Blockchain as anchorage in Embedded System

Gautam Khanna[1], Deepa Mehta[2]
{gautamk95@gmail.com, deepa.mehta@gdgoenka.ac.in}

University of Waterloo, Canada[1] , GDGoenka University, Sohna[2]

Abstract. Embedded systems are systems, which are dedicated towards specific core applications, based on computer technology along with a combination of both software as well as hardware. These systems can be devised with limited potential to fulfill the stringent demands of the functioning application system, based on the reliability, valuation, power requirements as well as size. The permeation of embedded computers in human lives has become extremely profound with the development in technology. However, with increase in demands and numbers, security of such systems is always a matter of concern. This paper scrutinizes the various types of security strategies employed for embedded systems, discusses the issues faced by the systems, followed by the proposal for the employment of a blockchain based security strategy

Keywords: Embedded System, Block chain, Security

1 Introduction

The recent development in the technology, primarily in the field of computers along with telecommunications, and the ubiquitous proliferation of Internet has detonated the advent of a novel paradigm of inescapable smart environment [1]. The smart and ubiquitous environment has led to a deeper pervasion of embedded systems into the real world. With the advent of Internet-of-Things, the existing services have been acquainted with higher efficiencies along with the new application classes. Services such systems simple systems as well as a growing number of systems include supplanting of decisionmaking of humans thereby providing them the capabilities much beyond those humans can provide [2]. Some instances include, various aviation systems, such as those employed in drones, which are designed integrate the data sensed by the sensor thereby acting upon the received information quicker than that of a human, thus, empowering the world with novel features of operation [3] . The basic structure of an embedded system is given below.

ICIDSSD 2020, February 27-28, New Delhi, India

DOI 10.4108/eai.27-2-2020.2303134

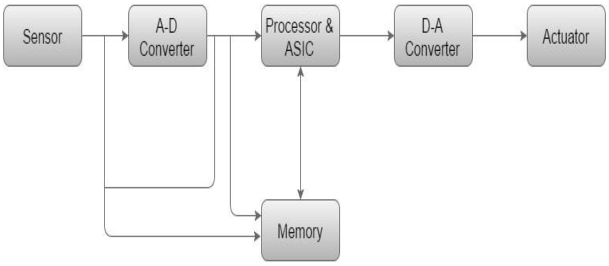

Figure.1 Structure of an Embedded System

Embedded systems are experiencing rapid growth with the invention of devices such as mobile phones, Personal Digital Assistants (PDAs), smart cards, and other music players [5]. The portability and convenience provided by such embedded systems privilege the customers to carry indispensable information, related to secure passwords, mobile numbers and so on, into the devices. The increased integration of embedded devices into the personal as well as commercial infrastructures has led to the problem of security, which strongly influences the credibility of such systems [6] .

2 Security in Embedded Systems

The embedded systems have faced plenty of well documented attacks on the associated devices which range from the hacking of anti-theft vehicles to hijacking of printers [7] which results in the sending of copies important documents to the attacker's machine. Though, embedded devices incorporate well-protected logins (passwords & OTPs) and encryption protocols (SSH/SSL), however, the security breaches reveal the inadequacy of such methods and hence, this highlights the need for robust security mechanisms in embedded systems. The past decade has discerned an elevation, not only in the number of attacks but also in the complexity of those attacks. The enterprise security fortifies protection with the help of multiple layers such as incorporating firewalls, utilizing authentication techniques, fostering the use of secured protocols as well as IDSs, which are efficacious and well manifested security fundamentals. However, security in embedded systems is based on simple authentication techniques (use of passwords & OTPs) rather than utilizing the multiple layered protection mechanisms. Since, embedded devices are vulnerable to attacks, there arises a need for efficient protection techniques for embedded devices. Although cyber security has been a prime area of focus for large enterprises, embedded computing devices still lack the incorporation of effective security mechanisms.

3 Security Challenges in Embedded Systems

Embedded devices are dissimilar in functionality to the standard PCs. They are dedicated functional devices devised essentially to accomplish an exclusive task. Embedded systems include the designing through the use of specialized operating systems (VxWorks, MQX) and Installation of any novel software on the system requires either upgrade process or is impossible for a few embedded systems. The embedded computing devices include optimization to reduce the processing cycles as well as memory usage and thus lack the availability of extra processing resources. As a result, the security challenges faced by embedded devices cannot be overcome by utilizing available PC security solutions. Due to the specialized nature of embedded systems, the available PC security solutions will not be compatible to most embedded devices [13] .

Additional challenges included in embedded device security are:

Criticality in functioning: Embedded computing devices render the possibility of controlling the infrastructure related to transportation, also involves the controlling of utility grids as well as other communication systems along with multiple capabilities related to the current environment [14]. Any attempt to interrupt the capabilities through any cyber-attack will consequentially lead to hazardous problems.

Replication Issue: After the designing of embedded devices, these are mass-produced. As one set of Embedded devices perform the same function and are identical. Any successful attack attempt against any one device can then be replicated to the other devices [15] .

Outdated assumptions on Security: It is assumed that embedded devices are not targeted for attacks. This results in the security not being considered as a critical requirement while designing the embedded devices [8]. But with the advancement in technology, the need for security has become critical.

Difficult to patch: Up gradation of most embedded devices is not possible. After the deployment, the embedded devices operate the complex software installed. Any update in the software remotely, will require designing of a capability unique to the device to ensure the updates in security [16]. The special operating systems utilized in building the embedded devices usually lack automated abilities to enable uncomplicated updates to the firmware of the device and hence enable frequent security capabilities.

Extended life cycle: The embedded devices need to run for longer years typically additionally longer than the typical PCs. The devices should be designed keeping in mind that devices should be capable of standing up to the security requirements for at least two decades but that imposes an immense challenge [17] .

Industry peculiar protocols: Embedded devices utilize peculiar protocols that are non-recognizable and not protected through the enterprise tools utilized for security [18]. Enterprise utilized firewalls and systems for intrusion detection include designs for protection against the threats specific to enterprises and have no mechanism to protect attacks on industrial protocols.

Deployment of devices outside secure perimeter: Most of the mobile embedded devices are deployed in the field. This results in the straight connection of the devices to the Internet, thus lacking all the security parameters.

4. Security Requirements in Embedded Systems

In order to design a proper security solution pertaining to the embedded devices, the factors to be put under consideration are ensuring that the firmware of the device remains untampered, data stored in the device should be safe, communication should be safe, and the device should be safe from cyber-attacks. This is achievable by incorporating security during the early stages of designing.

There is a lack of one-size fit all solution for enhancing the security of the embedded devices [20]. Security requirements also need to look into the economics of the security failure (economic, environmental, social, etc.), the risk factors involving attacks, the attack vectors, and also the economic dynamics while implementation of the security solution [21]. Features needing immediate consideration are:

Table 1: Critical Features requiring immediate attention

Features	**Embedded System enactment**
Safety from Cyber Extremism	A protocol barrier or wall used for safety from cyber extremism. A safe and secure transmission and reception can terminate attackers from hacking the software
Recognition of Intruders	While the recent devices can be hacked without any information to user, he/she should get notification alerts that their devices are being manipulated
Management of the System	A protocoled system must be introduced in the system, which can yield information about hackers and threats.
Manipulation Observation	Updated processors and motherboards are mechanized with detection software, which can observe any untoward activity

Secure Booting	Employs the use of cryptography involving the manufacturing which is done using a unique code and original hardware to justify the code hence, ensuring safety of the device and its software in ROM
Updating Safe Codes	The program on the platform confirms the updates for any bug fixing or security patching. This doesn’t allow any corrupt program to be involved in the software
Information Security	The embedded device cannot ingress without permission including safe cache memory and secured transmission and reception of information.
Validation	The transmission and reception in the device should be validated with difficult keys/passes or a validation protocol
Safe Reporting	Transmissions and Reception within the network be strong and safe using converting of data.

After studying various challenges ahead of effective IoT implementation, one of the indispensable challenge is the effective use of the plethora of data generated by the healthcare managing system. This paper presents studies the role of big data in containing the problem. The next section of this paper provides a comprehensive view of big data analytics and its uses in healthcare management.

5. Block Chain Security

Conceivably, blockchain technology is known to be an optimal solution for crypto currency. However, if applied to embedded systems, blockchain can also be manifested to be beneficial related to security [22] . The progress in the digital world has led to greater efficiencies, novel and innovative discoveries involving the utilization of mobile, IoT (Internet of Things), other analytics and cloud computing for the generation of framework for efficient decisions [23]. One of the lately introduced technology, transforming the digital world and providing a novel standpoint to making the systems more secure, resilient and efficient is blockchain [24]. Blockchain has gain popularity through bitcoin, however, researches reveal that blockchain happens to be much more promising for other areas than just a foundation for crypto currency. Block Chain is known to offer an effectively secure way of exchanging any type of transaction [25]. In order to achieve growths in the industrial areas, there needs to be formation of trusted partnerships, however, this expansion is inhibited by the cyber-attacks. These challenges can be addressed with the help of blockchain as it incorporates agile value chains, quicker innovated products, along with faster integration with emerging cloud and IOT [26] .

The dynamics of the block can be different: from a lone piece of data to several pieces of data in a single block. Another peculiar robustness of a blockchain is handling of transactions related to the variations in the state of data [29] . Blockchains proffer an ingenious process for handling transactions pertaining to the distributed environment with untrusted domain and transports. A blockchain system incorporates systems peculiarly devised to create and submit data; the task of serialization servers is to process the transactions orderly; another set of validation server are employed for verifying the transactions and creating the official blocks to be made part of blockchain; and finally, a mechanism for distribution of the validated blocks [30] . Thus, these unbeatable capabilities of blockchain incorporating the immutable and verified record of data pertaining to the distributed systems can prove to be successful in providing secrecy and integrity.

5.1 Block Chain in ESD

The previous sections of the paper included the capabilities of blockchain. This section elaborates the use of Blockchain for Embedded Systems. These capabilities in many ways can range from robust methods to gather sensor data to building more secure command and control systems that work even in the presence of system failure, degraded communications, and compromised or hostile nodes inside your perimeter [31] . While a blockchain can be implemented with standardized frameworks, such as Hyperledger or Ethereum, it can also be implemented with custom systems to meet specific needs. Embedded systems are likely to use custom blockchain implementations to meet the power, performance, and functional requirements of these systems [31] .

5.2 Blockchain in Action

One of another use of Blockchain is in the command and control of Embedded Systems. Certain embedded systems such as an autonomously functioning drone, would require verification and validation of commands along with maintenance of verifiable history. Blockchain can prove helpful in reassuring with the help of validation through validation servers and policies. The role of the validation servers to cryptographically sign the proposed transaction. The transactions related to sending a drone on a particular mission would need validations. At this particular point validation server will help validate the raw blockchain data either by utilizing the custom code dedicated to specific application. The validation server has mechanisms to verify any modifications on the data to ensure authenticity of data while it is in transit and application of additional checks to protect data. Blockchain can involve use of single validation server or multiple validation servers. The validation servers incorporate signing of the block by utilizing cryptographic hashes and corresponding private keys. After a block of data is validated, all parties involved are also sent a copy. Thus, as a result each entity possesses its own copy of the data and then they become capable of independently verifying the source of the data and also find out any modifications or tampering with records. Blockchain when applied to the drone example includes the verification of validity of the commands received by the drone and also verification of the issued commands validation by approved authorities, and confirmation of the reception of commands in proper order. Such steps avoid the risks associated with modifying the commands in transit or even having the commands changed by the person entering them into the drone. In addition to the drone, everyone else in the blockchain ecosystem can verify the sequence of commands and who authorized and approved them. The blockchain payload is encrypted thus allowing only authorized entities to read the contents. Thus, producing a an extremely robust system allowing everyone to verify the sequence as well as authority of all commands, but only the entities needing to implement a specific command can determine what that command is. This combination of properties renders blockchain to be a powerful tool for building robust, secure, highlytrustworthy systems. The blockchain is capable of supporting both low-performance as well as highperformance applications.

6. Conclusion and Future scope

The blockchain algorithms and protocols are extremely robust. However, software, and - systems using them aren't necessarily robust. However, the incorporation of blockchain technology can render the building of more robust and secure distributed systems. As the use of cryptography makes blockchain a powerful tool including various real-world applications. The researches have concluded that command and control systems face issue in the presence of disrupted and degraded communications systems. Use of blockchain also render extremely tolerant retransmission: A user is able to send (and receive) a block a thousand times and end up with a single command or transaction, not a thousand of them. There can be multiple partial transmissions of a block that then get reconstructed into a single verifiable block; blocks can come in out of order, as the blockchain enables the blocks to get assembled in the proper order no matter what order you receive them in.

References

[1] Saba Khan, Dinesh Kumar Tiwari, A Ubiquitous Computing- One of the Step Towards Smart Environment, ACEIT Conference Proceeding 2016.

[2] Professor James Larus, Chris Hankin, Markus Christen, When Computers Decide: European Recommendations on Machine-Learned Automated Decision Making, Informatics Europe & EUACM 2018.

[3] Konstantin Kakaes, Faine Greenwood, Mathew Lippincott, Patrick Meier, Serge Wich, Drones and Aerial Observation: New Technologies for Property Rights, Human Rights, And Global Environment, New America 2015

[4] Jairam Sankar, Embedded Systems- An Overview, electronicsforu.com, June 11, 2017

[5] Richard Wiggins, Personal Digital Assistants, Journal of Digital Imaging, 17(1):5-17- April.

[6] Diego Mendez, Ioannis Papapanagiotou, Baijian Yang, Internet of Things: Survey on Security and Privacy, Purdue University, arXiv:1707.01879v2 [cs.CR], 10 July 2017.

[7] Internet Security Threat Report (ISTR), Vol.22, April 2017.

[8] Alan Grau, President and Co-founder of Icon Labs, https://www.iconlabs.com/prod/securityrequirements-embedded-devices-%E2%80%93-whatreally-needed, Security Requirements for Embedded Systems.

[9] Alan Grau, President and Co-founder of Icon Labs, Icon Laboratories, Inc. 2014

[10] Ryoichi Sasaki, Professor and Director, Information and Security Laboratory, Tokyo Denki University, Cyber Security Measures, METI Journal.

[11] Dorottya Papp, Zhendong Ma, Levente Buttyan, Embedded Systems Security: Threats, Vulnerabilities, and Attack Taxonomy, Thirteenth Annual Conference on Privacy, Security and Trust (PST), 2015.

[12] Alan Grau, President and Co-founder of Icon Labs, https://www.iconlabs.com/prod/securityrequirements-embedded-devices-%E2%80%93-whatreally-needed, Security Requirements for Embedded Systems

[13] Alan Grau, President and Co-founder of Icon Labs, Icon Laboratories, Inc. 2014.

[14] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Internet of Things: A Vision, Architectural Elements, and Future Directions, https://arxiv.org/pdf/1207.0203.pdf

[15] Srinivas Vijayanand Nayani, Designing Secure Solutions for Embedded Systems, Oulu University of Applied Sciences, Autumn 2017.

[16] Eystein Stenberg, Key Considerations for Software Updates for Embedded Linux and IoT, September 19, 2017.

[17] Alan Grau, Internet of Secure Things, Icon Labs Inc. 2014

[18] Dr. John Johnson, CEO and Founder of Aligned Security, Securing Industrial IoT: There is no simple answer.

[19] Alan Grau, President and Co-founder of Icon Labs, https://www.iconlabs.com/prod/securityrequirements-embedded-devices-%E2%80%93-whatreally-needed, Security Requirements for Embedded Systems.

[20] Huichen Lin, Neil W. Bergmann, IoT Privacy and Security Challenges for Smart Home Environments, 2016, 7, 44; doi:10.3390/info7030044.

[21] Cyber Security Landscape in India, Innovation Norway, https://www.nsrorg.no/getfile.php/Dokumenter/Aktuelle%20saker/InnovationNorway_CyberSecurity%20Landscape%20in %20India.pdf

[22] . David Lee Kuo Chuen, Li Guo, Yu Wang, Cryptocurrency: A New Investment Opportunity, The Journal of Alternative Investments, 20 (3) 16-40.

[23] Ovidiu Vermesan, Peter Friess, Patrick Guillemin, Raffaele Giaffreda, Hanne Grindvoll, Markus Eisenhauer, Internet of Things beyond the Hype: Research, Innovation and Deployment

[24] Bernard Marr, 35 Amazing Real World Examples of How Blockchain is Changing our World, Jan 22 2018.

[25] Emmanuel Ferreira Jesus, Vanessa R.L. Chicarino, A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack,

Security and Communication Networks, Volume 2018, Article ID 9675050, Hindawi.

[26] Kai Wähner, Blockchain- The Next Big Thing for Middleware, InfoQ.

[27] Jimi S., How Does Blockchain Work in 7 Steps- A Clear and Simple Explanation, A Medium Corporation, May 6 2018.

[28] Jimi S., Blockchain: How Mining Works and Transactions are Processed in Seven Steps, A Medium Corporation, May 3 2018

[29] Marcella Atzori, Blockchain Technology and Decentralized Governance: Is The State Still Necessary, December 2015.

[30] Eliezer Kanal, Human Machine Interactions, What is Bitcoin? What is Blockchain? July 24 2017.

[31] Russell Doty, Blockchain for Embedded Systems, Military Embedded Systems.

[32] Margaret Rouse, MQTT (MQ Telemetry Transport), internetofthingsagenda.techtarget.com

[33] Sloane Brakeville, Bhargav Perepa, Blockchain Basics: Introduction to Distributed Ledgers, March 18 2018.

[34] Margaret Rouse, Cryptography, internetofthingsagenda.techtarget.com.

[35] Johan Ivarsson, A Review of Hardware Security Modules, Certezza, Fall 2010.