Security Enhancements to System on Chip Devices for IoT Perception Layer

Sudeendra kumar K, Sauvagya Sahoo, Abhishek Mahapatra, Ayas Kanta Swain, K.K.Mahapatra
kumar.sudeendra@gmail.com, sauvagya.nitrkl@gmail.com, kmaha2@gmail.com
National Institute of Technology, Rourkela

Abstract- **Internet of Things (IoT) will drive the growth for semiconductor industry in next decade. In the era of IoT, millions of smart computing things are connected to solve customized applications. The tenets of IoT design are agility, scalability and security. Security is one of the important tenets for the success of IoT. In this paper, we discuss the challenges and possible solutions for IoT security that needs to be addressed at IoT perception layer/Edge node. The inevitable component of the IoT edge node is microcontroller/System on Chip (SoC). The microcontroller/SoC used in sensitive applications consists of Trusted Execution Environment (TEE), a hardware support for security. TEE's are not sufficient to address all the security issues in IoT systems. Hardware security issues like hardware Trojans, counterfeiting and debug security are tightly interlinked with the IoT perception layer security. There can be common solution to the hardware security issues and IoT perception layer security. In this paper, we briefly discuss the challenges in IoT design, IoT security, vulnerabilities of edge device, existing solutions and need for new security architecture for IoT edge nodes. And finally we present what security features, the next generation SoC/microcontrollers should incorporate to solve both hardware intrinsic security and IoT perception layer security more holistically.**

Keywords: **Internet of Things, Microcontroller/System-on-Chip Security, Hardware Security, Security Infrastructure IP**

I. INTRODUCTION

The idea of Internet of Things (IoT) is to connect the digital and physical world seamlessly to create a network of objects which communicate with each other. There can be millions of objects in the network with a capability to take intelligent decisions. The success of IoT can raise the quality of human life to a new level. The complete IoT ecosystem consists of sensor and actuators, microcontrollers with modest processing and connectivity capabilities, network gateways and cloud computing. Generally, consumer of data is also a producer of data in IoT ecosystem. Smart devices enabled with microcontrollers suitable for IoT applications will interface with sensor, actuators and networks. The communication networks generally used are Wi-Fi, GPRS, 3G, Zigbee, Bluetooth, etc and finally cloud infrastructure to support large scale processing and data storage. The known challenges in an IoT ecosystem are: - identification or authentication for addressing an IoT node, choosing a right connectivity technique, maintaining data compliance across network and security. The permeation of IoT's will bring drastic change to every known sector including agriculture, manufacturing and services. The core tenets to follow in the IoT design are: - agility, scalability, cost and security. Security is of prime importance because it is a part of challenge and also it is one of the core tenets in the IoT design [1].

The simple architecture of IoT ecosystem contains edge nodes, gateways, network and cloud [2]. The edge nodes (devices) are found in industries, consumer electronics, and home appliances etc, which collect data from sensors and interact with physical objects in the ecosystem. The edge nodes are also called as perception layer devices in IoT ecosystem [2]. The edge nodes are generally powered by microprocessors/microcontrollers or System on Chip (SoC) chips. Edge nodes are connected to internet through gateways. Gateways are generally standalone devices, which support wireless and wireline communication protocols. In recent times, gateways are getting embedded with edge nodes [3]. Gateways are generally designed using microcontroller/SoC devices. The universal gateways can be designed with the right mix of hardware and software. IoT device connected to cloud through internet is a globally interconnected network used to share data, store data and used to extract the meaningful information out of data through large scale data crunching. The IoT value chain includes variety of solutions: - hardware (processors, chipsets, SoC's, gateways etc), custom designed software solutions, network services and cloud services [1].

There are many research problems associated with IoT. The well-known research issues in IoT are discussed briefly: -

Data interoperability: - Billions of devices generate disparate data with their own formats. Data transmitted from processor to gateways and to cloud servers should use data format, which is understood across the different IoT layers. The standardization of data and representation languages, with a scope for constant upgradation is a good research problem [2].

Low power device (edge node) support: - Most of the IoT edge devices are low power and battery operated. Choosing components to design an edge node is very important. The microcontroller/SoC used in edge device must support internet connectivity. Internet connection is not optimized for low power consumption [19]. Power management in IoT edge devices is crucial, as it should be powered on and connected to network continuously. Designing an edge device with low power components without affecting the performance is a challenge for designers [2].

Security and Privacy: - Success of IoT based product or solution highly depend upon its strong security features. Security of IoT system is complex and challenging because it is a network of many connected devices communicating with each other all around the globe. In this complex ecosystem, at any stage there can be malicious hardware or software which will compromise security. The security issues are serious, because data communicated in the IoT networks are sensitive ranging from personal health information, trade secrets of a commercial firm and sensitive government information. It is very critical to ensure data security and system security, which is a multidimensional research problem [2].

Product development and manufacturing: - Product development and manufacturing are highly diversified in the IoT ecosystem, due to large number of applications coming under IoT umbrella and high number of IoT hardware (mainly edge devices and gateways) designers and manufacturers. Lack of standards in edge device and gateway design will create compatibility issues across IoT edge nodes in future. There is a need for regulations and standards to follow in designing edge and gateway nodes. Developing standards and regulatory mechanisms needs serious research.

Analytics: - Data mining and crunching is a crucial component in IoT ecosystem, to extract meaningful information from raw data generated from different sensors and data collected from various sources including social media. Handling different patterns of data is a unique challenge in IoT. Each edge node will have some amount of processing capability, which is helpful in converting a data into standard pattern and small amount of processing. Based on this concept, fog computing technique is developed and discussed widely in recent IoT literature. The traditional data mining algorithms suitable for centralized computing infrastructure does not fit into IoT. There is a need to develop novel algorithms for data analytics which support fog computing and modern IoT requirements. Further, critical challenges are: - to decide on how much data to collect, aggregation of data through different edge nodes, routers, gateways and finally into cloud [4].

In paper [7], authors list the vulnerabilities and threats to the IoT edge node and paper [2] describes the categories of security issues ranging from hardware exploitation to power management in the perception layer of IoT ecosystem. SoC/Microcontroller is an inevitable part of perception layer and solutions to the vulnerabilities at IoT edge nodes should be addressed at SoC level. The SoC manufacturers are also facing hardware security issues like counterfeiting and debug security. This paper discusses solutions available to address security issues in current day microcontroller/SoC and necessary features in SoC to address the security challenges in IoT and hardware security.

In this paper, we mainly focus on security problems and solutions connected with IoT edge device (perception layer). The section II discusses the IoT security comprehensively and compares IoT with embedded systems and cyber physical systems security. Section III discusses the IoT edge device vulnerabilities and section IV discusses the existing solutions found in literature for IoT edge device security. Finally, in section V we present the possible solutions the SoC/microcontroller ODM's (Original Design Manufacturers) can incorporate in their products targeted to design IoT edge devices, which are useful in securing the IoT edge devices more holistically. Section VI concludes the paper.

II. IoT Security

In the development of embedded systems used in sensitive applications, security was considered as important part of product development lifecycle. IoT is unique in several aspects in comparison with traditional embedded systems and cyber physical systems.

IoT and Traditional Embedded Systems: Embedded systems are designed to perform specific applications with the right mix of hardware and software. In embedded systems, depending upon the functionality connection to internet is an optional one. Most of the embedded systems are isolated devices without connectivity to internet. In the case of IoT, connection to internet is mandatory. Embedded systems will communicate with few devices nearby and in the case of IoT, billions of heterogeneous devices talk to each other in the ubiquitous network. Another difference between IoT and conventional embedded systems is the amount of data getting processed. IoT ecosystem process large scale data compared to embedded system. Tamper resistance and suitable encryption schemes to protect sensitive data are generally found security measures in embedded systems. In IoT, we have to deal with range of security issues from perception layer edge devices to cloud data centres, which will be discussed in this section [5].

IoT and Cyber Physical Systems (CPS): - CPS is a system which comprises of both cyber and physical components. Both cyber and physical components are bind together using computers and communication systems makes the CPS [6]. CPS is an integration of sensors, actuators, communication networks and control systems, in which status of physical system is monitored with the help of sensors and suitable control action is taken. Data transactions will occur through communication channels. The concept of IoT is very similar to CPS. CPS is well established domain which has got numerous application areas similar to IoT like smart grid etc. IoT is very different from CPS in terms of number of systems connected to communication link (internet), the amount of data generated and scope for scalability. CPS is a system infrastructure and IoT is networking infrastructure connected to large number of devices compared to CPS. For CPS, real-time control is a primary goal, while in IoT, resource sharing, data sharing and effective data crunching with minimum latency are important. The security aspect in CPS is much simpler challenge than security of IoT. Applying conventional cryptographic techniques, the data security is achieved in CPS and techniques used in embedded systems security are equally applicable in CPS.

The factors responsible for emergence of IoT are: Availability of high performance processors at low prices, improvements in data storage techniques (cloud) and efficient wireless communication systems (4G) to connect multiple layers in the system hierarchy at affordable prices. All these factors made a concept of IoT into reality, which is redefining the products and services in most of the application verticals of semiconductors.

Factors affecting security of IoT:-

- Scalability: -The major challenge for security is scale, diversity and customization. The IoT system will have billions of devices connected in the network. Designing holistic data and system security using generic cryptographic techniques for a large system is difficult. Designing scalable security architecture in the presence of customization is a critical challenge [7].
- Diversity: - Diversity of IoT edge device platforms and gateways make generic security design challenging. Customized security architecture is deployed by edge device manufacturers (platform developers) which makes the designing security for whole IoT system more complex and challenging.
- Device life: - In few IoT applications, device life is very short and in few applications like automotive device life is very high. Security techniques needs to be designed based on application and device shelf life. For the devices with long life, there must be option to update security features through software/firmware updates to defend against new threats and attacks.
- Open-source systems: - Open source software is widely used in IoT systems. The usage of open source programs is advantageous for quick development of IoT devices. Developers should carefully choose the software and must have a framework to validate the open source software, that it does not contain any malicious functionality. At present, most of the IoT edge device manufacturers use open source software and most of the IoT edge devices use same open source software may have same type of vulnerabilities, which is an advantage, such that, same solution fits wide range of applications. At the same time, it is equally dangerous; the whole system will collapse if an adversary use the same vulnerability in all edge nodes and attack all devices in the network [2].
- Firmware/Software Update or Upgradation: - IoT systems can be upgraded remotely through the network. Most of the manufacturers send updates over the air (OTA). Supported by cloud, update distribution can be done using centralized infrastructure without much user involvement. In this case, security challenge is of two types: - proper authentication and identification of the edge device in the network of billions and to make sure no malicious drivers or software is not installed on edge devices in the name of updates and upgrades [2].
- Cloud Data centre: -All commercial activity in IoT is supported with cloud based data storage infrastructure. Cloud is an integral part of IoT ecosystem and enables most of the services. Cloud security and IoT edge device security are mutually dependent factors. In designing security, we have to look into complete ecosystem more holistically across different hierarchies from cloud to final edge devices to ensure there is no compromise in security at any layer.
- Authentication and pairing: - Large number of devices in the IoT network complicates the pairing of devices. Pairing is required to aggregate and segregate the data generated from edge nodes. It is important make pairing process secure. The adversary can tamper with data and node identification credentials. Compromise in the security at one node may open up communication channel among device to device and device to routers. And power consumption and security are closely interconnected in IoT [7]. Security architects must consider power consumption patterns and available power supply capacity at edge node in designing protection to edge nodes.

III. Vulnerabilities of IoT Edge Devices (Attacks on Perception Layer)

The IoT edge devices collect data from sensors and control the physical components of the system. The possible attacks on IoT edge devices are discussed below [7] [2]: -

- Node Capture Attacks: - In this type of attack, an adversary will capture the node or replace the entire node, or tamper the hardware device. The confidential information like cryptographic keys, access keys and other assets related to digital rights management are exposed. The fake node can act like a malicious node in the network, which further compromise the security of entire IoT network.
- Malicious Code Injection Attack: - The adversary will inject the malicious code into the memory of the node, using debug modules of the node. Malicious code will not only perform unintended functions, but can also give the adversary access to complete IoT network. This happens mainly during firmware/software upgradation through OTA.
- False Data Injection Attack: - An adversary can pump erroneous data through a tampered node, which lead to malicious events in delivery of services to end-user/customer. It may also cause denial of service (DoS) attack.
- Side-channel attacks (SCA): - Different types of SCA based on power consumption, timing, test infrastructures, fault attacks, electromagnetic and laser based attacks leak the secret keys used in encryption of sensitive data. Different types of countermeasures against various SCA are implemented with cryptographic modules in modern chips. Edge device should have defense against all types of possible SCA.
- Eavesdropping and Interference: - Adversary can eavesdrop at any point in the communication channel both wireline and wireless to leak the data. Light weight encryption algorithms must be used in IoT edge device to keep the data protected from eavesdropping. Adversary can also interfere and

create denial of service attack by pumping noise and distort the data during transmission.

- Sleep Deprivation Attacks: - This attack is similar to Denial of Service (DoS) attack, by draining out the battery connected to edge device. Generally, edge devices are designed for low power consumption. Either by tampering hardware or pumping malicious into memory (code executes in infinite loop) can increase the power consumption of the edge device which will lead to DoS type of attack by draining out the battery.
- Booting vulnerabilities: - During boot process, most of the protection mechanisms are not enabled and an adversary will try to access the sensitive sections of both hardware and software to get secret keys used for encryption, digital rights management etc. Securing the boot process is crucial in IoT edge devices.
- Hardware Exploitation: - Adversary can access the debug ports, JTAG, on-chip instruments used for debug and diagnosis and get an access to confidential assets of the edge device, which are commercial sensitive. This attack is performed by dumping malicious firmware and accessing the right ports and analysing the data using sophisticated test equipments. IoT designer should choose the microcontroller/SoC with suitable debug security features or designer has to create protection by developing security firmware.
- Software exploitation: - Software vulnerabilities in IoT are very similar to conventional general computing systems and traditional embedded systems. Software architecture of IoT is an extension to the framework followed in embedded systems and all types of vulnerabilities applicable to embedded software are equally applicable to IoT also.

We discussed the possible attacks on IoT edge devices in this section which is a part of the large IoT ecosystem. Most of the vulnerabilities discussed here are applicable to gateways also. Multi-level attacks using the vulnerabilities in edge devices, gateways, routers and data centres are possible. The holistic security architecture from edge device to cloud based data centre working with tight cooperation can mitigate the attacks on IoT ecosystem.

IV. Existing Solutions

Most of the IoT literature treats the IoT from network perspective and propose specific security solution for a given application or for a given device, which is not a generic solution and incompatible in many aspects when it comes to practical implementation. In this paper, our focus is mainly on IoT edge device. The microcontroller or SoC is a heart of IoT edge device. The root of trust coming from hardware is always better and reliable than the root of trust coming from software implementation. The dedicated security module in the microcontroller/SoC used in the IoT edge device will help in designing a better protection mechanism. We primarily focus on the solutions the modern day SoC devices offer in designing the security of IoT edge nodes. The security architectures defined for traditional embedded systems are currently used in IoT devices also. These architectures will solve few security issues. Further improvements to these architectures are required to address new variety of edge device vulnerabilities in IoT ecosystem. The literature towards standardizing the security architecture has led to developing a Trusted Execution Environment (TEE) [8]. TEE is a tamper resistant computing environment running a separation kernel. TEE guarantees the authenticity of program code, integrity of crucial assets of system (processor registers, secured memory) and confidentiality of code and data stored in persistent memory [8]. Apart from this, TEE is also useful in proving the authentication and identification of the system. The content of TEE (both code and data) should get securely updated time to time to resist all types of old and new attacks from adversary. For outside world, TEE is a module which guarantees the isolation between secure and non-secure environments for both code and data. Trusted program module (TPM) is a sub-set of TEE, which is a secure cryptographic processor designed to generate the cryptographic keys, authentication and remote attestation. Several TEE modules are designed in both industry and academic research. The TEE modules designed for microcontroller/SoC are: - ARM TrustZone [9], Intel Software Guard Extension (SGX) [10] and Samsung KNOX [11]. All these TEE modules are programmable. The security architecture can be reconfigured according to requirement of end-user.

ARM TrustZone is a virtualization scheme with hardware support for memory, I/O and interrupts. Due to virtualization, ARM core can provide two virtual cores; one for secure and another for non-secure operations [9]. Based on ARM TrustZone, companies define their own proprietary TEE schemes. The details of TEE of few companies are open to public, like Nokia (Microsoft) integrate TEE called ObC [12] in Lumia devices. Similarly, Samsung's TZ-RKP [13] TEE is deployed in its Galaxy series mobile phone. Documentation of TEE architectures of ObC and TZ-RKP is openly discussed. There are few other TEE techniques like SecuriTEE from Solacia [14], QSEE of Qualcomm for which documentation is not available for public. There are few more open source TEE's developed jointly by commercial organizations and open-source community like OP-TEE [15] from STMicroelectronics and TLK from NVidia.

The TEE techniques discussed above have more similarities than differences. All TEE's are software mechanisms supported by hardware (like key generation and operating modes etc). TEE's serve the security issues in traditional embedded systems, mobile phones and high-end electronic gazettes with a reasonable success. The capabilities of TEE are not enough to address all the IoT security related vulnerabilities discussed in the previous section. Significant improvements in TEE or security architectures are required to address the IoT security issues holistically. TEE does not address the modern hardware security issues like Hardware Trojans, using unreliable counterfeit parts and debug security. Current TEE provide protection to sensitive code, sensitive data and crucial assets like processor registers and software API's. Along with the security features TEE support, we need an enhanced version of TEE or Infrastructure IP (Intellectual

Property) core for security which also address modern hardware security threats. Recent research literature in this direction can be found. Li et al in [16], propose a language and framework for implementing security policies in software. A. Basak et al in [17] propose a microcontroller based security infrastructure core for implementing security policies, which is known as E-IIPS (Extended Infrastructure IP for Security), which address modern security threats like hardware Trojans and counterfeiting. Further, there is a need to improve both TEE and IIPS to address all security issues. In a new programmable solution a firmware update should be enough to update the TEE or IIPS to protect the systems against new variety of threats and attacks. The E-IIPS or TEE does not support debug and on-chip instrumentation security, digital rights management and defense against all types of SCA.

V. FUTURE SOLUTIONS

The future microcontroller/SoC should support security features required in IoT domain and these features are also equally useful in other standalone embedded applications. Every semiconductor application vertical will change with the advent of IoT. It is always better, if root of trust comes from hardware. In the IoT era, what extra security features the microcontroller/SoC should incorporate than the current TEE offer to system developers. The Table I show the vulnerabilities of the IoT edge devices, existing security features in current day microcontrollers and possible security solutions future microcontroller/SoC offer.

TABLE I
VULNERABILITIES, EXISTING SOLUTIONS AND FUTURE SOLUTIONS FOR IOT PERCEPTION LAYER SECURITY

Name of the Vulnerability	Existing Solution in current microcontroller/SoC.	Possible Security Solutions microcontroller/SoC should support in IoT era
Node Capture Attacks: - Edge Node replaced with a fake node. [2] [7]	Cryptography based Attestation in TEE	Physical Unclonable Function (PUF) based authentication and identification scheme.
Malicious Code/Data Injection Attack: - Malicious code/data into the memory of the edge node. [2] [7]	Solution can be of two ways: - (1) Protection of porting malicious code/data into memory. (2) Defense against malicious activity of code through some security program. Existing TEE partially supports both protection and defense, which is not sufficient for IoT security. Updates are ported to IoT through OTA, so further enhancements to existing techniques are required. Defense against Hardware Trojan (HT) is not available in current schemes (TEE and other schemes).	Proper Identification/Authentication of edge nodes in the billions of nodes in the IoT network and defense against all types of malicious activity either from the firmware or inherent hardware Trojans in the microcontroller/SoC. Physical unclonable functions (PUF) or any other hardware security primitive may become mandatory in future microcontrollers to mitigate counterfeiting, identification of edge nodes in IoT, authenticating the device during updating the firmware in IoT edge node.
Side-channel attacks (SCA): - Leaking secret keys used in cryptography using different SCA based on power consumption, timing, test infrastructures, fault attacks, electromagnetic and laser based attacks. [2] [7]	Few microcontrollers used in sensitive applications having cryptographic modules consist of a countermeasure against power analysis SCA. Defense against other SCA schemes and for multi-level attacks is not available in current microcontrollers/SoC.	Cryptographic modules in microcontroller/SoC play a crucial role in IoT security. Defence schemes to safeguard the crypto modules against all kinds of SCA and multilevel attacks is mandatory in future microcontroller/SoC.
Eavesdropping and Interference: - Leaking secret data and denial of service type attack. [2] [7]	TEE support data encryption which prevents eavesdropping.	Along with TEE features, microcontrollers should have mechanism to detect DoS type attacks and security program should take suitable remedial measure.
Sleep Deprivation Attacks: - This attack is similar to Denial of Service (DoS) attack, by draining out the battery connected to edge device. [2] [7]	Current microcontrollers/SoC does not have any mechanism against this type of attack.	Same as above.
Booting vulnerabilities: - During boot process, most of the protection mechanisms are not enabled. [2] [7]	TEE or few microcontrollers support secure boot mechanisms. Access to confidential and sensitive assets is restricted during boot process.	In the current TEE, boot is secured through password and cryptography. The hardware based boot security can incorporated in future microcontrollers.
Hardware Exploitation: - Adversary can access the debug ports, JTAG, on-chip instruments get an access to confidential assets of the edge device [2] [7]	Currently, TEE or any concrete mechanism towards securing the debug instruments is not found in microcontroller/SoC devices.	Debug security will be most important feature in future microcontrollers targeted to use in IoT. A holistic Debug security will be mandatory feature in future microcontrollers.
Software exploitation: - Similar to virus, software Trojans etc. [2] [7]	Light weight anti-virus and other software defense mechanisms for embedded systems are already present.	Role of microcontroller at application level will be very less. Operating system and software level anti-virus suitable to IoT may solve the problem. Still current TEE and in IIPS protects crucial assets, even the threat comes from software applications.

Based on the discussion in Table I, we can list the few features, microcontrollers should incorporate for better security: -

- Physical Unclonable Functions (PUF): - PUF is a hardware security primitive, which is useful for microcontroller manufacturer, system developer and end user.
- Microcontroller manufacturers can mitigate IC counterfeiting and implement digital rights management (DRM) using PUF. System developers can use a PUF for accurate identification of edge nodes in IoT and authenticating the edge node, when edge node requests for upgradation of firmware or a new feature. End user can make use of PUF for cryptographic key generation [20].
- PUF circuits generate the unique set of large challenge response pairs (CRP), which are helpful in addressing the security issues. PUF derive their uniqueness in their CRP's from the process variation occurring during the fabrication of IC's. The details on PUF can be found in [18]. So future microcontrollers should have PUF circuits which are highly useful.
- Countermeasures against Side-Channel Attacks (SCA): - Defense against variety of SCA is a well-established research and microcontroller/SoC should include best possible countermeasures against all kinds of SCA, without affecting power consumption and performance of the microcontroller.
- Debug Security: - Large number of test structures and on-chip instruments will go into the chip, which are required at different times of microcontroller life-cycle, starting from production tests to in-field maintenance. Access to these instruments has become streamlined and easy after adopting the IEEE P 1687 on-chip instrument access standards [21]. So the microcontroller designers should include well defined, easy and secure access mechanism to on-chip instruments to safeguard the critical assets of system developer and end-user.
- Defense against Hardware/firmware Trojans: - A Security Controller to protect the critical assets of system against hardware Trojans and firmware Trojans.
- Finally, microcontroller should have light weight, efficient cryptographic module to encrypt the sensitive data.

The scalable infrastructure IP for security which addresses all the components discussed above will serve as centralized resource, which can provide more holistic security.

VI. Conclusion

In this paper, we have discussed the security challenges of overall IoT systems; with main focus on vulnerabilities of IoT edge devices/node (also known as perception layer). The solutions to the security problems in perception layer lies in designing efficient security architecture in microcontroller/SoC, which is inevitable component of the IoT edge node. We discuss the existing Trusted Execution Environment (TEE) in current day microcontrollers and their capabilities to solve security issues. And based on the review of vulnerabilities and existing solutions, we present the list of security features the next generation microcontroller/SoC should have to address the IoT era security issues in a more holistic way. The comprehensive solution may be an infrastructure IP core for security which implements all the features listed for future microcontrollers.

References

[1] D.Evans, "The Internet of Things- How the next evolution of the internet is changing everything" Cisco Internet Business Solutions Group-white paper, 2011.

[2] Sandip Ray, et al "The Changing Computing Paradigm With Internet of Things: A Tutorial Introduction". IEEE Design & Test 33(2): 76-96, 2016.

[3] J.Folkens "Building Gateways for internet of things" Texas Instruments White Paper, www.ti.com/lit/wp/spmy013/spmy013.pdf.

[4] Z. Chen, G. Xu, V. Mahalingam, L. Ge, J. Nguyen, W. Yu, and C. Lu., "A cloud computing based network monitoring and threat detection system for critical infrastructures", *Big Data Research*, 3:10–23, 2016.

[5] J. Wu and W. Zhao. Design and realization of winternet: From net of things to internet of things. *ACM Transactions on Cyber-Physical Systems*, 1(1), November 2016.

[6] S. H. Ahmed, G. Kim, and D. Kim. Cyber physical system: Architecture, applications and research challenges. In *Proc. of 2013 IFIP Wireless Days (WD)*, November 2013.

[7] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, "A survey on internet of things: Architecture enabling technologies security and privacy and applications", *IEEE Internet-of-Things Journal 2017*.

[8] Mohamed Sabt, et al," Trusted Execution Environment: What It is, and What It is Not", **IEEE** Trustcom/BigDataSE/ISPA -2015.

[9] ARM Limited, "Building a secure system using Trustzone technology," 2009.

[10] F. McKeen et al, "Innovative instructions and software model for isolated execution". In Hardware and Architectural Support for Security and Privacy (HASP). ACM,-2013.

[11] Samsung, "Samsung KNOX," www.samsungknox.com.

[12] K. Kostiainen, et al, "On-board credentials with open provisioning," in Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, ser. ASIACCS '09. New York, NY, USA: ACM, 2009, pp. 104–115.

[13] A. M. Azab, et al, "Hypervision across worlds: real-time kernel protection from the arm trustzone secure world," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, ser. CCS '14. New York, NY, USA: ACM, 2014, pp. 90–102.

[14] Solacia, "SecuriTEE." [Online]. Available: http://www.solacia.com/en/securiTee/product.asp.

[15] P. Brand, "Op-tee." [Online]. Available: https://github.com/OP-TEE.

[16] X. Li, et al, "Sapper: A Language for Hardware-Level Security Policy Enforcement," in International Conference on Architectural Support for Programming Languages and Operating Systems, 2014.

[17] Abhishek Basak, et al, "Security Assurance for System-on-Chip Designs With Untrusted IPs", IEEE Trans. Information Forensics and Security, 1515-1528, June-2017.

[18] C.Herder et al, "Physical Unclonable Functions and Applications: A tutorial", Proceedings of the IEEE, Volume: 102, Issue: 8, Aug. 2014.

[19] http://www.ieee802.org/15/pub/TG4.html.

[20] H. Kang et al, Cryptographic key generation from PUF data using efficient fuzzy extractors, 16th International Conference on Advanced Communication Technology (ICACT), 2014

[21] https://standards.ieee.org/findstds/standard/1687-2014.html.