International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.85 (SJIF-2019), e-ISSN: 2455-2585
Volume 06, Issue 03, March-2020

Addressing Hardware Based Security Techniques in Internet of Things (IoT)

Gurdeep Kaur[1] ,Ramandeep Kaur[2],Paramjeet Singh[3]

[1,2,3] Department of Computer Science, GSSDGS Khalsa College, Patiala – 147001, India.

Abstract— In IoT, there are a wide range of electronic devices (cameras, mobiles and sensors) that are interconnected. These devices gather and transmit huge volume of data every day by various means of devices. Because of these connected devices, there is a great risk of device and server manipulation, falsifies data and later impact on various application platforms. These devices collects data and uploads on server that store large data volume in databases, then application extract information by analyzing it based on which various services are provided. In this data flow, S/W in the upper layer rely on the H/W in the lower layer, which contains information collecting devices. If the collected data is altered, services in the upper layer could be interrupted. Therefore, to ensure service continuity in the IOT, it is important to secure the hardware layer. In this paper, we focus on hardware level security in IoT systems and various techniques such as HSM, TPM, FPGA, PUF, DICE, etc. for physical security of IOT systems.

Keywords—Internet of Things (IoT), hardware security, SoC, Hardware Root of Trust (HRoT), Physical Unclonable Function (PUF),DICE.

I. INTRODUCTION

In the year 1982, Kevin Ashton was first who projected this term "Internet of Things"[1]. IoT concept has started to shape our world including a common man's daily life. An era in which devices of diverse shapes and sizes are deployed with "smart" capabilities that allows them to communicate not only with other devices, it interacts with humans to exchange information, take decisions and execute multiple tasks. Just to provide an illustration how IoT would change our day by day life: when you go in the market and get your fridge's text message: "You are out of milk." and when you reach the dairy area, sensors alert that you've taken milk pack [2].This system provides us with the features like we are able to control our home's light remotely using a smart device to create an impression of you being at home for security measures and even we can remotely turn on our Air conditioner exactly 20 minutes before stepping in home to maintain the room temperature [3]. IOT enable people to machine & machine to machine interactions. In addition, IoT mainly focuses on the physical devices networks, vehicles, homes & other items [4]. By year 2025, IoT is expected to have more than 75 billion connections of units all across the world. IOT is powered by many technologies like wireless sensors, connectivity, electronics, actuators, radio frequency identification (RFID) etc [8]. There are some IoT applications like e-health system ,Cloud computing, Sensor Nodes, Mobile devices, which can provide a automated setup for global connectivity that facilitate humans by being susceptible, adaptive, and reacting to their requirements [7].

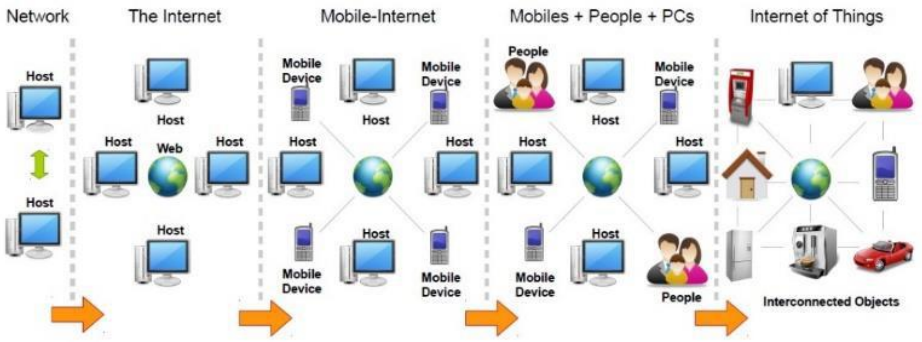

Fig. 1 Evolution from Internet to Internet of Things [6].

But as information exchange with all these things through internet, IoT is vulnerable to different security problems and has some significant protection concerns for the users [5]. IoT devices are normally associated with different devices on a similar system, which puts every other devices in danger in the event that one of them gets compromised [9].Therefore, the security dangers in IOT frameworks are not limited in software level only but hardware level security is progressively turning into a developing cerebral pain towards the designers as well as researchers [10-13].

This paper means to discover the different security issues with respect to IoT devices and techniques to determine the hardware level security. Remaining paper is sorted out as follows. Part II depicts the architecture of IoT. Part III outlines the fundamental security Issue of IoT and part IV outlines various hardware security techniques.

II. INTERNET OF THINGS ARCHITECTURE

Security of IOT is very challenging due to its heterogeneous nature[4]. In order to analyze security aspects of IoT, architecture of IOT would be of a good use. Most of the projected architectures have these layers [15,17].Hence, we draw this architecture (Fig.2) to identify and classify various security issues in IoT.

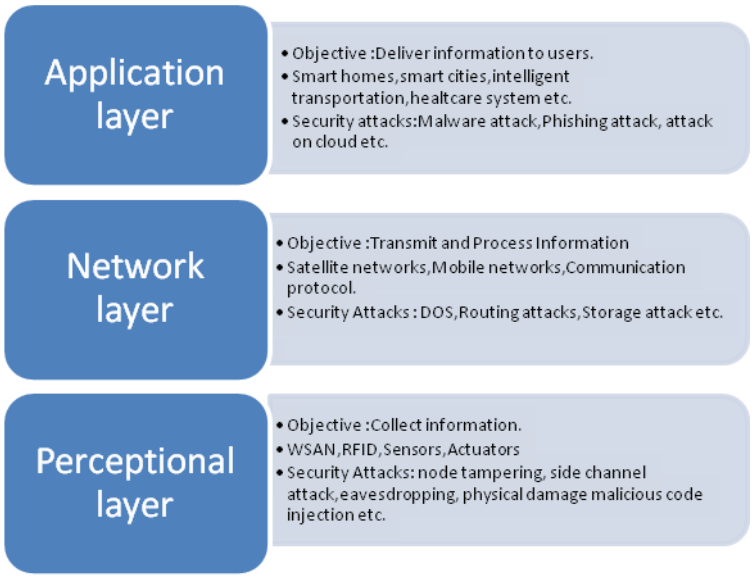

Fig. 2 IOT Architecture

A. ***Perceptual layer:*** It works like nose, ears and eyes of human beings that's by it's also called as sensor layer. The main task of this layer is to recognize the objects and gather data from them. It includes several kinds of sensors connected to objects like Radio-Frequency Identification (RFID), 2D barcode, Wireless Sensor Network (WSN), camera, GPS (Global Positioning System), etc[4,14].These are responsible for collecting data as per demand of applications and providing data to the objects.

B. ***Network Layer:*** This layer is responsible for securely transfer the data gathered by lower layer to main cloud, fog nodes or directly to another IoT node and this layer also examine as brain of IoT . Various mechanics used in this layer such as Phone N/W, Satellite N/Ws, wired, Wireless Ad hoc N/W etc [10-13].This layer gathers security tools and protocols that are responsible of transporting data in a secure manner and is also responsible for connecting the smart network devices with each other [17].And so, it is very sensitive to attacks.

C. ***Application layer:*** This layer act as application user interface between IoT users and applications. This layer gives services to users as per their necessities. These services are application dependent as they work upon the information analysed by sensors [4].Responsibility of this layer is providing various services where IoT can be deployed, such as, smart cities, smart healthcare devices, smart homes, Smart agricultures, smart automated vehicles etc.[17,18].

III. SECURITY ISSUES IN IOT

There are three main challenges that IoT H/W manufacturers and S/W developers to design complete security devices which are **processing capabilities, limited memory and power [11,19]. Small sizes** of these IoT devices are another challenge for developers. It is a major concern for IoT developers to create a device with security measures within a low memory 64KB to 640KB [20].However, they have to leave sufficient space for security software to protect against security dangers. But in IoT ,the memory and CPU is very limited .So present complex security calculations are not appropriate for them. Due to any additional security module, regardless of whether hardware or software, it needs additional vitality to perform. However, wireless frameworks that have a battery controlled, are constantly expected to be vitality productive [21].Besides, IoT devices surpass 25 billion Internet-connected devices worldwide. Testing all security-related aspects is difficult. This challenge makes IoT devices vulnerable to hacking ,attacks and other security problems[22]. Security issues can be divided into two major sections:

A. ***Software level security issues:*** Software level security incorporates Hacking, data spillage, illegal access and so on. Because of absence of legitimate security and protection assurance we can't set out to utilize those high tech frameworks in our day by day life [11]. It is conceivable to malware attack the IOT framework without users knowledge, in light of the fact that the majority of them never power the framework to breakdown and they can hack our secret data like passwords or MasterCard data and so on. Though, utilization of updated antivirus, firewall or other software can secure us somewhat against these attacks. The encryption algorithms should be stronger, basic, and vitality proficient so that tiny devices in IoT can afford the cost of them.

B. ***Hardware level security issues*****:** To get a complete H/W secured IoT structure, we have to make safe Integrated Circuits in the IoT [11]. As IC organizations rely upon different vendors because of significant expense of creation process, this carries us to a generally insecure environment to design them [23]. Utilization of third

party Intellectual Property (IP) and other structure tools (CAD) make the circumstance progressively complicated [24,29]. As threats can likewise be infused during the running of a chip after fabrication without any knowledge of users. Also, specific threats can run and power the IC to breakdown after the chip is begun working. Therefore, confidential data can be leaked. Hardware Trojan is one of them [28].It is true that security of IoT device must be accomplished by securing underlying hardware of these devices.

These days, people are more reliant on latest technological digital devices than even before. Such devices include Smart Mobiles, Smart refrigerators, Smart door lock, Smart watches and Smart home automation systems which are becoming inseparable part of our daily life. Yet it is seen that none of these systems work securely, and putting our personal identifiable information in risk. This was even proved by researchers in late 2016, as they show the way hackers can put individual's lives at risk, by accessing a Tesla Model S car's system remotely. It allowed the hackers to access and control the braking system, engine, sunroof, door locks, trunk, side-view mirrors, and more (Fig. 3) [27]. The attack can be possible through the infotainment and WiFi connection where the hackers can be able to attack to gain access to the car's controller area network (CAN) bus.

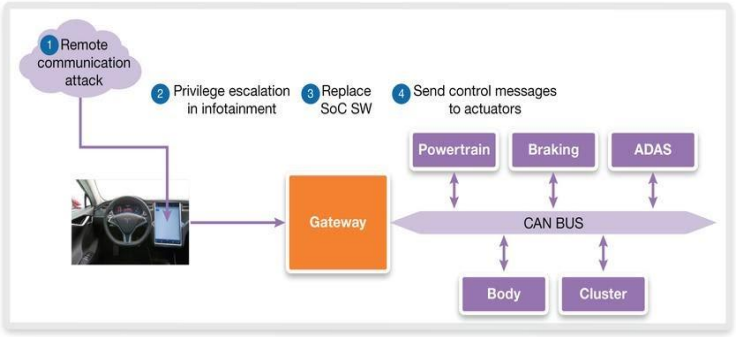

Fig.3

IV **VARIOUS HARDWARE SECURITY TECHNIQUES**

A. ***Hardware Security Module (HSM):*** HSM is a crypto processor use to give another coating of security over cryptographic keys and other secured information [31]. It act as trust anchors that safe the cryptographic system of some of the most security-cognizant organizations by securely managing, handling, and storing cryptographic keys within a fortified, tamper -resistant devices[15].These hardware machines, which are structured as well as confirmed to be tamper proof and interruption safe, give the maximum rank of physical safety. These hardware devices are frequently include in another equipment, or associated with a server, or be utilized as an independent device. Giving every device an unique identity would expand the authenticity of the devices, and this is attainable by infusing a semiconductor chip with a remarkable unique identity in every device. This procedure is known key infusion [32]. The H/W layer of IoT products are mostly exposed to physical attacks, which can change hardware or software functions by physical intervention (e.g., altering non-volatile storage or deactivate security alarm processes). One plausible method to deter such physical attacks is to integrate especially tamper-protected hardware security modules (HSM) with IoT devices(Fig. 4).

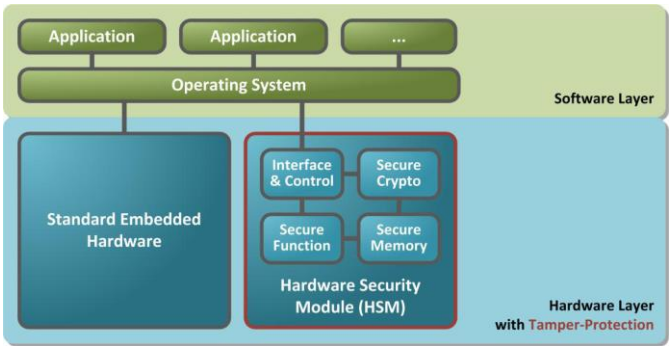

Fig.4 Hardware-security-enabled embedded systems [34]

a) **Secure memory:** Small non-volatile storage within the tamperproof HSM to stop illegitimate access of essential information (e.g., PINs or passwords)[34].
b) **Secure cryptography**: Secure encryption and decryption algorithms (Advanced **Encryption** Standard (AES) or Triple Data Encryption Algorithm (3DES)), data integrity enforcement (MAC or HMAC) or verification of data(using digital signature algorithms **like** RSA).

c) **Secure functions**: Consist of all shielded functions, which don't seem to be directly associated with cryptography, **as an example,** a physically protected clock signal, **an enclosed** random number generator, a bootstrap protection mechanism etc.

d) Interface and control: Which manages the overall operations of the HSM and provide the interface to communicate with outside the world [34,37].

e) Tamper-protection: Hardware security modules are enclosed by a physical border line (special shielding or coating which enable to tamper-evidence, temper resistance). HSMs mainly used to protect cryptographic keys. These days variety of HSMs operate in Large banks or corporate offices[38].

B. ***Roots Of Trust (ROT):*** RoT is used to guarantee that remote associated devices used in IoT is connected safely [32]. HRoT contains the keys utilized for cryptographic functions and enables a safe boot process. The most secure usage of a root of trust is in hardware making it insusceptible from different attacks[45]. it tends to be an independent security module or inside a processor or system on chip (SoC). It is used for highly security-sensitive functions. RoT is a vital part of public key infrastructures (PKIs) to create and secure, root and certificate authority keys, code signing to ensure software remains secure and generating digital certificates for credentialing and authenticating proprietary electronic devices for IoT applications. [44].This can also be utilized in a TPM combine along with several security components to provide complete security functions to IoT devices[32]. Also, Numerous VSLI dealers are tailoring security systems for a specific IoT devices which require less power, less processing power and are small sized, such security chips are called HRoT chips. Moreover, companies like intel, synopsys, microsemi have developed security patches to provide security support on behalf of client applications running on host CPUs. HRoT also utilized to stop attack codes,like root kits and bootkits[32,41].Fixed and programmable are two kinds of hardware root of trust .

a) **Fixed** ROT is normally straightforward, little and intended to perform a specific set of limited static functions (like encryption, certificate validation and key management) that can just do what it is explicitly designed to do.

b) **Programmable** ROT is worked around a CPU. It is flexible and upgradable, empowering it to run completely new cryptographic algorithms and secure applications to meet evolving attack vectors [41,42].

C. ***Trusted Platform Module (TPM):*** TPM is chip(secure microprocessor) that is added into a computing device to give H/W based security[32].TPM can safely store artifacts (passwords, endorsements or encryption/decryption keys) utilized to validate the platform (like PC or laptop).It gives platform to RoT and is able to stretching out its trust to different parts of the platform[48].It includes capabilities such as random number generation, secure generation of cryptographic keys, remote attestation and sealed storage etc [49].

For H/W verification on an end point, a specific kind of TCP chip is used for saving RSA encryption keys explicit to that system[53]. It saves multiple RSA keys to provide security to the system. First one is EK (endorsement key) which is the most safe as it is stored within the chip that cannot be examine by any S/W. Next , Storage Root Key (SRK) created by storage root at the point when the administrator takes responsibility of the system, this key is created by TPM by referencing EK. Furthermore, TMP chip also protect system from illegitimate firmware updations by creating a different key known as AIK (attestation identity key). It take care of hardware based software by segregation of critical sections of the firmware and software before they are executed. In this case, whenever someone try to change anything on firmware, the fragmented components are transferred to server for confirmation.If any of the fragmented components has been changed, there will be no match and the system can't modify the firmware. Therefore, TMP can be utilized for trusted secure boot. TPM was first established by IBM and afterward formalized by Trusted Computing[47][51]. RSA, SHA1, and HMAC cryptographic algorithms used by TPM [52,53]. TPM provides following three key features:

a) **Establishing a root of trust.**

b) **Secure boot** (complete process by which the trustworthiness of a device is established right from the chip)[52].

c) Device identification (To check the identity of the device ,the method is to create key pairs for the devices, which are then used encrypt the traffic. but, key pairs save on the disk are vulnerable to manipulate)[54,56].

D. ***Device Identifier Composition Engine (DICE):*** Dice is a protection protocols defined by trusted computing group which gives a strong device identity, secure deployment and verification of software updates, resiliency, which frequently are a source of malware and other attacks[58]. It has few hardware prerequisites which make it perfect for security and protection of limited resource devices .It is implemented in the hardware during setup. Another advantage for device manufactures is that there is no necessity to hold or store databases of unique secrets. Simple HW requirements mean DICE is versatile to any system[59]. Even the smallest microcontrollers can afford DICE support. It Provides HW-based identity and attestation, as well as sealing, data integrity, device recovery and update. Several SOCs contain fuse-banks (or other NV-memory) that can be utilized to store cryptographic keys for encryption or device identity. But, if the code running on the SoC is compromised, the fused secret key value (Unique Device Secret) can leak. Securely re-keying such compromised devices might be difficult or not possible. SoC vendors sometimes limit the risks of UDS-compromise by limiting the run-time conditions that can examine the fuse value [58].Its simplicity and robust security approach is main advantage of DICE**.** it is depends on simple cryptographic standards and fundamental features, which are "baked" into the hardware by the silicon manufacturer[59] & it also enabling unique identity and attestation of the IoT system.

a) Architecture of DICE is intended to deal with the requirement for security improvement in IoT devices, mainly when TPM might be unfeasible because of restricted resources.
b) It organizing the boot into layers and making secrets unique to every layer which is kept private by each layer and configuration dependent on a Unique Device Secret (UDS) (Fig. 5).
c) Anytime in the chain ,when setup is booted, the secrets will be different. Every layer keeps the secret private.
d) If secret is uncovered, fixing the code automatically and creates a new secret, efficiently re-keying the device. In other words, when malware is there, the device is automatically re-keyed and secrets are protected.

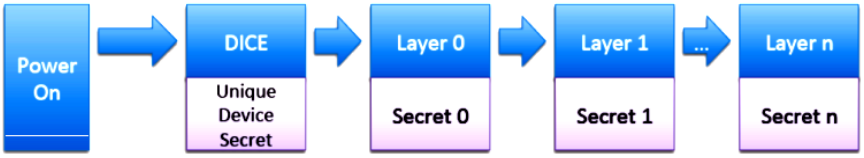

Fig.5 DICE model [34]

Firstly who accept DICE with Azure IoTs and new Device Provisioning Services (DPS) was microsoft[15,48].

E. ***Physical Unclonable Function (PUF)***:PUF is a lightweight security which can be use for secret key generation, device detection, confirmation, and capacity. They are only one of its kind due to their unclonability and tamper-resistant , as some pernicious alterations of the PUF are simply detectable [32].

a) It is a physical object that for a given input and conditions (challenge), gives a physically-defined "digital fingerprint" output (response) that serves as a unique identifier, most often for a semiconductor unit.
b) The challenge and response form a pair, called the Challenge Response Pair (CRP) and generally compared with each other to verify the authenticity of the device.
c) The distinction among the challenge and response of a PUF is alluded to as the challenge response error [56].

PUFs are most often support unique physical variations which happen normally during semiconductor producing. Today, PUFs are generally implemented in integrated circuits and are commonly used in applications with high security requirements, more specifically cryptography. The PUF utilizes the inherent assembling variations in a device to generate a unique fingerprint of the hardware that offers the valuable advantage of unclonability. This implies that the device cannot be cloned in any one even when a hacker has physical access to the device. Thus, the PUFs are unique to their device and can be utilized as a security primitive to enable device-based identification, verification and secret key generation [56].

Conventional protection methods used EEPROM and battery- supported nonvolatile SRAM in order to save secret keys, which are vulnerable to several type of attacks[42]. In addition to this, the utilization of tamper-resistant devices to save and defend keys from attacks, is essential. The conventional techniques are difficult to use in IoT devices due to the resource limitation which makes it hard to store these keys. Alternatives like Silicon PUFs give a promising security choice for IoT devices. Also, Ring oscillator PUFs are a incredible decision for key generation as they create a restricted number of CRPs for validation, which makes it very efficient for small-sized devices [46]. The techniques used for securing data transfer are public/private key exchanges. In this technique, two devices know their public key, however each must get their private key. This public and private key pair is generated by a computer instead of human and these keys cannot be decoded. Devices based on PUF uses the slight change in every die in the chip to produce a unique key based on the unique properties of each piece of silicon.

F. **The Field Programmable Gate Array (FPGA) :**FPGA is a family of reconfigurable hardware devices, where “Field Programmable” means the operation changing capability in the field and “Gate Array” means the building of internal architecture of the device. It is computing device that works like microcontroller but in different methods. A microcontroller carries a CPU that run instructions one at a time (but it can’t execute two instructions at the same time). Rather than CPU instructions .FPGA uses a **grid of electronic Logic Modules** which have lots of Logic Gates(like AND,OR,NOT etc). it offers benefits like: **low power consumption, parallel processing, Flexibility, Reliability, Low cost, and Long term maintenance.** FPGA is the most preferable reconfigurable hardware setup for the implementation of the IoT applications. FPGAs are mainly used to install cryptographic hardware, to provide secure authentication, and storage of secret data allows them to be used for IoTs[56].IoT will soon be driven by field-programmable gate array (FPGA)-like devices, for the reason that these devices can interface with the outside world very easily and provide least power, lowest latency and best determinism.

V CONCLUSIONS

To recapitulate, as per above details it is evident that it is hard to design a generic and one-size-fit-all solution which could curb diverse hardware security threat and risks. Instead to finding a generic solution, it is recommended to build the segregated security patches tailored as per application domain and type of hardware utilized, to counteract the probable security issues in that specific setup. Nowadays, hardware security has become an pivotal area seeking attention of software engineers. We cannot completely secure our Internet dependent devices without developing secure hardware for them. However, it is important to understand that there is no use of dedicating resources to find a secure solution for IoT devices if these devices have HT inserted in them which can destroy a complete system in a snap of fingers. This

research has provided us with an overview on the various techniques which are being used in post-silicon phase to ensure the complete security of IoT devices at hardware layer. We have presented a brief survey of hardware security challenges and plausible solutions. Considering the need of time, a step towards building a smart hardware security is essential not exclusively to prevent the attacks, but in addition respond in the most ideal way could be available and keep privacy during imminent devastation.

REFERENCES

[1] Yang Lu, Member, IEEE, Li Da Xu, Fellow, IEEE,*"Internet of Things (IoT) Cyber security Research: A Review of Current Research Topics"*.

[2] Muhammad A. Iqbal, Oladiran G.Olaleye & Magdy A. Bayoumi, "*A Review on Internet of Things (Iot): Security and Privacy Requirements and the Solution Approaches"*, 2016.

[3] https://www.quora.com/What-are-the-best-examples-of-the-Internet-of-Things-IOT-What-is-the-concept-of-the-Internet-of-Things-IOT#rzkQL.

[4] I. Ali, S. Sabir, Z. Ullah, *"Internet of Things Security, Device Authentication and Access Control: A Review"*, International Journal of Computer Science and Information Security (IJCSIS). Vol. 14, No. 8, August 2016

[5] T. Borgohain,U. Kumar, S. Sanyal, "*Survey of Security and Privacy Issues of Internet of Things".*

[6] Anass Sedrati, Abdellatif Mezrioui, *"A Survey of Security Challenges in Internet of Things*". pp.274-280 ,2018.

[7] Minerva, R., Biru, A. and Rotondi, "*D., 2015. Towards a definition of the Internet of Things (IoT),*. IEEE Internet Initiative, 1, pp.1-86.

[8] Evdokimov, S. Fabian, B. Gunther, O. Ivantysynova, L. and Ziekow, H., 2011. *"RFID and the internet of things: Technology, applications, and security challenges"*, Foundations and Trends® in Technology, Information and Operations Management, 4(2), pp.105-185, 2011.

[9] Maryam Daud, Quratulain Khan, Yasir Saleem, "*A Study of Key Technologies for IoT and associated Security Challenges",* Department of Computer Science & Engineering, University of Engineering and Technology, Lahore 54000, Pakistan.

[10] Yuichi hayashi, Ingrid verbauwhede, William A. radasky, *"Introduction to EM information security for IOT devices"*, IEEE ,2018.

[11] P. Ghosal, *"Addressing Hardware Security Challenges in Internet of Things: Recent Trends and Possible Solutions,"* IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing, 2015.

[12] S. Rizvi, J Pfeffer,A Kurtz, M.Rizvi, "*Securing the Internet of Things (IoT): A Security Taxonomy for IoT".2018.*

[13] T. Siddiqui, S. Saffah, B. Alazzawi, *"Security of Internet of Things"* , Int J Appl Sci Res Rev Vol.5 No.2:8, May 2018.

[14] T. Borgohain, U. Kumar, S. Sanyal, "*Survey of Security and Privacy Issues of Internet of Things".2015.*

[15] Simranjeet Sidhu , Bassam J. Mohd and Thaier Hayajneh, *"Review: Hardware Security in IoT Devices with Emphasis on Hardware Trojans"*.

[16] S. Ibrahim, Sharekh, Khalil, H. Shqeerat, " *Security challenges and limitations in IOT environments"*.

[17] M. Burhan, R. A. Rehman, B. Khan, "*IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey*".

[18] Kin Fun Li,Narges Attarmoghaddam,*"Challenges and Methodologies of Hardware* Security", Conference Paper, May 2018.

[19] E. R. Naru, Dr. H. Saini, M. Sharma, A. Omary et. al, "*A Recent Review on Lightweight Cryptography in IoT* ".

[20] Y. Labiod,A. Korba ,N. Ghoualmi, M. Amine, "*Authentication Schemes in Internet of Things: A Review"*,2019.

[21] S.babar,A. stango, N. prasad, R. Prasad, " *Proposed Embedded Security Framework for Internet of Things (IoT)*", IEEE,2011

[22] A. Bahnasaw, K. Ibrahim, A. Mohamed, et. al., "*ASIC-Oriented Comparative Review of Hardware Security Algorithms for Internet of Things Applications"*, IEEE Challenges and Methodologies of Hardware Security Conference Paper, 978-1-5090-5721-4/16/$31.00 ©2016, May 2018.

[23] N. Potlapally, *"Hardware Security in Practice: Challenges and Opportunities*," IEEE International Symposium on Hardware-Oriented Security and Trust, 2011.

[24] A. Das, G. Memik, J. Zambreno, and A. Choudhary, *"Detecting/Preventing Information Leakage on the Memory Bus due to Malicious Hardware"*, In Proceedings of Design Automation and Test in Europe (DATE), 2010.

[25] Jaya Dofe, Jonathan Frey, and Qiaoyan Yu, *"Hardware Security Assurance in Emerging IoT Applications"*, Department of Electrical and Computer Engineering University of New Hampshire Durham, New Hampshire 03824, United States.

[26] S. Koley, P. Ghosal, "*Addressing Hardware Security Challenges in Internet of Things: Recent Trends and Possible Solutions,"* IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing, 2015.

[27] https://www.synopsys.com/designware-ip/technical-bulletin/understanding-hardware-roots-of-trust-2017q4.html.

[28] R. S. Chakraborty, S. Narasimhan and S. Bhunia, *"Hardware Trojan: Threats and Emerging Solutions"*, In proceedings of IEEE International High Level Design Validation and Test Workshop, 2009.

[29] M. Rostami, F. Koushanfar, and R. Karri, *"A Primer on Hardware Security: Models, Methods, and Metrics*," in *Proc. the IEEE*, vol. 102, no. 8, pp. 1283–1295, 2014.

[30] A. Pouraghily, T. Wolf, R. Tessier, "*Hardware Support for Embedded Operating System Security*," IEEE 28th International Conference on Application-specific Systems, Architectures and Processors (ASAP), 2017

[31] https://safenet.gemalto.com/data-encryption/hardware-security-modules-hsms/

[32] Alauddin Al-Omary, Haider M. AlSabbagh, and Hussain Al-Rizzo, 2018. "*Survey of Hardware-based Security support for IoT/CPS Systems*" , pages 52–70.DOI 10.18502/keg.v3i7.3072
[33] http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.prd29-genc-009492c/ch02s01s02.html
[34] "Hardware Security Modules for Protecting Embedded Systems", Marko Wolf, ESCRYPT GmbH – Embedded Security, Munich, Germany André Weimerskirch, ESCRYPT Inc. – Embedded Security, Ann Arbor, USA
[35] L. Karter, L. Ferhati, I. Tafa, "*Challenges and Methodologies of Hardware Security"*, Security Evaluation of Embedded Hardware Implementation, Science and Information Conference, 2015.
[36] https://www.cryptomathic.com/news-events/blog/understanding-hardware-security-modules-hsms
[37] https://www.marketwatch.com/press-release/111-growth-for-hardware-security-modules-hsm-market-size-to-reach-2020-million-usd-by-2024-2019-05-15
[38] https://atos.net/en/2019/press-release_2019_05_16/atos-enforces-security-of-iot-ecosystems-with-new-dedicated-hardware-security-module
[39] L. Kim, John D. Villasenor, *"Dynamic Function Verification for System on Chip Security Against Hardware-Based Attacks,*" IEEE transactions on reliability, Vol. 64, No. 4, 2015.
[40] https://www.rambus.com/blogs/hardware-root-of-trust/
[41] A. Chen, X. Sh. Hu, Y. Jin, M. Niemier, X. Yin, *"Using Emerging Technologies for Hardware Security Beyond PUFs,*" Design, Automation & Test in Europe Conference & Exhibition (DATE), 2016
[42] Y. Chen , W. Zhang , H. Li, "*A Hardware Security Scheme For RRAM-Based FPGA,*" 23rd International Conference on Field programmable Logic and Applications, 2013
[43] https://www.thalesesecurity.com/faq/hardware-security-modules/what-root-trustNewsletter
[44] *"THE UNTRUSTED IOT A Path to Securing Billions of Insecure Devices*,Steve Hanna Senior Principal, Infineon TechnologiesCo-Chair, IoT Sub Group, Trusted Computing Group
[45] Yier Jin, "*Review Introduction to Hardware Security*", Published: 13 October 2015,ISSN 2079-9292.
[46] SECURING IoT WITH TRUSTED COMPUTING*Trusted Computing Technologies Supported: TPM and TNC*
[47] https://trustedcomputinggroup.org/resource/trusted-platform-module-tpm-summary/
[48] https://www.iotworldtoday.com/2019/02/07/trusted-platform-modules-8-surprises-for-iot-security/
[49] https://www.iotworldtoday.com/2019/03/13/trusted-platform-modules-8-more-surprises-for-iot-security/
[50] https://docs.microsoft.com/en-us/windows/iot-core/secure-your-device/tpm
[51] https://www.embedded-computing.com/embedded-computing-design/ensuring-trust-in-iot-with-trusted-platform-modules-and-trusted-brokered-io
[52] Subha Koley, Prasun Ghosal, *"Addressing Hardware Security Challenges in Internet of Things: Recent Trends and Possible Solutions*".
[53] https://aws.amazon.com/blogs/iot/using-a-trusted-platform-module-for-endpoint-device-security-in-aws-iot-greengrass/
[54] https://trustedcomputinggroup.org/wp-content/uploads/Trusted-Platform-Module-Summary_04292008.pdf
[55] A. Shamsoshoara, A. Korenda, and F. Afghah, "*A Survey on Hardware-based Security Mechanisms for Internet of Things"*, School of Informatics, Computing, and Cyber Systems, Northern Arizona University.
[56] Dhananjay Singh (IEEE, Senior Member),Antonio Jara (IEEE Member), *"Secure Layers Based Architecture for Internet of Things*".
[57] https://www.electronicdesign.com/technologies/embedded-revolution/article/21806215/a-roundtable-qa-on-the-device-identity-composition-engine-dice
[58] https://www.microsoft.com/en-us/research/project/dice-device-identifier-composition-engine/
[59] The Internet of Things-How the Next Evolution of the Internet Is Changing Everything – Cisco white paper – April 2011,www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf Accessed by July 14, 2015.
[60] Trusted Platform Module (TPM) Work Group. TCG specification architecture overview (TPM 2007), 2007, http://www.trustedcomputinggroup.org/
[61] M. Rostami, F. Koushanfar, J. Rajendran, R. Karri, "*Hardware Security: Threat Models and Metrics*," IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 2013