drive even more widespread adoption of IoT that could, like the present IoT, continue to contribute immeasurably to the public, and domestic and global economies. Conversely, today's developments point to future opportunities and risks that will arise when people can incorporate artificial intelligence (AI) into everyday life. Moreover, to the extent that everyday objects become even higher information security risks, the IoT of the future could distribute those risks with much more severe consequences for the U.S. military. Therefore, the researcher proposes that future researchers conduct in-depth analyses of the implications of IoT on the U.S. military.

APPENDIX. SURVEY AND INTERVIEW QUESTIONS

- What is the IoT?
- In what ways is the IoT viewed as relevant in today's world?
- What are the known risks associated with IoT?
- What are some of the known issues which affect the implementation and development of IoT, and in what way are these risks to be solved?
- What is PKI?
- How does PKI work?
- What are the amenities obtainable by PKI?
- How does public key encryption work, and how does public key encryption and digital certificate provide security and authentication services?
- What are some of the known security risks that necessitate the use of PKI in the IoT systems?
- What is the significance of PKI in the IoT?
- What are the technical enhancements that PKI adds to IoT systems?
- How is PKI seen as a solution to the security, privacy, and authentication risks of the IoT?

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- Adams, C., Lloyd, S., & Adams, C. (2003). *Understanding PKI : Concepts, standards, and deployment considerations*. Addison-Wesley.
- Adams, C., & Lloyd, S. (2007). *Understanding PKI: Concepts, standards, and deployment considerations*. Addison-Wesley.
- Adams, C., Burmester, M., Desmedt, Y., Reiter, M., & Zimmermann, P. (2000). Which PKI (Public Key Infrastructure) is the right one? *Proceedings of the 7th ACM Conference on Computer and Communications Security*, 98–101.
<https://doi.org/10.1145/352600.352615>
- Afshar, R. (2015). *Digital certificates: Public Key Infrastructure*. Indiana State University. <http://cs.indstate.edu/~rafshar/documents/paper2.pdf>
- Akhila, V., Vasavi, Y., Nissie, K., & Rao, P. V. (2017). An IoT based patient health monitoring system using Arduino Uno. *International Journal of Research in Information Technology (IJRIT)*, (1)1, 1–9. www.ijrit.net
- Alrawais, A., Alhothaily, A., Cheng, X., Hu, C., & Yu, J. (2018). SecureGuard: A certificate validation system in Public Key Infrastructure. *IEEE Transactions on Vehicular Technology*, 67(6), 5399–5408.
<https://doi.org/10.1109/TVT.2018.2805700>
- Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), 2787–2805. <https://doi.org/10.1016/j.comnet.2010.05.010>
- Barcena, M., & Wueest, C. (2015). *Insecurity in the Internet of Things*.
https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/insecurity-in-the-internet-of-things.pdf
- Berners-Lee, T., Cailliau, R., Luotonen, A., Nielsen, H., & Secret, A. (1994). The World-Wide Web. *Communications of the ACM*, 37(8), 76–82.
<https://doi.org/10.1145/179606.179671>
- Boualouache, A., Nouali, O., Moussaoui, S., & Derder, A. (2015, November). A BLE-based data collection system for IoT. *2015 First International Conference on New Technologies of Information and Communication (NTIC)*, Mila, 2015, 1–5.
<https://doi.org/10.1109/NTIC.2015.7368748>
- Boldyreva, A., Fischlin, M., Palacio, A., & Warinschi, B. (2007). A closer look at PKI: Security and efficiency. In Okamoto T., Wang X. (eds) *Public Key Cryptography – PKC 2007: PKC 2007. Lecture Notes in Computer Science*, 4450, 458–475. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-71677-8_30

- Carfagno, J., (April 24, 2019). First AI medical monitoring wearable approved by FDA for home use. Docwirenews. <https://www.docwirenews.com/docwire-pick/future-of-medicine-picks/first-ai-wearable-approved-by-fda-for-home-use-monitoring-vitals/>
- Casola, V., Mazzeo, A., Mazzocca, N., & Vittorini, V. (2007). A policy-based methodology for security evaluation: A security metric for Public Key Infrastructures. *Journal of Computer Security*, 15(2), 197–229. <https://doi.org/10.3233/JCS-2007-15201>
- Chapman, L., & Bell, S. (2018). High-resolution monitoring of weather impacts on infrastructure networks using the Internet of Things. *Bulletin of the American Meteorological Society*, 99(6), 1147–1154. <https://doi.org/10.1175/BAMS-D-17-0214.1>
- Chase, J. (2013). *The evolution of the Internet of Things* (white paper). Texas Instruments. <http://www.tij.co.jp/jp/lit/ml/swrb028/swrb028.pdf>
- Chen, L., Thombre, S., Jarvinen, K., Lohan, E., Alen-Savikko, A., Leppakoski, H. ... Kuusniemi, H. (2017). Robustness, security and privacy in location-based services for future IoT: A survey. *IEEE Access*, 5, 8956–8977. <https://doi.org/10.1109/ACCESS.2017.2695525>
- Chen, S., Hui Xu, Dake Liu, Bo Hu, & Hucheng Wang. (2014). A vision of IoT: Applications, challenges, and opportunities with China perspective. *IEEE Internet of Things Journal*, 1(4), 349–359. <https://doi.org/10.1109/JIOT.2014.2337336>
- Chodos, M., Reiniger, T., & Bruch, R. (2019). The emergence of the online notary: Implications for the probate bar. *Probate & Property*, 33(4).
- Chokhani, S., Ford, W., Sabett, R., Merrill, C., & Wu, S. (2003). Internet X. 509 Public Key Infrastructure certificate policy and certification practices framework. <https://www.hjp.at/doc/rfc/rfc3647.html>
- Chui, M., Loffler, M., & Roberts, R. (2010). The Internet of Things. *The McKinsey Quarterly*, (2), 70–79.
- Coetzee, L., & Eksteen, J. (2011). The Internet of Things - promise for the future? An introduction. *2011 IST-Africa Conference Proceedings*, Gaborone, Botswana 2011, 1-9.
- Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., & Polk, W. (2008). *Internet X.509 Public Key Infrastructure certificate and certificate revocation list (CRL) profile*. HJP. <https://www.hjp.at/doc/rfc/rfc5280.html>

- Corbò, G., Foglietta, C., Palazzo, C., & Panzieri, S. (2018). Smart behavioral filter for industrial Internet of Things. *Mobile Networks and Applications*, 23(4), 809–816. <https://doi.org/10.1007/s11036-017-0882-1>
- Creswell, J., & Plano Clark, V. (2017). *Designing and conducting mixed methods research*. Los Angeles, CA: Sage Publications.
- Deif, D., & Gadallah, Y. (2017). A comprehensive wireless sensor network reliability metric for critical Internet of Things applications. *EURASIP Journal on Wireless Communications and Networking*, (1), 1–18. <https://doi.org/10.1186/s13638-017-0930-3>
- Dener, C., Watkins, J., & Dorotinsky, W. (2011). *Financial management information systems 25 years of World Bank experience on what works and what doesn't*. World Bank. <https://doi.org/10.1596/978-0-8213-8750-4>
- Deng, Z. (2010). Curriculum planning and systems change. *International Encyclopedia of Education*, 384–389. <https://doi.org/10.1016/B978-0-08-044894-7.00062-2>
- Desai, P., Sheth, A., & Anantharam, P. (2014). *Semantic gateway as a service architecture for IoT Interoperability*.arXiv.org. <http://search.proquest.com/docview/2084562805/>
- Dijkman, R., Sprenkels, B., Peeters, T., & Janssen, A. (2015). Business models for the Internet of Things. *International Journal of Information Management*, 35(6), 672–678. <https://doi.org/10.1016/j.ijinfomgt.2015.07.008>
- Dinha F. (2018). How to secure the Internet of Things. *Forbes*. <https://www.forbes.com/sites/forbestechcouncil/2018/04/13/how-to-secure-the-internet-of-things/#4f00e3651cbb>
- Ellison, C., & Schneier, B. (2000). Ten risks of PKI: What you're not being told about Public Key Infrastructure. *Computer Security Journal*, 16(1), 1–7. <https://doi.org/10.1201/9780203498156.ch23>
- Entrust provide free PKI and multi-platform toolkits for download. (1999). *Network Security*, 1999(7), 4–5. [https://doi.org/10.1016/S1353-4858\(99\)90006-5](https://doi.org/10.1016/S1353-4858(99)90006-5)
- Evans, D. (2011) *The Internet of Things how the next evolution of the Internet is changing everything*. Cisco Internet Business Solutions Group. https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FIN_AL.pdf
- Feki, M., Kawsar, F., Boussard, M., & Trappeniers, L. (2013). The Internet of Things: The next technological revolution. *Computer*, 46(2), 24–25. <https://doi.org/10.1109/MC.2013.63>

- Fettweis, G. (2016). 5G and the future of IoT, *ESSCIRC Conference 2016: 42nd European Solid-State Circuits Conference*, Lausanne, 2016, 21–24.
<https://doi.org/10.1109/ESSCIRC.2016.7598234>
- Firdous, S., Baig, Z., Valli, C., & Ibrahim, A. (2017). Modelling and evaluation of malicious attacks against the IoT MQTT Protocol. *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Exeter, 2017, 748–755.
<https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.115>
- Foote K., (2016). *A brief history of the Internet of Things. Data education for business and IT professionals.* <http://www.dataversity.net/brief-history-internet-things/>
- Fu, K., & Xu, W. (2018). Risks of trusting the physics of sensors: Protecting the Internet of Things with embedded security. *Communications of the ACM*, 61(2), 20–23.
<https://doi.org/10.1145/3176402>
- Gershenfeld, N., Krikorian, R., & Cohen, D. (2004). The Internet of Things. *Scientific American*, 291(4), 76–81. <https://doi.org/10.1038/scientificamerican1004-76>
- Govinda, K., & Saravanaguru, R.A. (2016). Review on IoT technologies. *International Journal of Applied Engineering Research*, 11(4), 2848–2853.
- Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. *Proceedings of the 13th ACM Conference on Computer and Communications Security*, 89–98.
<https://doi.org/10.1145/1180405.1180418>
- Greengard, S. (2015). *The Internet of Things*. MIT Press.
- Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2012). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645–1660. <https://doi.org/10.1016/j.future.2013.01.010>
- Guida, R., Stahl, R., Bunt, T., Secrest, G., & Moorcones, J. (2004). Deploying and using public key technology: Lessons learned in real life. *IEEE Security & Privacy*, 2(4), 67–71. <https://doi.org/10.1109/MSP.2004.41>
- Gupta, M., Patchava, V., & Menezes, V. (2015). Healthcare based on IoT using Raspberry Pi. *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, Noida, 2015, 796–799.
<https://doi.org/10.1109/ICGCIoT.2015.7380571>

- Gusmeroli, S., Piccione, S., & Rotondi, D. (2012). IoT access control issues: A capability based approach. *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, Palermo, 2012, 787–792. <https://doi.org/10.1109/IMIS.2012.38>
- Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S. L., Kumar, S. S., & Wehrle, K. (2011). *Security Challenges in the IP-based Internet of Things*. *Wireless Personal Communications*, 61(3), 527–542. <http://doi.org/10.1007/s11277-011-0385-5>
- Höller, J., Boyle, D., Karnouskos, S., Avesand, S., Mulligan, C., & Tsiatsis, V. (2014). *From machine-to-machine to the Internet of Things: Introduction to a new age of intelligence*. Elsevier. <https://doi.org/10.1016/C2012-0-03263-2>
- Hong, N. (2013). A security framework for the Internet of Things Based on Public Key Infrastructure. *Advanced Materials Research*, 671–674, 3223–3226. <https://doi.org/10.4028/www.scientific.net/amr.671-674.3223>
- Horrigan, J. (2009). Home broadband adoption 2009: Broadband adoption increases, but monthly prices do too. <https://www.pewinternet.org/wp-content/uploads/sites/9/media/Files/Reports/2009/Home-Broadband-Adoption-2009.pdf>
- Housley, R. (2004). *Public Key Infrastructure (PKI)*. The Internet encyclopedia. <https://doi.org/10.1002/047148296x.tie149>
- Housley, R. (2011). Security standards activities. *Encyclopedia of Cryptography and Security*. Springer. https://doi.org/10.1007/0-387-23483-7_379
- Holsapple, C., Lee-Post, A., & Pakath, R. (2014). A unified foundation for business analytics. *Decision Support Systems*, 64, 130–141. <https://doi.org/10.1016/j.dss.2014.05.013>
- Housley, R., & Polk, T. (2001). *Planning for PKI: Best practices guide for deploying Public Key Infrastructure*. John Wiley & Sons, Inc.
- Huh, S., Cho, S., & Kim, S. (2017). Managing IoT devices using blockchain platform. *2017 International Conference on Advanced Communication Technology (ICACT)* Bongpyeong, 2017, 464–467. <https://doi.org/10.23919/ICACT.2017.7890132>
- Istepanian, R., Hu, S., Philip, N., & Sungoor, A. (2011). The potential of Internet of m-health Things “m-IoT” for non-invasive glucose level sensing. *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, Boston, MA, 2011, 5264–5266. <https://doi.org/10.1109/IEMBS.2011.6091302>

- Jeevitha, B. K. (2017). Data storage security and privacy in cloud computing: A comprehensive survey. *International Journal of Computer Applications*, 156(12), 16–27.
- Jing, Q., Vasilakos, A., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: Perspectives and challenges. *Wireless Networks*, 20(8), 2481–2501. <https://doi.org/10.1007/s11276-014-0761-7>
- Johnson, R., Onwuegbuzie, A., & Turner, L. (2007). Toward a definition of mixed methods research. *Journal of Mixed Methods Research*, 1(2), 112–133. <https://doi.org/10.1177/1558689806298224>
- Jorgensen, P. (1996). Applied cryptography: Protocols, algorithm, and source code in C: By Bruce Schneier. *Government Information Quarterly*, 13(3), 336–336. [https://doi.org/10.1016/S0740-624X\(96\)90083-0](https://doi.org/10.1016/S0740-624X(96)90083-0)
- Kamaludin, H., Mahdin, H., & Abawajy, J. (2018). Clone tag detection in distributed RFID systems. *PLoS ONE*, 13(3), e0193951. <https://doi.org/10.1371/journal.pone.0193951>
- Khan, R., Khan, S., Zaheer, R., & Khan, S. (2012). Future Internet: The Internet of Things architecture, possible applications and key challenges. *2012 10th International Conference on Frontiers of Information Technology*, Islamabad, 2012, 257–260. <https://doi.org/10.1109/FIT.2012.53>
- Kolbe, N., Kubler, S., Robert, J., Le Traon, Y., & Zaslavsky, A. (2017). Towards semantic interoperability in an open IoT ecosystem for connected vehicle services. *2017 Global Internet of Things Summit (GIoTS)*, 1–5. <https://doi.org/10.1109/GIOTS.2017.8016229>
- Kumari, S., Karuppiah, M., Das, A. K., Li, X., Wu, F., & Kumar, N. (2017). A secure authentication scheme based on Elliptic Curve Cryptography for IoT and cloud servers. *The Journal of Supercomputing*, 74, 6428–6453. <https://doi.org/10.1007/s11227-017-2048-0>
- Latvakoski, J., Iivari, A., Vitic, P., Jubeh, B., Alaya, M. B., Monteil, T., Lopez, Y., Talavera, G., Gonzalez, J., Granqvist, N., Kellil, M., Ganem, H., & Väisänen, T. (2014). A Survey on M2M service networks. *Computers*, 3(4), 130–173. <https://doi.org/10.3390/computers3040130>
- Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, 58(4), 431–440. <https://doi.org/10.1016/j.bushor.2015.03.008>

- Lesjak, C., Hein, D., & Winter, J. (2015). Hardware-security technologies for industrial IoT: TrustZone and security controller, *IECON-2015 41st Annual Conference of the IEEE Industrial Electronics Society*, Yokohama, 2015, 2589–2595. <https://doi.org/10.1109/IECON.2015.7392493>
- Locasto, M., Parekh, J., Keromytis, A., & Stolfo, S. (2005). Towards collaborative security and P2P intrusion detection. *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop*, 2005, 333–339. <https://doi.org/10.1109/IAW.2005.1495971>
- Lopez Research LLC. (2013). *An introduction to the Internet of Things (IoT). Part 1 of the IoT series*. Cisco. https://www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november.pdf
- Liping, H., & Lei, S. (2011). Research on trust model of PKI. *2011 Fourth International Conference on Intelligent Computation Technology and Automation*, Shenzhen, Guangdong, 232–235. <https://doi.org/10.1109/ICICTA.2011.67>
- Lu, C. (2014). *Overview of security and privacy issues in the Internet of Things*. Washington University. <https://www.cse.wustl.edu/~jain/cse574-14/ftp/security/index.html>
- Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). Internet of Things (IoT) security: Current status, challenges and prospective measures. *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, London, 2015, 336–341. <https://doi.org/10.1109/ICITST.2015.7412116>
- Mandula, K., Parupalli, R., Murty, C., Magesh, E., & Lunagariya, R. (2015). Mobile based home automation using Internet of Things (IoT). *2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, Kumaracoil, 2015, 340–343. <https://doi.org/10.1109/ICCICCT.2015.7475301>
- Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2015). *Unlocking the Potential of the Internet of Things*. McKinsey Global Institute. <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world>
- Marburger, J. (2011). Science, technology and innovation in a 21st Century context. (Editorial). *Policy Sciences*, 44(3), 209–213. <https://doi.org/10.1007/s11077-011-9137-3>
- Martín-Ruíz, M., Fernández-Aller, C., Portillo, E., Malagón, J., & Barrio, C. (2018). Developing a system for processing health data of children using digitalized toys: Ethical and privacy concerns for the Internet of Things paradigm. *Science and Engineering Ethics*, 24(4), 1057–76. <https://doi.org/10.1007/s11948-017-9951-x>

- Mathaba, S., Adigun, M., Oladosu, J., Oki, O., Thampi, S., & El-Alfy, E. (2017). On the use of the Internet of Things and Web 2.0 in inventory management. *Journal of Intelligent & Fuzzy Systems*, 32(4), 3091–3101. <https://doi.org/10.3233/JIFS-169252>
- Messerges, T., Dabbish, E., Puhl, L., & Kuhlman, D. (2002). *A system and method for secure and convenient management of digital electronic content* (U.S. Patent Application No. 10/028,164). Google Patents. <https://patents.google.com/patent/WO2002086725A1/en>
- Meyer, B. (2015). Case studies. *Researching Translation and Interpreting* 195–202. Routledge.
- McPherson, S. (2009). *Tim-Berners-Lee: Inventor of the World Wide Web*. Minneapolis, MN: Twenty-First Century Books
- Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of Things: Vision, applications and research challenges. *Ad hoc networks*, 10(7), 1497–1516. <https://doi.org/10.1016/j.adhoc.2012.02.016>
- Misra, S., Goswami, S., Taneja, C., & Mukherjee, A. (2016). Design and implementation analysis of a public key infrastructure-enabled security framework for ZigBee sensor networks. *International Journal of Communication Systems*, 29(13), 1992–2014. <https://doi.org/10.1002/dac.2893>
- Nachappa, M., Aparna, M., & Varun Somanna, M. (2018). Internet of Things (IoT): An overview of security concerns. *International Journal of Engineering and Techniques*, 4(1), 280–286. www.ijetjournal.org
- Najjar-Ghabel, S., Yousefi, S., & Farzinvas, L. (2018). Reliable data gathering in the Internet of Things using artificial bee colony. *Turkish Journal of Electrical Engineering & Computer Sciences*, 26(4), 1710–1723. <https://doi.org/10.3906/elk-1801-100>
- Nash, A., Duane, W., & Joseph, C. (2001). *PKI: Implementing and Managing E-security*. New York, NY: McGraw-Hill, Inc.
- Ning, H., & Wang, Z. (2011). Future Internet of Things architecture: Like mankind neural system or social organization framework? *IEEE Communications Letters*, 15(4), 461–463. <https://doi.org/10.1109/LCOMM.2011.022411.110120>
- Nymi. (n.d.). Retrieved May 31, 2020, from <https://nyimi.com>
- OEGB. (2016). Internet of Things: *Seizing the benefits and addressing the challenges*. <https://dx.doi.org/10.1787/5jlwvzz8td0n-en>

- Olssen, M., Codd, J., & O'Neill, A. (2004). *Education policy globalization, citizenship and democracy*. SAGE.
- Pal, S. (2008). 21st Century information technology revolution. *Ubiquity*, (June), 3. <https://doi.org/10.1145/1403922.1399619>
- Porambage, P., Schmitt, C., Kumar, P., Gurtov, A., & Ylianttila, M. (2014). Two-phase authentication protocol for wireless sensor networks in distributed IoT applications. *2014 IEEE Wireless Communications and Networking Conference (WCNC)*, Istanbul, 2014, 2728–2733. <https://doi.org/10.1109/WCNC.2014.6952860>
- Prakashan, K., Karthika, A., Anayarkanni, R., & Jose, J. (2017). Transformation of health care system using Internet of Things in villages. *2017 IEEE International Conference on Industrial Engineering and Engineering Management*, Singapore, 2017, 914–918. <https://doi.org/10.1109/IEEM.2017.8290025>
- Rao, N. M., Sasidhar, C., & Kumar, V. S. (2012). Cloud computing through mobile-learning. <https://arxiv.org/abs/1204.1594>
- Ratasuk, R., Vejlgard, B., Mangalvedhe, N., & Ghosh, A. NB-IoT system for M2M communication. *2016 IEEE Wireless Communications and Networking Conference*, Doha, 2016, 1-5. <https://doi.org/10.1109/WCNC.2016.7564708>
- Rea, S. (2015, February 4). *IoT: Taking PKI where no PKI has gone before*. [Video] <https://www.slideshare.net/DigiCertCom/app-sec2015>
- Reddy, G. Rama Mohan, & Reddy, E. M. (2018). At initial stage forest fire detection through Internet of Things. *International Journal of Recent Research Aspects*, 5(1), 252–254.
- Reddy, G. Rama Mohan, & Reddy, E. M. (2018). Fast identification of earth quake detected through Internet of Things. *International Journal of Recent Research Aspects*, 5(1), 255–257. <https://www.ijrra.net/Vol5issue1/IJRRRA-05-01-56.pdf>
- Reid, R., & Dhillon, G. (2003). Integrating digital signatures with relational Databases: Issues and organizational implications. *Journal of Database Management*, 14(2), 42–51. <https://doi.org/10.4018/jdm.2003040104>
- Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. *Computer Networks*, 57(10), 2266–2279. <https://doi.org/10.1016/j.comnet.2012.12.018>
- Rouse, M. (2018). PKI (Public Key Infrastructure). Searchsecurity. <https://searchsecurity.techtarget.com/definition/PKI>

- Rowley, J. (2017, March 6). *Automating PKI for the IoT platform*. Helpnetsecurity.
<https://www.helpnetsecurity.com/2017/03/06/automate-pki-iot/>
- Ruggeri, G., & Briante, O. (2017). A framework for IoT and e-health systems integration based on the social Internet of Things paradigm. *2017 International Symposium on Wireless Communication Systems*, 426–431.
<https://doi.org/10.1109/ISWCS.2017.8108152>
- Santofimia, M., Villa, D., Aceña, O., Del Toro, X., Trapero, C., Villanueva, F., & Lopez, J. (2018). Enabling smart behavior through automatic service composition for Internet of Things–based smart homes. *International Journal of Distributed Sensor Networks*, 14(8), 1–20. <https://doi.org/10.1177/1550147718794616>
- Schatz, B., & Hardin, J. (1994). NCSA Mosaic and the World Wide Web: Global hypermedia protocols for the Internet. (National Center for Supercomputing Applications) (Computing in Science) (Cover Story). *Science*, 265(5174), 895–901. <https://doi.org/10.1126/science.265.5174.895>
- Scheirer, W., Bishop, B., & Boulton, T. (2010). Beyond PKI: The biocryptographic key infrastructure. *2010 IEEE International Workshop on Information Forensics and Security*, 1–6. <https://doi.org/10.1109/WIFS.2010.5711435>
- Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76(15), 146–164. <https://doi.org/10.1016/j.comnet.2014.11.008>
- Sicato, J., Sharma, P., Loia, V., & Park, J. (2019). VPNFilter malware analysis on cyber threat in smart home network. *Applied Sciences*, 9(13), 2763. <https://doi.org/10.3390/app9132763>
- Singh, H. (2018). *The Internet of Things: IoT solutions and its benefits*.
<https://customerthink.com/the-internet-of-things-iot-solutions-and-its-benefits/>
- Stajano, F. (2002). *Security for ubiquitous computing*. John Wiley & Sons.
<https://doi.org/10.1002/0470848693>
- Stankovic, J. A. (2014). Research directions for the Internet of Things. *IEEE Internet of Things Journal*, 1(1), 3–9. <https://doi.org/10.1109/jiot.2014.2312291>
- Sundmaeker, H., Guillemin, P., & Friess, P. (2010). *Vision and challenges for realizing the Internet of Things*. European Union. <https://doi.org/10.2759/26127>
- Suo, H., Wan, J., Zou, C. and Liu, J. (2012) Security in the Internet of Things: A review. *2012 International Conference on Computer Science and Electronics Engineering*, Hangzhou, 2012, 648–651.
<https://doi.org/10.1109/ICCSEE.2012.373>

- Tahir, H., Tahir, R., & McDonald-Maier, K. (2018). On the security of consumer wearable devices in the Internet of Things. *PLoS ONE*, 13(4), 1–21. <https://doi.org/10.1371/journal.pone.0195487>
- Tashakkori, A., & Teddlie, C. (2010). *SAGE handbook of mixed methods in social & behavioral research*. Thousand Oaks, CA: SAGE Publications, Inc. <https://doi.org/10.4135/9781506335193>
- Thompson, M., Essiari, A., & Mudumbai, S. (2003). Certificate-based authorization policy in a PKI environment. *ACM Transactions on Information and System Security*, 6(4), 566–588. <https://doi.org/10.1145/950191.950196>
- Tianbo, Z. (2012). The Internet of Things promoting higher education revolution, 2012 *Fourth International Conference on Multimedia Information Networking and Security*, Nanjing, 2012, 790-793. <https://doi.org/10.1109/MINES.2012.231>
- TipTopSecurity, (2017, September 10). *How does HTTPS work? RSA explained*. <https://tiptopsecurity.com/how-does-https-work-rsa-encryption-explained/>
- Uchihira, N., Ishimatsu, H., & Inoue, K. (2016). IoT service business ecosystem design in a global, competitive, and collaborative environment. 2016 *Portland International Conference on Management of Engineering and Technology (PICMET)*, Honolulu, HI, 1195-1201. <https://doi.org/10.1109/PICMET.2016.7806694>
- Ukil, A., Sen, J., & Koilakonda, S. (2011). Embedded security for Internet of Things. 2011 *2nd National Conference on Emerging Trends and Applications in Computer Science*, Shillong, 1-6. <https://doi.org/10.1109/NCETACS.2011.5751382>
- VitalConnect. (n.d.). VitalPatch. Retrieved May 31, 2020, from <https://vitalconnect.com/solutions/vitalpatch/>
- Weber, R. H. (2011). Accountability in the Internet of Things. *Computer Law & Security Review*, 27(2), 133–138. <https://doi.org/10.1016/j.clsr.2011.01.005>
- Weise, J. (2001). *Public Key Infrastructure overview*, Sun PSSM Global Security Practice, Sun Blue Prints. <https://linuxsecurity.com/news/cryptography/public-key-infrastructure-overview>
- Wong, B., Locasto, M., & Keromytis, A., & Columbia University. Computer Science (2005). *PalProtect: A collaborative security approach to comment spam*. <https://doi.org/10.7916/D8HT2X71>
- Yang, X., Wang, L., Xie, J., & Zhang, Z. (2018). Cross-layer model design in wireless ad hoc networks for the Internet of Things. (Research Article). *PLoS ONE*, 13(5), 1–11. <https://doi.org/10.1371/journal.pone.0196818>

- Yao, X., Han, X., Du, X., & Zhou, X. (2013). A Lightweight multicast authentication mechanism for small scale IoT applications. *IEEE Sensors Journal*, 13(10), 3693–3701. <https://doi.org/10.1109/JSEN.2013.2266116>
- Yeh, W.-C., & Lin, J.-S. (2018). New parallel swarm algorithm for smart sensor systems redundancy allocation problems in the Internet of Things. *Journal of Supercomputing*, 74(9), 4358–4384. <https://doi.org/10.1007/s11227-016-1903-8>
- Zhang, Y., & Yu, J. (2013). A Study on the fire IoT development strategy. *Procedia Engineering*, 52(C), 314–319. <https://doi.org/10.1016/j.proeng.2013.02.146>
- Zhang, Z. K., Cho, M. C. Y., Wang, C. W., Hsu, C. W., Chen, C. K., & Shieh, S. (2014). IoT Security: Ongoing challenges and research opportunities. 2014 *IEEE 7th International Conference on Service-Oriented Computing and Applications*, Matsue, 2014, 230–234. <https://doi.org/10.1109/SOCA.2014.58>
- Zhao, W. Keynote: WInternet: From net of things to Internet of Things. 2014 *IEEE International Conference on Pervasive Computing and Communications (PerCom)*, Budapest, 1-1. <https://doi.org/10.1109/PerCom.2014.6813936>
- Zou, Z., Guo, C., Zeng, Z., & Shi, S. (2011). A dynamic adjusting carrier coverage-based load balancing scheme in LTE-advanced system based on carrier aggregation. 2011 *7th International Conference on Wireless Communications, Networking and Mobile Computing*, Wuhan, 2011, 1–4. <https://doi.org/10.1109/wicom.2011.6036661>

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California