Al-Furat Journal of Innovations in Electronics and Computer Engineering (FJIECE)
ISSN -2708-3985

Securing the Systems Integrated from Cyber Threats

Rawaa Hamza Ali [1*]

[1]University of Misan, College of Science, Department of Biology, Maysan, Iraq, rawaaha@uomisan.edu.iq
[*]Corresponding author: rawaaha@uomisan.edu.iq

https://doi.org/10.46649/fjiece.v4.1.6a.25.3.2025

Abstract. *With the continued spread of integrated systems such as medical systems, Internet of Things systems and car control systems, securing these systems has become of electronic threats of utmost importance. the paper aims to provide recommendations for developers, researchers, and practitioners in the field of embedded systems security to address the increasing challenges of cyber security. Embedded systems are vulnerable to threats and hacks that could compromise their security. Overloading a power product can lead to power consumption by overusing peripherals or sensors. Embedded systems are also vulnerable to direct attacks: if a hacker gains access to the hardware, they can perform intrusion attacks on the system bus, tamper with the integrity of the system, and potentially cause peripheral damage.*
In this paper, we discuss the unique characteristics of embedded systems that address their vulnerability to attacks, exploring challenges and techniques in protecting embedded systems from cyber threats. In addition to providing an overview of common types of attacks targeting these systems, we also delve into the best practices and various security measures that can be used to mitigate the risks associated with embedded systems. These include access control methods, intrusion detection, security methods, encryption, and secure software development. In addition, we highlight the importance of continuous monitoring and updating of embedded systems to ensure their security and ability to withstand advanced cyber threats for long periods. Finally, The study focuses on reducing the uses of traditional software to include a variety of methods and techniques to identify and evaluate to produce radical ways to deal with security problems. The attack framework and types of partial analysis are reached as a business model and implemented to further implement and analyze various security methods as a means to address security problems.

Keywords: *Embedded systems; Cyber Threats; Security; Hacking; Authentication.*

1. INTRODUCTION

Embedded systems are a major target for cybercriminals because they are crucial to many different sectors, like healthcare, manufacturing, transportation, and energy. As embedded devices become increasingly integrated into personal and commercial infrastructures, security has become a critical issue. For example, if a patient wears a heart monitor that wirelessly sends data to a doctor, the embedded system must keep that information confidential and deliver it intact to the doctor. An embedded network sensor that monitors water quality to prevent bioterrorism must have multiple ways to detect tampering in both hardware and software, lest an attacker bypass security measures and compromise the water supply. Security design for embedded systems differs from traditional security design because these systems are resource-constrained in their capabilities (and therefore in their defenses) and are easily accessible by adversaries at the physical layer. Embedded security cannot be solved in a single security abstraction layer;

rather, it is a system problem that spans multiple abstraction levels. Security design for embedded systems differs from traditional security design because these systems are resource-constrained in their capabilities (and therefore in their defenses) and are easily accessible by adversaries at the physical layer Strong security measures must be in place for the purpose of protecting embedded systems as well as infrastructure as cyberattacks grow more complex and technology develops. Through using cutting-edge security protocols for solving such challenge, researchers are striving hard to enhance the defense of such systems.

The risk of unauthorized access, data breaches, and interference with embedded systems is expected to be decreased by such security measures. Embedded systems are expected to contain in the next years encryption technologies, intrusion detection systems (IDSs) and authentication processes in order to identify and halt such cyberattacks. Leveraging cutting-edge technologies like blockchain and artificial intelligence (AI) helps embedded systems' security to be enhanced, so offering threat assessment, real-time monitoring, and incident response capability. Industries could guard their vital infrastructure and raise general system reliability. Building secure embedded systems helps one to guarantee the integrity and security of private information. [1] [The use of embedded systems, which rely on the Internet, is growing in popularity across many industries. It exposes their timing and security and several technological threats.

Consequently, practitioners, policy makers, and scholars have paid much attention to the security of integrated systems. An overview of the relevance of safeguarding compact systems from electronic attacks and the difficulties in their protection is given in this study. The compact systems are special in nature, and low computing capability of resource constraints usually serves a particular purpose. Those systems operate in heterogeneous environments since their effective functioning depends on a safe and consistent interaction with other parts. Still, the spread of electronic hazards Targeting integrated systems is fast rising and seriously jeopardizes human life as well as the infrastructure. Given their special qualities, securing integrated systems offers various difficulties. First of all, such systems may need replies in actual time, therefore imposing strict time limitations that restrict the application of security methods. Furthermore, embedded systems are usually made to be resource-constrained, which makes it challenging to incorporate strong security measures considering limited processor capacity, power supplies, and storage capacity.

Additionally, the complexity of developing a unified security framework is increased by the large variety of embedded systems with regard to hardware architectures, operating systems, and application domains. A few embedded systems' long-life cycles and legacy designs make quick security vulnerability updating challenging. Dealing with changing cyber threats and safeguarding public safety, privacy, and key infrastructure depend on securing embedded systems. Nonetheless, various challenges have to be resolved including legacy designs, limited resources, real-time needs, and variability. Effective security measures and addressing such challenges depend on multidisciplinary cooperation among engineering, computer science, and other pertinent fields.

Protects embedded systems infrastructure and personal property from attacks by today's system developers. The security of the embedded devices that run our lives is not taken seriously in our society. Increased use of these devices has led to the need for security remediation methods to ensure that the devices in use are viable against threats.

System developers must add security components that often compromise system functionality, have a dedicated function, when implementing security features in an embedded system. To avoid this compromise, developers want to take a well-structured and structured code method for built-in system functionality and cybersecurity.

In particular, organizations that become a point of attack may not intend to make the incident public for a variety of reasons. It could reveal a vulnerable location in their systems or it could raise issues against their other security. Most computers are the same and it is easy for a security threat to replicate itself in another form, which is why a security risk against embedded devices does not spread as quickly as it does in a standard computer. [2]

Al-Furat Journal of Innovations in Electronics and Computer Engineering (FJIECE)
ISSN -2708-3985

This study is organized as follows: In section II, a brief description of previous studies is provided, and in the section III, the problem formulation is described. The security needs of embedded systems are presented in section IV. Methodologies of our research are followed by Section V. Section VI concludes with a summary.

2. LITERATURE REVIEW

Many studies were done to solve embedded systems' security problem through suggesting several algorithms and methods for securing such systems. One such related effort is the investigation carried out by W. Zhang W. [3], et al. who suggested an automotive embedded system security framework. With the use of methods include secure boot, code signing, and hardware IDS for protecting the system from attacks, framework of their concentrations on hardware and software security. The work of H. A. KhanH. [4], et al. suggesting a machine learning (ML)-based anomaly detection method is another pertinent investigation on securing embedded systems. Their method detects and prevents any abnormal system behavior by means of DL algorithms. Training the model using a dataset of normal system activity allows any deviation from this trend to be identified as a possible cyber threat. Since this approach does not depend on signature-based techniques, it is efficient in spotting previously unseen attacks. B. Sathianarayanan et al. have tackled the problem of ensuring embedded systems in the healthcare sector in their study [5]. Their efforts center on ensuring patient privacy and safety by protecting wearable and implantable devices among other medical devices. Their suggested all-encompassing security system calls for secure communication, encryption methods, and secure authentication. This structure guarantees safe transmission and storage of patient information, therefore lowering the possibility of unauthorized access or manipulation. Encryption is the method of data encoding such that it is difficult for unauthorized users to decode. By means of several investigations [6], several researchers have presented a novel encryption method especially intended to protect embedded devices. By means of advanced cryptographic algorithms, this method effectively guarantees the integrity and confidentiality of data transferred inside such systems. Using intrusion detection and prevention systems (IDPS) is yet another crucial component of ensuring embedded systems.

Those systems track network traffic, spot possible threats, and act preventatively to stop any malicious activity. In their 2019 work Jones and Smith assessed current IDPS methods and suggested fixes to target particular embedded system vulnerabilities. Their studies expose graduate students to IDPS's work and offer ideas on how to create increasingly successful protection systems. Furthermore, ongoing technical progress calls for ongoing security measure evolution for embedded systems. S. Khant, A. Patel [7] and others concentrate on ML-based methods to improve the security of such systems. Analyzing real-time data and identifying possible hazards helps ML algorithms to adjust and react to new cyber threats. This development forces functions—especially in terms of security—to be more flexible and integrated. Those systems are increasingly important for our daily activities as they develop more complex, network, and allow operational extension via their software. Security must therefore be our main concern. Studies [8] show that introducing security at the application level causes notable costs.

Software bug management is significantly hampered by complexity, extensibility, and connection. By taking advantage of every software problem in the firmware, operating system, and apps operating on these embedded devices, adversaries can utilize this security hole to take logical authority over the device. Since most systems with embedded systems lack distinct operating systems, operating system capability is usually handled by the software firmware of those devices. By submitting phony inputs or protocols that the program incorrectly handles, adversaries can exploit this to cause an overflow of buffers and hence seize control sequences. [9]

Al-Furat Journal of Innovations in Electronics and Computer Engineering (FJIECE)
ISSN -2708-3985

These systems' vulnerability to several known and undiscovered threats is caused by the fact that security is not usually strictly adhered to [10]. The restricted resource nature of this type of hardware further exacerbates the problem because it makes it challenging to implement widely used mitigation techniques, including address area mapping, flow of control integrity, randomization, which is and memory authorizations toward hacking attempts. [11]

In Table 1, an analysis of previous studies was made in terms of developing the main security methods and countermeasures against security attacks, which are used as references for the current research. Where development methods such as cost, power, memory size, flexibility, reliability, etc. are considered the basics of using embedded systems.

Table1. Comparison of the methods proposed in previous studies

Countermeasures against security attacks			**Developing the main security methods**			**Previous studies / Comparison methods**
Arithmetic time	SW attack	HW-attack	Cost	Flexibility	Energy efficiency	
	V		V		V	Implementation of built-in security protection on dual-processor virtual systems
	V	V		V		Compiler device model for software protection for embedded systems
	V	V	V			Embedded protection: new directions in personality recognition systems
	V		V			Safety method for off-chip memory in embedded microcontroller systems
	V		V	V		Implementation of the HW-SW model for public key cryptography for wireless sensor networks
	V					Data-driven method for secure built-in protection

3. PROBLEM FORMULATION

The main objective of this research is to suggest models and methods to solve the security problems of embedded systems at a certain stage. This goal can be achieved by defining a method that targets two categories of working individuals. Security researchers should be given the opportunity to describe the development of security processing in a reusable approach. It enables the designer of the embedded system to choose a set of security approaches given the way to consider system resource constraints and the security requirements of the embedded device.

The proposed model introduces the following principles:

1. Typical Path: Works in early development phase and is fully prepared in dealing with security issues.

Al-Furat Journal of Innovations in Electronics and Computer Engineering (FJIECE)
ISSN -2708-3985

2. Special field: which increases the efficiency of the final processing by focusing on a specific field.
3. Separation of Concerns and Responsibilities: Re-use the security process by separating the roles of the embedded system expert and the security engineer. [12]

Embedded systems are vulnerable to threats and hacking that may compromise their security. Overloading a power product may be consumed by overloading by overusing peripherals or sensors. Embedded systems are also vulnerable to face-to-face attacks: if a hacker gains access to the hardware, they can perform system bus snooping attacks, tamper with system integrity, as well as potentially cause perimeter damage.

Embedded systems have general security goals: availability, confidentiality, and integrity. This is where malware can attack systems that are embedded in the network. Encryption keys, information stored for an embedded device, or digital currencies are at risk of being unauthorized, and must be kept secure to ensure the security of the embedded systems, such as malicious or false information from system sensors or an unauthorized user.

The most important feature to consider is the capabilities of the processor, and often cannot apply sophisticated security models such as fingerprinting and encryption. A more efficient processor can reduce many threats and attacks, but it has a higher material cost and is usually only used in digital cards. The processing speed has also been increased depending on the encryption method, and this is the reason for a slight increase in the material cost of resources and the necessary need for a large amount of energy, which may not be present in mobile devices. [13]

A cyberattack describes the steps an attacker takes to infect or damage a system. There is a range of cyber-attacks, including: access attacks, attacks on privacy, surveillance attacks, and denial-of-service (DoS) hacking. A set of challenges has been shown before [14], such as confidentiality, integrity and security, as well as reliability and availability; This focuses on the need to implement processes to defend cyber security in embedded devices see Fig.1

As for network nodes, consideration of the first levels of TCP/IP will contribute to the development of embedded systems in the first steps of embedded system design. [15, 16, 17]

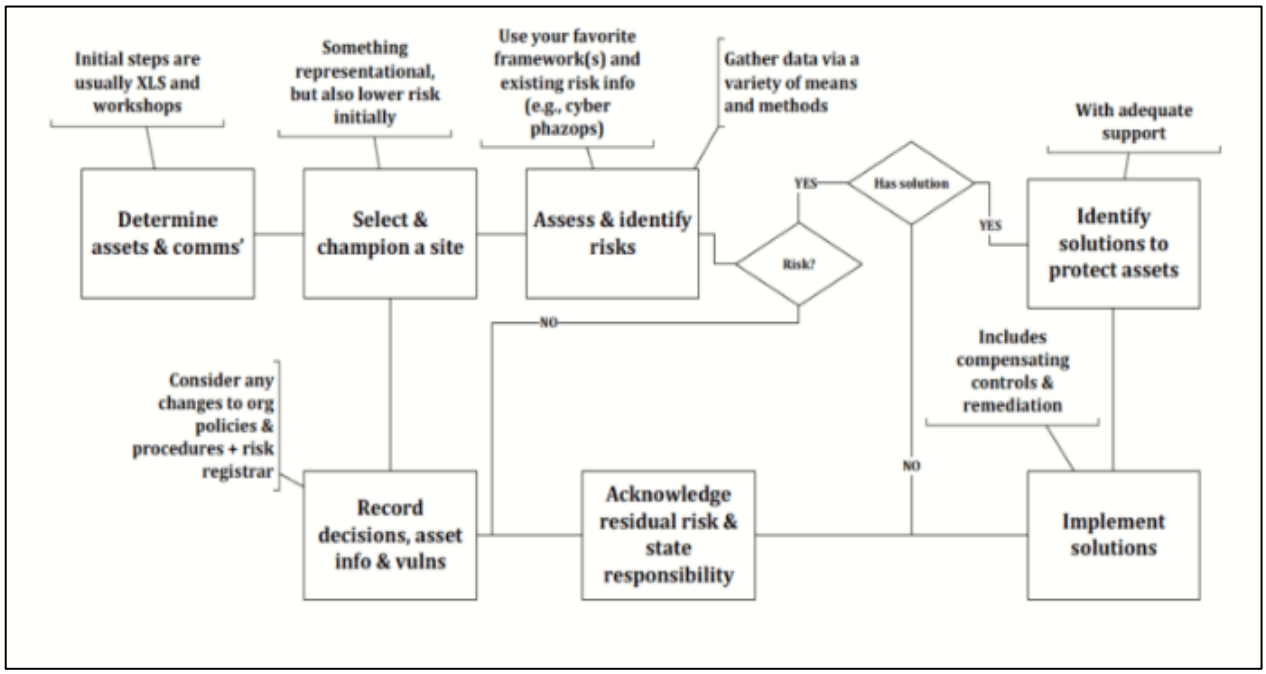

Fig. 1. Protect embedded systems from vulnerabilities

Al-Furat Journal of Innovations in Electronics and Computer Engineering (FJIECE)
ISSN -2708-3985

Embedded devices and their schemas, vulnerabilities, and network threats can now be selected and located for a host of vulnerable and insecure network protocols and outdated authentication applications.

To manage or address the risks potentially posed by embedded vulnerabilities, we recommend that asset owners:

1. Make sure to get app updates from a legitimate source.
2. Evaluate the levels of security you want for the devices, their functionality, or the area under study.
3. Maintain or upgrade the respective systems for which stable application development is available upon implementation, and/or reconfigure the systems so that they do not use outdated protocols where possible.
4. Managing the entrances to protect merchants through digital technologies and postal accounts.
5. Hardware security, network design, and the most vulnerable entry and exit points that have a statistical probability of being targeted.
6. Ensure that the original passwords are modified to a word of reasonable strength, and that unused and insecure accounts should not be activated when sending if there are safe alternatives.

4. THE SECURITY NEEDS OF EMBEDDED SYSTEMS.

Fig.2 shows the basic security needs that manifest across broad bundles of embedded devices, which are described as follows:

1. User identification Verifies the identity of users before giving their rights to access the device.
2. Disable online network access or application access unless a license has been granted to the system.
3. The specifications of secure communications include authentication of users, integrity of data, ensuring the confidentiality of transmitted data, disabling repudiation of the communication process, and protecting the accounts of users who make the connection.
4. Ensure the safe storage, confidentiality and integrity of the accurate content stored in the device.
5. Integrity of information Restricts the use of digital data saved or that can be captured by the device.

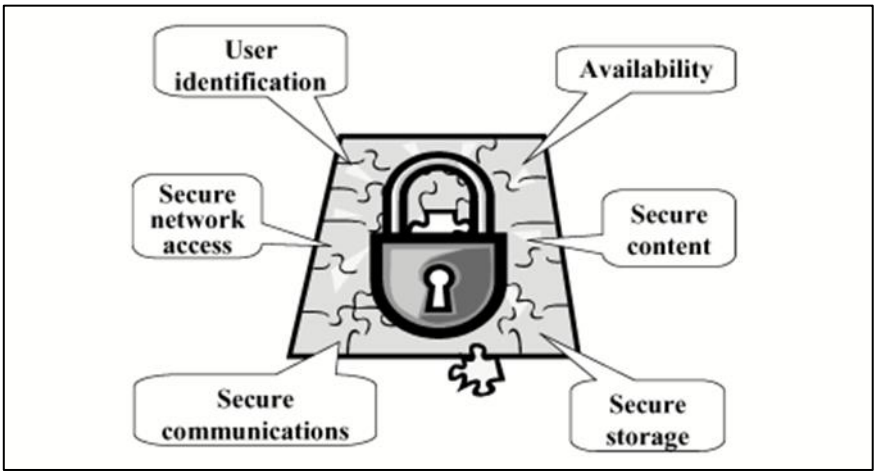

Fig. 2. Common security needs for embedded systems.

Al-Furat Journal of Innovations in Electronics and Computer Engineering (FJIECE)
ISSN -2708-3985

4.1 Basic security method - Hash Function

We have used segmentation models in order to provide a means of calculating their results, but we must first generate data based on the desired results: it is an effective one-way method. Hash methods have the following specifications:

1. The first resistance (original image): for a result denoted by y of the hash method, it is not easy to find the corresponding input x so that such that m(x) = y.
2. The second resistance before the image: For two values of (x, y) such as m(x) = y, it is not easy to search for a new parameter x^{l} that differs from x such as m (x) = m (x^{l}) = y.
3. The third resistance: (collision) It is not easy to search for inequality data x and x^{l} such as m (x) = m (x^{l}).
4. Avalanche specification: A single modification to the data can produce very different results. Makes the function more difficult for the attacker to traverse through the result space.

Hash methods are usually implemented to ensure content integrity based on checksum calculations. It is also implemented in challenge and response protocols. instance of effective hash models are Secure Hash Model (SHA) - 1 and 2 and Message Digest v5 (MD5). [18]

5. PROPOSED METHOD

This paper offers a thorough approach focusing toward threat modelling, intelligence collecting, continuous monitoring, and defensive actions. With the fast development of technology, embedded systems are becoming more susceptible to cyberattacks, therefore endangering critical data and underlying infrastructure and so providing major risks against cyberattacks. Thus, using cutting-edge techniques for protecting such systems is really vital. To provide embedded systems security, intelligence gathering comes first in safeguarding embedded systems. This calls for compiling and researching information about possible weaknesses, threats and attack approaches. Advanced intelligence systems could apply ML algorithms and AI techniques to handle enormous volumes of data from many sources, including threat intelligence, public feeds, and security advisories. Through monitoring and evaluating such sources in real time, companies could be able to proactively identify and analyse new threats, so enabling swift response to help to reduce risks. [19], Once the data is acquired, comprehensive threat identification has to be done. It is crucial to model attack scenarios for embedded systems and give such possible threats top priority and clear understanding of their possible consequences. By means of threat modelling, companies could be able to more precisely pinpoint particular weaknesses in their embedded systems and design appropriate responses.

Prioritizing activities depending on the degree of possible threats helps maximize resource allocation and direct the choice and application of security measures. Another essential part of embedded system security are defensive approaches. To either mitigate or prevent the consequences of cyberattacks. This could call for applying secure coding techniques, encrypting data, and safeguarding of communication connections. Organizations must apply hardware-based security tools such encrypted boot as well as trusted operating environments for protecting against tampering and unauthorized access. Additionally carried out must be routine penetration tests, security audits, and vulnerability assessments to identify and correct any shortcomings. [20] Continuous monitoring forms the last pillar of embedded system protection technology. Continuous monitoring and evaluation of system activities, network traffic, and security activities is necessary to identify anomalies and possible cyber threats. Advanced security information and event

Al-Furat Journal of Innovations in Electronics and Computer Engineering (FJIECE)
ISSN -2708-3985

management (SIEM) systems may combine and correlate security data from many sources, therefore enhancing the capacity of an organization to identify and respond.

Continuous monitoring helps companies quickly identify threats and take appropriate action, minimizing potential damage and ensuring the robustness of embedded systems. The engineer can also control the Trojan horse remotely, such as using television broadcast lines, in a stand-alone system. A

Trojan horse can be a peripheral of an embedded device in the form of non-contact elements or on the transistor layer of an integrated circuit. In the first approach, usually in the form of transistors in an integrated circuit, the second approach, the horse may be located on top of a device's integrated circuit board. [21]

To send all system data to an unauthorized environment through a secret passage and can be applied to remote control of the embedded device by an unauthorized party. To allow this hacking, some dangerous cell may be a periphery of the intelligent system, whether it is an embedded device that uses control models and microprocessors.

Bypass hacking can be applied to extract some confidential data that is inside a smart system. The smart device is treated as a secret box, in which a set of checks are carried out by using different stimulus packages on its inputs and observing the pattern of sources against all inputs. By comparing the results, the hacker attempts to extract the development of the ironing system and the secret data contained in it. That is, bypass attacks exploit a security vulnerability in the application of the model, given that model attacks attack a security vulnerability in the current model. [22]

As the degree of exposure of an embedded system to the Internet increases, so does the security risk. Link Internet exposure to a dynamic network configuration, and an embedded system requires degrees of defenses to maintain the security of its knowledge of other devices it communicates with. These integrity defenses scores are called Authentication, Authorization, and Accountability (AAA). AAA provides a degree of integrity to the system embedded in designating the rest of the devices on its network to which it can access and what type of data packets to use.

The information and its completeness are verified through a mathematical equation called hashing. There are a range of hash algorithm programs, the goal of which is to mitigate, if not completely eliminate, the risk of collision where more than one piece of information can output the same results. These types of hashes are called Secure Hash Algorithms (SHA). [23]

Diluting the variable data hash value to the same amount of input data reduces collision risk and increases the likelihood that the data that is detected will be modified. As shown in Fig. 3, the categories of embedded system integration are data integration and AAA model

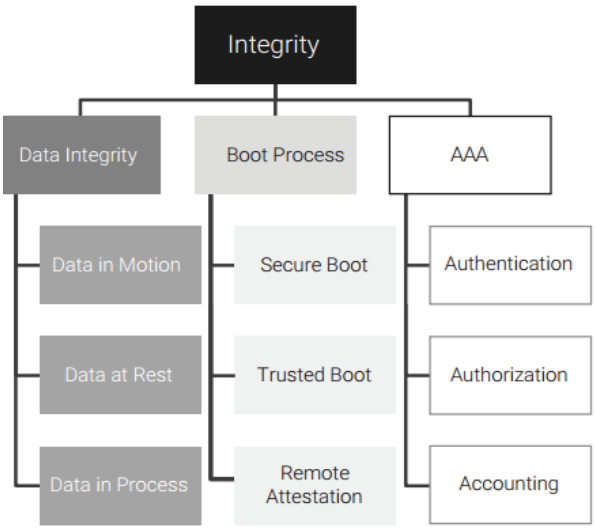

Fig. 3. Integrity applications

Al-Furat Journal of Innovations in Electronics and Computer Engineering (FJIECE)
ISSN -2708-3985

Authentication typically occurs in the device that is embedded with its software and system. The trusted neutral part consists of both the security instructions and the operating system, which will have a set of identifying tasks unique to each program. The user system will have access to the identification tasks at application time. When a program requests a service from the operating system, the request contains identification tasks. Then the operating system see fig.4 checks the source of the request before providing the service. [24]

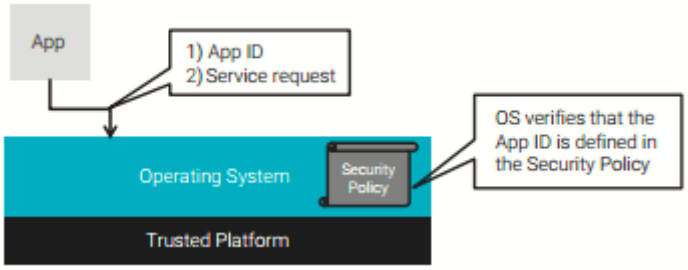

Fig.4. Authentication provided by a powerful operating system

Authorization is the designation of the class of possible access to any node in the network. Network security instructions specify the type of resources and communication channels to and from each node and to which layer access can occur. The embedded system's security instructions are routed to the robust operating system shown in fig. 5 to see if the program is able to request the service. [25]

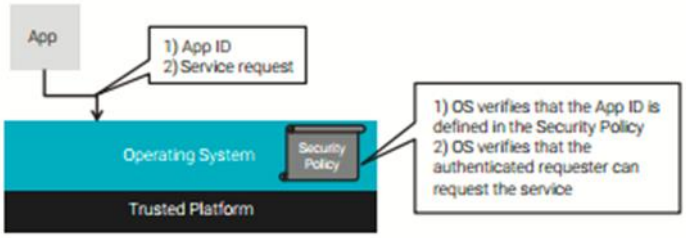

Fig. 5. Delegating a request made by a robust operating system

5.1. Remote control agent (RCA)

A Remote Control Agent (RCA) with broadened characteristics for the Mobile transversal network (NTMobile), such as virtual IP address tasks over ELDs, in Address Allocation Table (AAT) administration, and a NAT-Lite address for translation is the newly discovered home device that is carrying out the intended scheme [26].

Figure 6 depicts the RCA module's structural layout. An RCA daemon is built along with the typical RS and NTM node modules. Then, if a multiplex request arrives by the RCA daemon, it generates an RCA daemon, that utilizes the multicast request to construct a device lookup message. Network filters are also a common NAT feature in Linux that was developed for the RCA translation of addresses function [27].

Create an AAT to keep track of several default IP addresses, and proactively set an initial IP address for every ECHONET LIGHT equipment. Additionally, RCA serves as the Routing Information Protocol (RIP) component that receives the response message (VIPMN) that is sent by the ELD on behalf of the MN's virtual IP address.

Al-Furat Journal of Innovations in Electronics and Computer Engineering (FJIECE)
ISSN -2708-3985

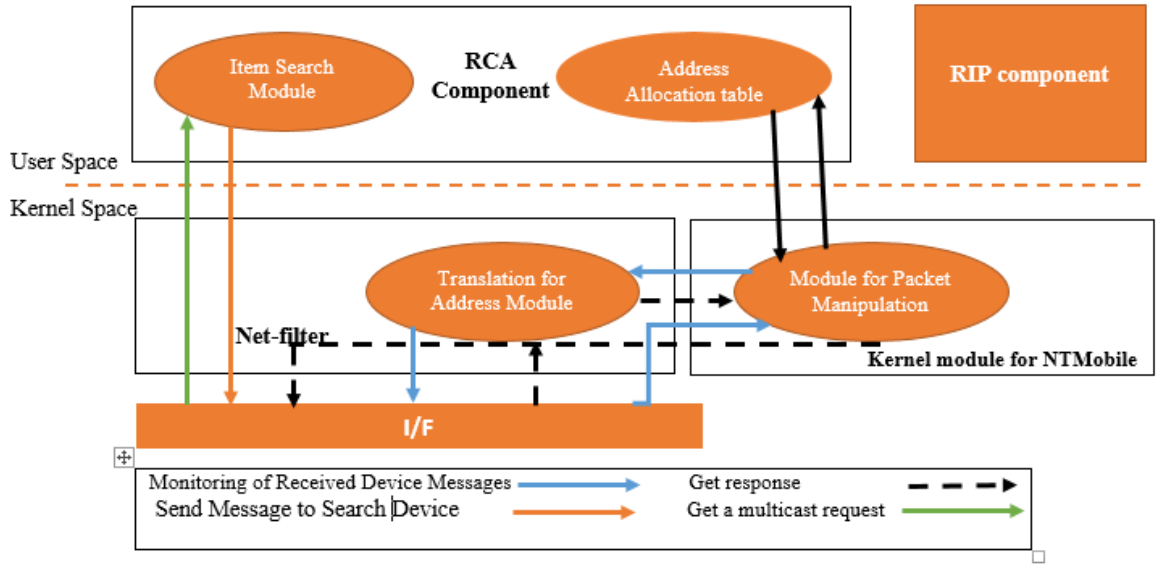

Fig. 6. RCA's module architecture

5.2. Design Space Exploration (DSE) Security at the system level

The suggested method for investigating the system-wide design space (DSE) for systems with embedded components, using a multifaceted, registry-based security quantification methodology, is shown in Fig.7.

Fig.7 shows methodology components that only require to be defined or used once in blue, while sections in red depending upon the method of investigating the space for design and must be reconsidered every time an entirely novel design instance is developed or assessed from scratch are shown in red.

Performance, energy use, and security are all other functional aspects that fall under the purview of this article. But first, we will talk about a few presumptions that define our recommended strategy before going into more depth about our method.

It does not consider any observable security issues that are merely at the application level; rather, the emphasis is on security concerns in which the fundamental embedded system structure plays a major role. As a result, we restrict our use to the following categories of attacks:

1. Side channel assaults such as electromagnetic analysis assaults, timing assaults like the latest Specter and Eclipse attacks, sweeps assaults, differential error assaults, and attacks on power analysis;
3. Software-based assaults such as buffer delays, for which defensive mechanisms may be provided at the system's level;
2. Attacks that cause denial of service;
4. Attractions meant to undermine encryption protocols.

Additionally, we take into account DSE at the system's level, where both the platform's architecture (such as the choice of platform elements like analyzing objects, recollections, and networking elements) and the allocation of application development and communication duties to particular structure elements are optimized for not only security but also for more conventional goals like efficiency, consumption of energy, and cost. [28]

Al-Furat Journal of Innovations in Electronics and Computer Engineering (FJIECE)
ISSN -2708-3985

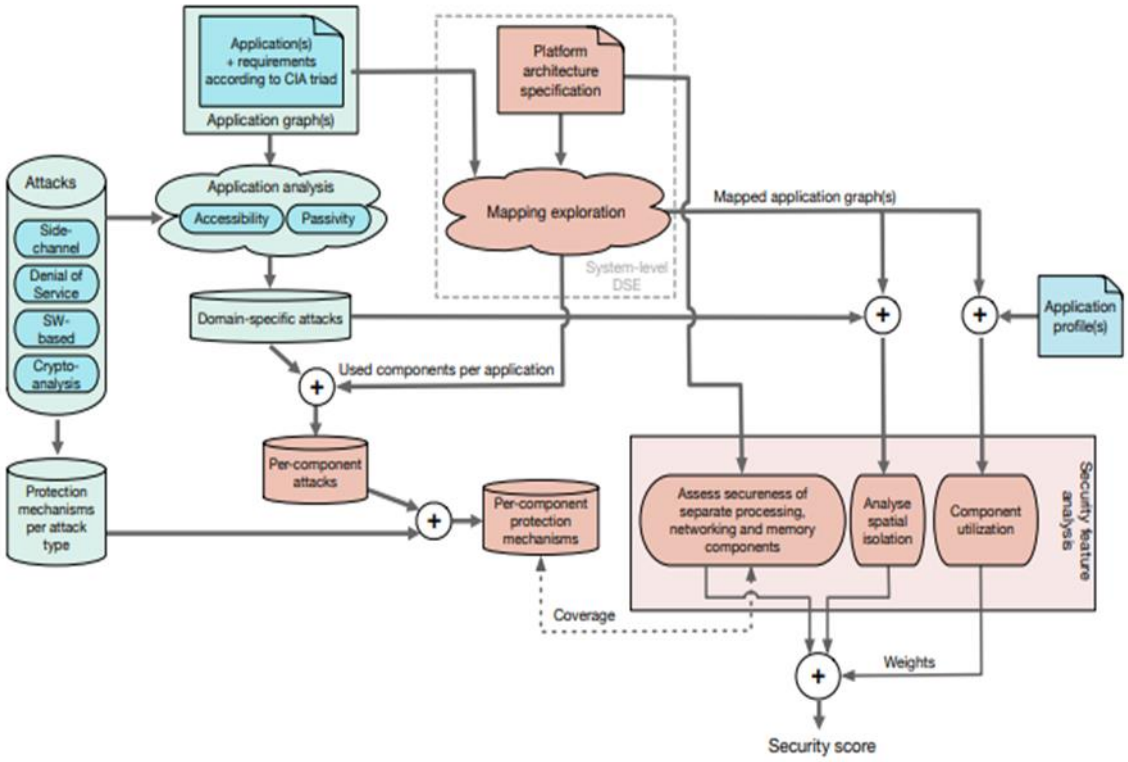

Fig.7. Examining the complex, registry-based security quantifying technique known as the safety-aware at the system level DSE using the suggested method

6. PERFORMANCE EVALUATION

Users are unable to exert authority from outside There is an analogous problem with the internet address number if the RCA servers are offline or the intrusion prevention system is fully terminated. The suggested manager and RCA [29] do not directly address issues with the existing system, and users can still utilize applications without having a place to alter them. Producers are not required to create apps away from their homes. The intended system's servers can normally be utilized for NTMobile interactions, but they may also be used for purposes other than remote control. By using its access control feature and blocking connections from other devices, RCA may also quickly ascertain that it only permits tunneling with a certain NTM node. By the way, a console often uses a VPN to access an external tool on an individual's network [30]. Technically, a VPN may be used to remotely manage ECHONET Lite devices.

However, if a manufacturer offers a service like remote maintenance and remote diagnostics [31], they can use something other than ECHONET Lite. On the other side, the system is secure since it only permits remote management of an ECHONET Lite instrument session.

7. CONCLUSION

In this study, an analysis of integrated systems within the scope of cybersecurity was conducted in order to capture the security weaknesses that require additional study to further improve the cybersecurity

of environmental services. The lack of security processing compatible with the embedded hardware specification gave attackers the opportunity to gain access to vulnerabilities and trigger multiple attacks.

This is due to the poor security of the embedded devices and the limitations of their products. Some modern security processing models require high power consumption and a lot of computational resources, so there is a great need to find good methods that do not exploit the resources of the embedded device.

All Internet communications under ECHONET management are encrypted, and the computing device does not log used. Thus, a secure and trustworthy remote-control system that safeguards user privacy may be developed.

In this paper, the topics of attacks and threats addressed against embedded devices are discussed. Hardware threats can be organized at any level of abstraction which is involved in system production to different degrees. Finally, some reverse operations against security hacking were analysed.

REFERENCES

[1] C. Duru, A. Azubogu, A. J. U. J. o. E. Aniedu, and A. Sciences, "Review of embedded systems security," vol. 17, no. 1, pp. 196-206, 2020.

[2] S. Falas, C. Konstantinou, and M. K. Michael, "A hardware-based framework for secure firmware updates on embedded systems," in 2019 IFIP/IEEE 27th International Conference on Very Large Scale Integration (VLSI-SoC), 2019: IEEE, pp. 198-203.

[3] C.-l. Xia, W. Zhang, and Z.-c. Wang, "Reduction rules for Petri net with inhibitor arcs based representation for embedded systems," in Proceedings of the 2019 International Conference on Computer Science, Communications and Big Data (CSCBD 2019), Beijing, China, 2019, pp. 24-25.

[4] H. A. Khan, N. Sehatbakhsh, L. N. Nguyen, M. Prvulovic, A. J. J. o. H. Zajić, and S. Security, "Malware detection in embedded systems using neural network model for electromagnetic side-channel signals," vol. 3, pp. 305-318, 2019.

[5] B. Sathianarayanan, Y. C. Singh Samant, P. S. Conjeepuram Guruprasad, V. B. Hariharan, and N. D. J. C. T. o. I. T. Manickam, "Feature-based augmentation and classification for tabular data," vol. 7, no. 3, pp. 481-491, 2022.

[6] P. Johnson, R. Lagerström, and M. Ekstedt, "A meta language for threat modeling and attack simulations," in Proceedings of the 13th International Conference on Availability, Reliability and Security, 2018, pp. 1-8.

[7] S. Khant, A. Patel, S. Patel, N. Ganatra, and R. Patel, "Cyber Security Actionable Education during
COVID19 Third Wave in India," in 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM), 2022: IEEE, pp. 274-278.

[8] X. Wang et al., "An Architectural-Enhanced Secure Design in Embedded System," in 2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS), 2018: IEEE, pp. 100-103.

[9] L. Z. Cai and M. F. Zuhairi, "Security challenges for open embedded systems," in 2017 International Conference on Engineering Technology and Technopreneurship (ICE2T), 2017: IEEE, pp. 1-6.
[10] K. Ott and R. Mahapatra, "Continuous authentication of embedded software," in 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2019: IEEE, pp. 128-135.

[11] A. Wetzels, "Identifying & addressing challenges in embedded binary security," ed: Eindhoven, Netherlands: Eindhoven University of Technology, 2017.

[12] M. Voelter et al., "DSL engineering-designing, implementing and using domain-specific languages," 2013.

[13] A. A. Süzen, B. Duman, and B. Şen, "Benchmark analysis of jetson tx2, jetson nano and raspberry
pi using deep-cnn," in 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 2020: IEEE, pp. 1-5.

[14] S. Hameed, F. I. Khan, B. J. J. o. C. N. Hameed, and Communications, "Understanding security requirements and challenges in Internet of Things (IoT): A review," vol. 2019, pp. 1-14, 2019.

[15] M. Abomhara, G. M. J. J. o. C. S. Køien, and Mobility, "Cyber security and the internet of things:
vulnerabilities, threats, intruders and attacks," pp. 65–88-65–88, 2015.

[16] H. Boyes, B. Hallaq, J. Cunningham, and T. J. C. i. i. Watson, "The industrial internet of things (IIoT): An analysis framework," vol. 101, pp. 1-12, 2018.

[17] S. I. Tay, T. Lee, N. Hamid, A. N. A. J. J. o. A. R. i. D. Ahmad, and C. Systems, "An overview of
industry 4.0: Definition, components, and government initiatives," vol. 10, no. 14, pp. 1379-1387, 2018.

[18] https://learn.snyk.io/lesson/insecure-hash/. "Insecure hash Using strong hashes to store passwords."(accessed).

[19] B. Tan, M. Biglari-Abhari, and Z. J. A. T. o. E. C. S. Salcic, "An automated security-aware approach for design of embedded systems on MPSoC," vol. 16, no. 5s, pp. 1-20, 2017.

[20] M. Rocchetto, A. Ferrari, and V. J. R. o. C.-P. S. F. R. M. t. T. C. Senni, "Challenges and opportunities for model-based security risk assessment of cyber-physical systems," pp. 25-47, 2019.

[21] S. J. E. S. w. A. Ntalampiras, "Automatic identification of integrity attacks in cyber-physical systems," vol. 58, pp. 164-173, 2016.

[22] N. Masmoudi, L. Bossuet, and A. Ghazel, "Experimental Implementation of 2ODPA attacks on AES design with flash-based FPGA Technology."

[23] J. Boyens, C. Paulsen, R. Moorthy, N. Bartol, and S. A. J. N. S. p. Shankles, "Supply chain risk management practices for federal information systems and organizations," vol. 800, no. 161, p. 32, 2015.

[24] P. Marwedel, P. J. E. S. D. E. S. F. o. C.-P. S. Marwedel, and t. I. o. Things, "System software," pp. 203-237, 2021.

[25] E. Barker and A. J. N. S. P. Roginsky, "Transitions: Recommendation for transitioning the use of
cryptographic algorithms and key lengths," vol. 800, p. 131A, 2011.

[26] K. Naito et al., "Proposal of seamless ip mobility schemes: Network traversal with mobility (ntmobile)," in 2012 IEEE Global Communications Conference (GLOBECOM), 2012: IEEE, pp. 2572-2577.

[27] G. Villarrubia González, J. F. De Paz, J. Bajo Pérez, and J. M. Corchado Rodríguez, "Ambient Agents: Embedded Agents for Remote Control and Monitoring Using the PANGEA Platform," 2014.

[28] D. Papp, Z. Ma, and L. Buttyan, "Embedded systems security: Threats, vulnerabilities, and attack
taxonomy," in 2015 13th Annual Conference on Privacy, Security and Trust (PST), 2015: ieee, pp. 145-152.

[29] M. Jafari, A. M. Shahri, and S. H. Elyas, "Optimal tuning of brain emotional learning based intelligent controller using clonal selection algorithm," in ICCKE 2013, 2013: IEEE, pp. 30-34.

[30] Y. Kosta, U. D. Dalal, and R. K. Jha, "Security comparison of wired and wireless network with firewall and virtual private network (VPN)," in 2010 International Conference on Recent Trends in Information, Telecommunication and Computing, 2010: IEEE, pp. 281-283.

[31] M. S. Roşu, G. J. C. S. Drăgoi, and I. Systems, "VPN solutions and network monitoring to support virtual teams work in virtual enterprises," vol. 8, no. 1, pp. 1-26, 2011.