# Privacy Preservation, Trust, and Security in Intelligent Embedded Systems

**Kusum Yadav** ( ✉ profkusumyadav@gmail.com )
University of Hail

**Yasser Alharbi**
University of Hail

**Research Article**

**Keywords:** Embedded system, intelligence, privacy, security, quality, electronic device, and sensors

**Posted Date:** October 11th, 2021

**DOI:** https://doi.org/10.21203/rs.3.rs-959603/v1

# PRIVACY PRESERVATION, TRUST, AND SECURITY IN INTELLIGENT EMBEDDED SYSTEMS

[1]**Kusum Yadav,** College of Computer Science and Engineering, University of Ha'il, Ha'il 81481, Saudi Arabia. Email: profkusumyadav@gmail.com

[2]**Yasser Alharbi,** College of Computer Science and Engineering, University of Ha'il, Ha'il 81481, Saudi Arabia. Email: y.alharbi@uoh.edu.sa

**Abstract:** An embedded system is a software and hardware system that is based on a microcontroller or microprocessor designed to accomplish the dedicated functions within a massive electrical or mechanical system. An intelligent embedded system (IES) is a generation or promising evolution of an embedded system (ES). IES has the ability of reasoning about their external atmosphere and acclimates their nature accordingly. The capacity of IES is characterized by the ability of process, service, or product to expose the performance of the environment to enrich the lifetime, quality, and satisfaction of the individual. IES facilitates the processing of information gathered from the embedded sensors. IES rely on numerous multidisciplinary methods for the successive operation.IES is widely employed in consumer electronics, industrial machines, agriculture, medical equipment, and other automated applications. It is programmable and necessary functionalities can be achieved effectively. In this article diversified utilities of embedded intelligence, challenges, issues, privacy, and security metrics of IES are discussed.

**Keyword:** Embedded system, intelligence, privacy, security, quality, electronic device, and sensors.

## 1. Introduction

In the current era of the modern and cultured universe, every human being is bounded with numerous kinds of electronic devices and computer systems. Mankind is living in the biosphere that is a physical as well as the natural world. In the progression of evolution, an artificial world is formulated with the assistance of diverse artifacts, which is accomplished by humans. The artificial world encompasses numerous machines integrated with the mechanism that simplifies and automates the performance of numerous kinds of physical activities. In this world, transmission, processing, automating, and decision-making of digital information are done by communication channels and computer systems [1].

The information perceived from the atmosphere is converted into action with the support of an embedded system. It is a combination of software and hardware that is developed for performing the necessary function with a huge system. The embedded systems are designed from the range of user interface (UI) without user interaction to the complicated graphical user interface (GUI) [2]. User interactive system enables numerous facilities to the user and the remotely accessible UI is also available with the support of ES [3].An embedded system is widely utilized in applications namely automobiles, medical equipment, mobile phone, industrial machines, and other sensor-embedded devices [4]. The embedded system is categorized based on the requirement and hardware component that is given in Figure 1.

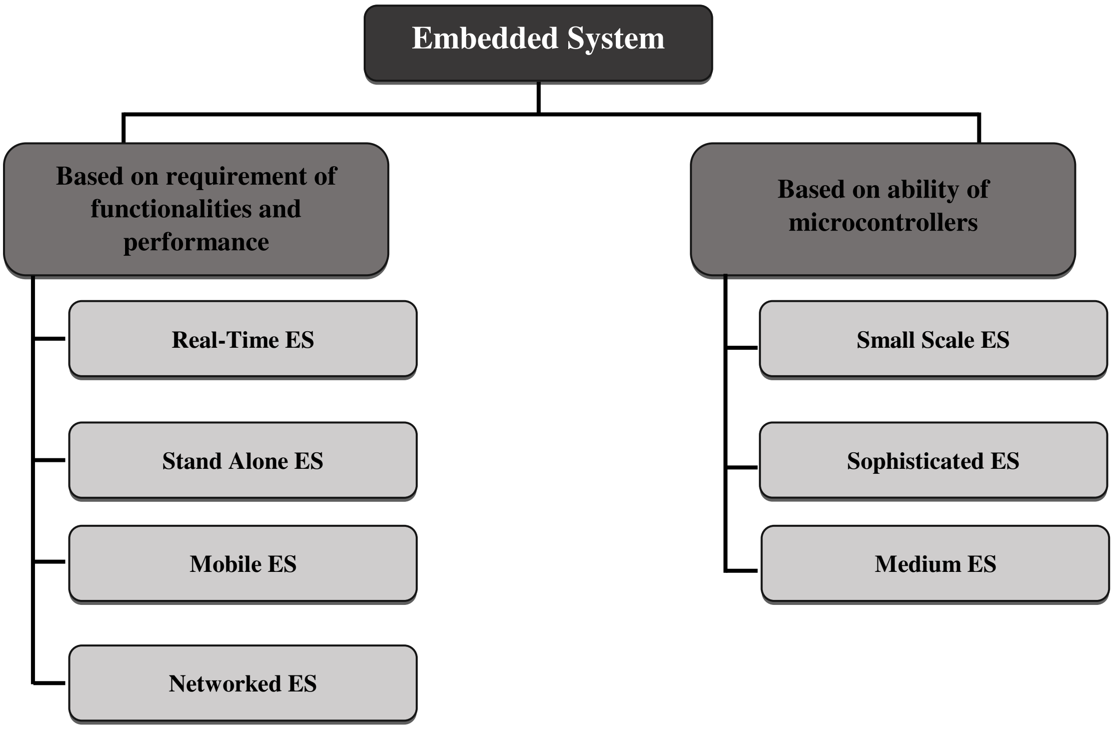

Figure 1. Types of Embedded System

Generally, an ES functions as a whole device that is embedded with necessary electronic components and needed programmable software. It comprises of power supply unit, communication port, memory unit, and processor where the embedded system utilizes the transmission port to broadcast the data among the peripheral devices and processor. The data transmission or communication among the software and hardware is done by the communication protocol. The software system is highly distinct to perform the necessary function or service where an ES serves. The communication among the hardware is established by the real-time operating system (RTOS) [5].

An embedded system is revolutionized based on the needs and the prominent generation of these ES is determined as an intelligent embedded system (IES). The capability of external world intellectual's and nature is progressed effectively by an IES [6]. The product, service, process, and other amenities are successively characterized by this approach. An individual's satisfaction and automation facility is provided by the applications developed with the IES. Itassists the processing of data gathered from the embedded sensors. IES rely on various multidisciplinary approaches for consecutive operation and performance. IES has been widely employed in sensor-embedded smart devices [7]. The embedded intelligence is programmable, highly effective, and essential functionalities can be achieved effectively [8].

Typically, embedded intelligence is relatively simple and modest to instigate in real-time applications.Based on the necessity and the addition of sensors as well as other processors into the system have made the system complicated. For an instance, aviation systems are encompassed by drones that integrate the complicated processing unit and sensor data. IES perform the action based on the processed information, which is faster than human or cloud and it permits to perform a new variety of operating feature.The utilization of IES is rapidly emerging, driven in huge part by the internet of things (IoT) [9]. Intensifying IoT-based applications namely smart home, video surveillance, smart transportation, smart hospital, wearables, and drones are anticipated to fuel embedded system progression.

The remainder of the article is structured as follows: characteristics of IES is elucidated in Section 2, diversified utilities of IES and their functionality are discussed in Section 3, issues in the IES are given in Section 4, privacy and security aspects of IES is detailed in Section 5, different significant metrics for the enhancement of IES are elaborated in Section 6 and the article is concluded in Section 7.

## 2. Characteristics of Embedded System

Task-specific in natureis the significant characteristic of the intelligent embedded system [10, 11]. Additionally, IES encompasses the following characteristics,

- Generally, IES is composed of firmware, hardware, and software-related components.
- The firmware, hardware, and software are embedded into a huge system to accomplish a specialized or specific task within the system.
- It can be a microcontroller or microprocessor-based integrated circuit system that deliver power for computation.
- IES is often utilized in the real-time sensing environment and the devices in the IoT are interconnected, which doesn’t require any user for operating the system.
- Variations in function and complexity can influence the usage of firmware, hardware, and software.
- It often necessitates performing the task or function under a certain time constraint to keep the huge system properly functioning.

## 3. Applications of Intelligent Embedded System

An Intelligent Embedded System (IES) is widely utilized in numerous applications for its task-specific nature and effectiveness in accomplishing the task [12, 10]. Different IES-based applications are discussed in this section and illustrated in Figure 2.

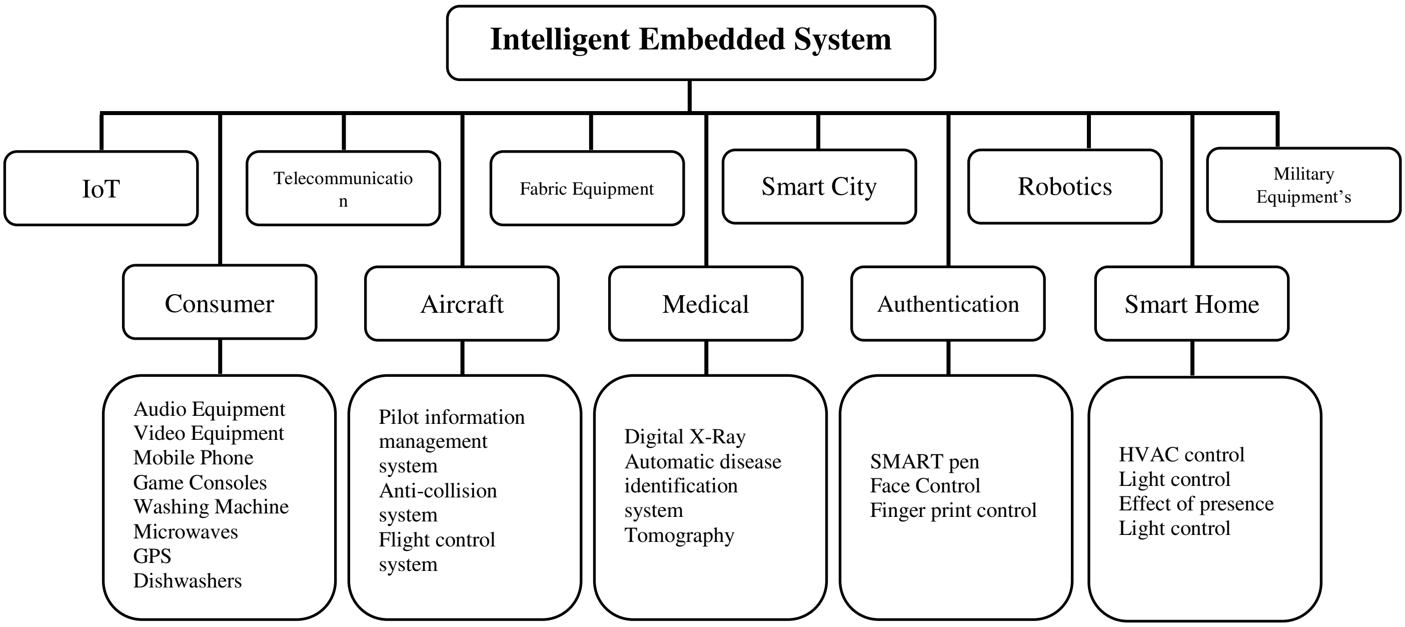

Figure 2. Application-based on IES

In the electronic industry, video and audio devices are considered significant, which includes embedded systems into television (TV) sets that lead to smart TV sets. In recent timessmartwatches and wrist bands are prevalent that are based on IESs. Different digital signal processors (DSP) are utilized in mobile phones that makes them smartphones. Also, IES is spotted in the electrical furnace, GPS-enabled devices, dishwashers, microwaves, washing machines, and game consoles. The existence of microprocessors in recent cars forms embedded systems in a distributed manner for controlling the operation of airbags, GPS, engines, electronic components, anti-breaks, and so on.

Modern planes, satellites, and helicopters are filled with numerous electronic devices, which functions together by the embedded technology and the necessary operations are performed. The term “avionics” was forged explicitly to signify the electronics systems utilized in aircraft systems. So, the first known ES was intended for a spacecraft. Now, ESs are employed in the systems utilized for anti-collision, pilot information, flight control, and others. In the military, IES is utilized in making the military equipment. The tendency of linking the distinct military-oriented embedded systems in the context or architecture of the IoT is termed as Internet of Battlefield Things.

Digital processing system permits the enhancement of medical application and equipment. Diverse forms of medical devices are converted as smart devices namely magnetic resonators, automated internal defibrillators, electronic scales, activity monitors, and digital x-rays. The possibility of remote monitoring of health and remote access is achieved by the embedded intelligent systems that are IoT. The objects in the IoT perceive the information from the environment and act accordingly that is the objects in the IoT are termed as intelligent objects. The comfort levels in the building and home are improved by the automation that is attained by the IES. The embedded intelligent technology plays a prominent role in the automation of things across the world. Evolution of diverse embedded system has raised the usage of connected devices that is given in Figure 3 [13].

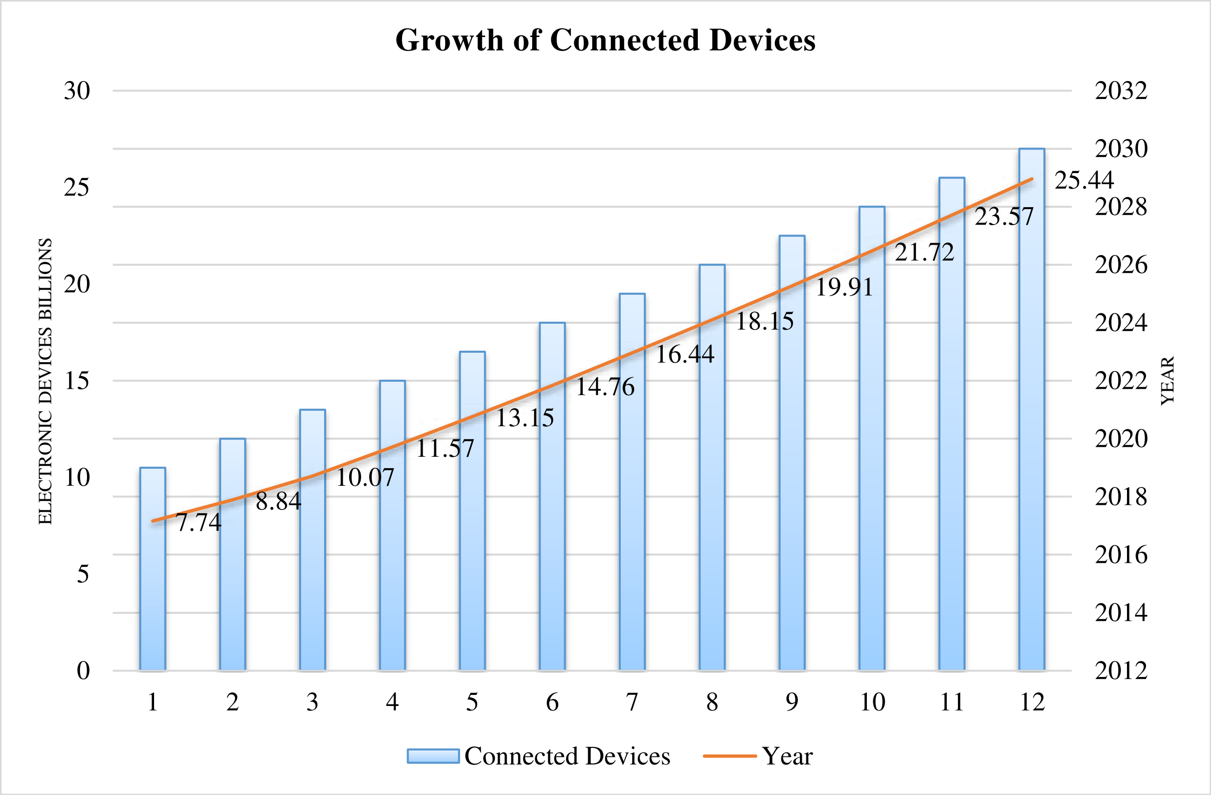

Figure 3. Connected Devices Growth

## 4. Challenges and Issues in Intelligent Embedded System

Intelligent Embedded System (IES) is composed of huge devices and functions namely smartphones, digital watches, industrial or vehicle automation systems.An IES is immune to alteration and this also generates numerous issues [14]. The challenges and issues in IES is given as follows,

- Stability: Unexpected nature of IES is inadmissible and poses complicated risks.The task-specific nature of IES may lose their stability in functioning.
- Safety: The safety of IES is considered a special feature and it is a lifesaving feature in a complicated atmosphere. IES is characterized by the strict necessities and shortcomings in terms of expertise in engineering, quality, and testing.
- Security and Privacy:In IES, security and privacy concerns are significant issues that are due to the massive amount of interconnected devices and data generated from those devices. The information shared across the devices may be confidential or personal information that might be secured. The privacy of every individual data has to be ensured over the IES.

- Integrity and Compatibility: IES is composed of diversified devices that pose issues like integrity and compatibility. The connectivity among the devices pressurizes the adaptability of devices. Integrity is the main reason for security and to prevent the system from malicious attacks at diverse levels are protected by incorporating security standards.

- Design Limitation: The challenges faced during designing an IES are limit with minimum energy, small form factor, and stability for the long-term without the need for maintenance.

Due to the challenges and limitations, the usage of embedded system is not widely recognized and the enhancement of privacy and security standards had encouraged the usage of embedded system based connected devices. The connected car is one of the prominent feature of embedded system based connected device and its growth is given in Figure 4 [14].

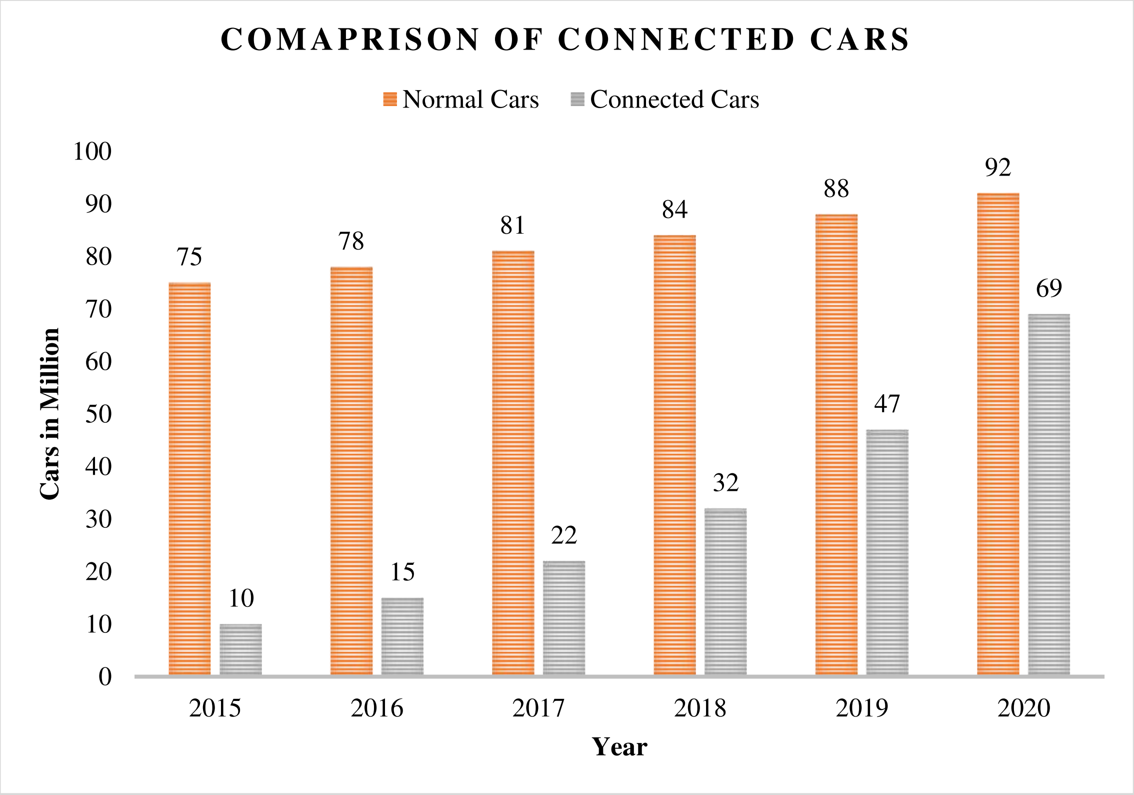

Figure 4. Evolution of Connected cars and Normal Cars

## 5. Privacy and Security Aspects of Embedded System

The traditional internet service and embedded system are susceptible to numerous privacy issues and security threats. The emergence of technology and the usage of embedded system-based smart applications generated a huge amount of data. The information generated is from diverse resources such as health care, banking, financial sector, industry, and other government organization. The personal information transmitted over the internet and processed by the embedded system, which may lead to information leakage and privacy issues.The solutions formulated for handling the privacy of the individual are given in Table 1.

Table 1. Privacy-Preserving Solution for Embedded System

| **Privacy Solution** | **Inference** | **Description** |
|---|---|---|
| Authorization and Authentication | • Establishment of key and initiation of lightweight-based authentication mechanism.<br>• Context-aware enforcing models and access control mechanism.<br>• Architecting the device based on the fingerprinting method. | This approach facilitates the identification of legitimate users. The end-to-end security scheme is progressed via two phases namely authentication and registration. The information over the system is authorized and authenticated for privacy concerns [15]. |
| Data Summarization and Digital Forgetting | • The encrypted data is deleted when the decryption key is deleted.<br>• Only necessary information is retrieved rather than the entire data.<br>• Exploits data mining and other approaches for the discovery of needed information from the database. | All the replications or copies of the dataset are deleted in the process of digital forgetting. In data summarization, the confidential information and its details are hidden or their granularity is minimized, which providesa high level of data abstraction. [16, 17]. |
| Plug-in Architecture and Edge Computing | • Software modules situated at the edge region overcome the concerns of privacy.<br>• A privacy-aware device permits every individual user to control the data.<br>• Personal cloud butlers establish the decentralized framework. | The paradigm of edge computing is widely adopted where the storage and processing occur partially on the edge of the network. The increasing of huge data generation at the edge has leveraged the concerns namely security, latency, limitations of the device, and user privacy [18 - 20]. |
| Denaturing and Data Anonymizing | • Separation techniques and data brokers deliver flexibility to the service providers and also the | In the process of data anonymization, identifiable information is removed where |

|  |  |  |
|---|---|---|
|  | access rules predefined by the user are also considered.<br>• Masking personal information is accomplished by the generalized masking technique.<br>• Emotion analytics lifestyle delivered by the privacy concerned embedded system and its frameworks, which also permit denaturing. | this information assists in the identification of an individual. This technique maintains the information about the object or people remains anonymous. Initiation of scalable and privacy-aware framework enables theprivacy features [21, 22]. |

The security issues such as replication of attack, irregular updates in the security, dependability, remote and protocol deployment [23]. Some of the properties projected for securing an intelligent embedded system from malicious activity are given in Table 2.

Table 2. Properties of Secure Embedded System

| Challenge | Goal | Mitigation |
|---|---|---|
| Data integrity is a complicated issue in IES. | The package system and its properties in integrity are protected as a container, which is attached to the system and facilitates any time of access. | Every executable system is marked as non-writable that is utilized as a disk-based solution for the protection of integrity that secures the boot. |
| At rest mode, it is susceptible to data confidentiality. | Avoids the existence of a threat from exfiltration or altering the confidential and sensitive information on the system. | The file-based encryption scheme is developed for handling this issue. |
| The resource managers are permitted unrestricted access to the system. | Avoids unapproved system and their components from accessing channels of the system resource manager or the requested operation can be restricted, which is often attached with the system. | Necessary security policies are incorporated that is access control list (ACL) and portable operating system interface (POSIX). |
| Access control for objects is permitted for the file system. | Access permission for the file system and objects are restricted by numerous process. | Access control and permission of POSIX are accomplished. |
| The data or process flow control is redirected. | The threat actor in the system is prevented from altering the executable process or control flow. | Utilization of the compiler is subjected to the relocation of the marked section in the read-only executable format. |
| Execution of code in an untrusted mode. | The threat actor in the system is prevented from loading or running the file | Utilize the utility to accomplish the files and file'sin the system that is |

| | | |
|---|---|---|
| | system in binary form. | highly reliableor trusted. |
| Repeatability of diverse forms of attacks. | This makes a complicated situation for the attackers to speculate the memory where the energy is loaded. | Randomization of address space and its layout. |
| Overflow of stack data | The existence of stack overflow based attack is mitigated by instrument code | Stack canaries are utilized in the construction of compile code. |
| Overflow of buffer data | The existence of buffer overflow based attacks is mitigated by instrument code | The fortified function is deployed to utilize the complier that supports in deletion of memory access in the out-of-bound region. |
| Confidential or sensitive information of an individual is exposed. | The process and private data on the system are prevented from the threat. Also, threat actor impact is avoided. | Implements security policies and secures the file system. |
| Delivering the least privilege for the execution of the process. | The privileged access of the system is restricted by the system configuration. Based on the necessity or requirement they execute the task with the least privilege. | Security policies are incorporated<br>Access control and permission of POSIX are accomplished.<br>Utilize the granularity of the policies that govern the distinct operation and permit them to accomplish the task. |
| Denial of Service (DoS) attack. | The interference is avoided by the threat actor with the critical device by draining the resources in the system. | Resource limitation is assigned with system call and setrlimit() in C. |
| The kernel memory is accessed by the device hardware access mechanism. | The threat actor is prevented from utilizing the devices namely network card or GPU that directly accesses memory (DMA) where the devices are not granted explicitly for the assessment of devices. | The management of system memory and unit manager utilizes the DMA containment |

## 6. Significant Metrics of Intelligent Embedded System

The issues and challenges faced in the incorporation of an embedded intelligent system are rectified by privacy preservation and security schemes. The assessment of an intelligent embedded system is attained by the following metrics.

### 6.1. Privacy Metric

The privacy measurement and their research mainly focus on user location privacy. The location-based privacy metric is projected to emphasize the significance of a single qualifier's outcome [24]. The error, uncertainty, and k-anonymity based metrics are developed for preserving the privacy that is also a location-based privacy-preserving mechanism. The k-anonymity and entropy are ineffective in measuring the privacy of the location. In the attack-centric approach, the preceding information is accessible to the attacker that will lead the attacker to perform diverse actions on the system [24].

In the location-based privacy framework, the components namely users of mobile, probable traces of distinct users, recognizable traces, mechanism of location-based privacy-preserving, evaluation, and adversary forms of inference attacks. The communication scheme in the vehicles utilizes entropy to estimate the privacy range of location [26].The dependability and security ranges of the smart vehicle are estimated from the privacy-preserving metrics.The combination of dependability and privacy achieves various levels of privacy concerns with the assistance of privacy levels [26].

### 6.2. Security Metric

The security features in IES are mainly concentrated on the software level security that is categorized as function, system, and code level.The code bugs are investigated with the code level metrics by weighting the code where the bugs are assigned with similar significance. The overall security of the system is enhanced by lowering the existence of bugs in the code. One of the main issue in the code level bug detection is giving similar significance to every bug, it doesn't denote which bugs are simple to exploit [27].

The security aspects at the system level depend on the websites and organizations, which broadcast the identified vulnerabilities in numerous systems. Some of the organization utilizes security level aspects are MITRE [28], US-CERT [29], Security Focus [30], and NIST [31]. In the US-CERT, a distinct level of vulnerability is identified by measuring the frequency of the incident [32]. The characteristics of the system, malevolent, and potentially neglectful factors are utilized in measuring the vulnerability of the system [32].The appropriate time for incorporating the security patches and the optimum uptime for the exploiting security mechanism can enhance the security features [33].

IES is a blend of software and hardware components that work together to deliver diverse services. One of the chief issues of software-based security metrics is that they just concentrate on a distinctoperating system or software package. They do not include the security aspects that are a combination of different software packages. Thus, they do not comprise the correlation amongdiverse systems. From the perspective of IESs, it is essential to examinenot only a single aspect of security, but it necessitates a combination of numerous components. Hence, the Multi-Metricsbasedapproach is necessary for handling these security aspects.

## 6.3. Quality Metric

The optimized outcome of algorithms requiresa certain amount of information and in the context of constrained resources,a trade-off will occur. The best optimal outcome with certain deviation is accepted such as lossy video, audio, and encoding of the image that lead to approximate computing. The quality of the outcome is determined by performance estimation factors namely simple analysis of criteria and criteria for analysis of data. The mean squared error (MSE), root MSE (RMSE), mean absolute error (MAE), signal-noise ratio (SNR), peak signal-to-noise ratio (PSNR), and bit error ratio (BER) falls under the simple analysis of criteria. True positive rate (TPR), false-positive rate (FPR), true negative rate (TNR), false-negative rate (FNR), precision, recall, accuracy, sensitivity, specificity, and F1 score falls under criteria for analysis of data [34-37].

### 6.3.2. Simple analysis of criteria

- MSE: It is the estimation of the square of errors and it is given as

$$MSE(p,q) = \frac{1}{N}\sum_{i=1}^{N}(p_i - q_i)^2.$$

- RMSE: It is the estimation of the closeness of the fitted points and it is given as

$$RMSE(p,q) = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(p_i - q_i)^2}$$

- MAE: It is the measure of error among the paired observation and it is calculated as,

$$MAE(p,q) = \frac{1}{n}\sum_{i=1}^{N}|p_i - q_i|$$

- SNR: It is the ratio of signal from the desired and undesired signal information. It is denoted in decibel (DB) and it is calculated as,

$$SNR(p,q) = 10 \times log\frac{power\ of\ the\ needed\ signal}{power\ of\ the\ noise\ signal}$$

$$SNR(p,q) = 20 \times log\frac{power\ of\ the\ needed\ signal}{power\ of\ the\ noise\ signal}$$

- PSNR: It is the ratio of signal from the desired and undesired signal information. It is denoted in decibel (DB) and it is calculated as,

$$PSNR(p,q) = 10log_{10}\left(\frac{p_{max}^2}{MSE(p,q)}\right)$$

$$PSNR(p,q) = 20log_{20}\left(\frac{p_{max}^2}{RMSE(p,q)}\right)$$

- BER: It is the ratio of the count of the error bits that is divided by the total count of the transmitted bits.

The n number of sample signals are denoted as $p_1,p_2,\ldots..p_n$ in the p discrete-time, and the estimated samples are $q_1,q_2,\ldots..q_n$.

### 6.3.2. Criteria for analysis of data

- True-Positive Rate: TPR is the possibility that a definite positive will test positive. It is equated as,

$$\text{TPR} = \frac{TP}{\text{TP} + \text{FN}}$$

- False-Positive Rate: FPR measures the samples of proportion that the classification incorrectly determine all instances for which actual category is negative, it is calculated by

$$\text{FPR} = \frac{\text{FP}}{\text{FP} + \text{TP}}$$

- True-Negative Rate: TNR is the possibility that a definite negative will test positive. It is equated as,

$$\mathrm{TNR} = \frac{TN}{\mathrm{TN} + \mathrm{FP}}$$

- False-Negative Rate: TNR measures the samples of proportion that the classification incorrectly determine all instances for which actual category is positive, it is calculated by

$$\mathrm{FNR} = \frac{\mathrm{FN}}{\mathrm{TP} + \mathrm{FP}}$$

- Precision: It provides a good measurement when false positive is high, and it is calculated by,

$$\mathrm{P} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}}$$

- Accuracy: The amount of corrected predictions for all input samples is referred to as accuracy. It is calculated by,

$$\mathrm{Accuracy} = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN}}$$

- Sensitivity or Recall: The sum of true positives and false negatives is used to calculate sensitivity. It's also known as a false positive or true positive. It is estimated as,

$$\mathrm{r} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}}$$

- Specificity: When the actual ailment is not present, the negative classification of assault is measured by specificity. It is calculated by,

$$\mathrm{Specificity} = \frac{\mathrm{TN}}{\mathrm{TN} + \mathrm{FP}}$$

- F-Score: The F-Score is estimated from the perfect precision and recall value. It is calculated as

$$\text{F-Score} = 2*(p*r/p+r)$$

From the assistance of these metrics privacy, security, trust, and quality of the IES are estimated and investigated.

## 7. Conclusion

An embedded system is a combination of memory, processors, software, and peripheral devices that is a whole system. This poses a dedicated function within a huge electronic or mechanical system. The necessity of automation and intelligent sensor-based objects makes the evolution in ES paved the way for intelligent embedded systems. IES is characterized by the process, service, or product to interpret the performance of the atmosphere to enrich the lifetime, quality, and satisfaction of the individual. IES facilitates the processing of gathered information from different embedded sensors. The existence of numerous devices and task-specific framework is subjected to numerous issues like integrity, security, and other functionality issues. In this article, diverse applications of IES and their challenges are detailed. The privacy or security threats in IES as well as the requirement of privacy and security features in IES are elucidated with the analysis metrics.

**Declaration:**

Ethics Approval and Consent to Participate:

No participation of humans takes place in this implementation process

Human and Animal Rights:

No violation of Human and Animal Rights is involved.

Funding: No funding is involved in this work.

Conflict of Interest: Conflict of Interest is not applicable in this work.

Authorship contributions:

There is no authorship contribution

Acknowledgment :

No acknowledge

## Reference

1. Pierdicca, R., Liciotti, D., Contigiani, M., Frontoni, E., Mancini, A., & Zingaretti, P. (2015, June). Low cost embedded system for increasing retail environment intelligence. In *2015 IEEE International Conference on Multimedia & Expo Workshops (ICMEW)* (pp. 1-6). IEEE.

2. Emilio, M. D. P. (2015). Features of Embedded System. In *Embedded Systems Design for High-Speed Data Acquisition and Control* (pp. 25-31). Springer, Cham.

3. Tseng, Y. W., Liao, C. Y., & Hung, T. H. (2015, May). An embedded system with realtime surveillance application. In *2015 International Symposium on Next-Generation Electronics (ISNE)* (pp. 1-4). IEEE.

4. Huang, Y., Guan, X., Chen, H., Liang, Y., Yuan, S., & Ohtsuki, T. (2019). Risk assessment of private information inference for motion sensor embedded iot devices. *IEEE Transactions on Emerging Topics in Computational Intelligence*, *4*(3), 265-275.

5. Kim, B., & Yang, H. (2020). Reliability Optimization of Real-Time Satellite Embedded System Under Temperature Variations. *IEEE Access*, *8*, 224549-224564.

6. Jaber, A. A. (2016). *Design of an intelligent embedded system for condition monitoring of an industrial robot*. Springer.

7. Shamrat, F. J. M., Ghosh, P., Mahmud, I., Nobel, N. I., & Sultan, M. D. (2021). An intelligent embedded AC automation model with temperature prediction and human detection. In *Emerging Technologies in Data Mining and Information Security* (pp. 769-779). Springer, Singapore.

8. Ye, L. (2020). Study on embedded system in monitoring of intelligent city pipeline network. *Computer Communications*, *153*, 451-458.

9. Marwedel, P. (2021). *Embedded system design: embedded systems foundations of cyber-physical systems, and the internet of things* (p. 433). Springer Nature.

10. Madasamy, K., Shanmuganathan, V., Kandasamy, V., Lee, M. Y., & Thangadurai, M. (2021). OSDDY: embedded system-based object surveillance detection system with small drone using deep YOLO. *EURASIP Journal on Image and Video Processing*, *2021*(1), 1-14.

11. Marwedel, P. (2021). *Embedded system design: embedded systems foundations of cyber-physical systems, and the internet of things* (p. 433). Springer Nature.

12. Wang, X., Wang, Z., Huang, W., Wen, G. Q., & Zhang, S. L. (2017). Summary of Embedded Systems Development.

13. Received From https://www.infopulse.com/blog/challenges-and-issues-of-embedded-software-development/

14. Received From https://www.mordorintelligence.com/industry-reports/embedded-security-market

15. Sharaf-Dabbagh, Y., & Saad, W. (2016, June). On the authentication of devices in the Internet of Things. In *2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)* (pp. 1-3). IEEE.

16. Diesburg, S., Meyers, C., Stanovich, M., Mitchell, M., Marshall, J., Gould, J., ... & Kuenning, G. (2012, December). Trueerase: Per-file secure deletion for the storage data path. In *Proceedings of the 28th annual computer security applications conference* (pp. 439-448).

17. Baraniuk, R. G. (2011). More is less: Signal processing and the data deluge. *Science*, *331*(6018), 717-719.

18. Langheinrich, M. (2002, September). A privacy awareness system for ubiquitous computing environments. In *international conference on Ubiquitous Computing* (pp. 237-245). Springer, Berlin, Heidelberg.

19. Langheinrich, M. (2001, September). Privacy by design—principles of privacy-aware ubiquitous systems. In *International conference on Ubiquitous Computing* (pp. 273-291). Springer, Berlin, Heidelberg.

20. Koukis, D., Antonatos, S., Antoniades, D., Markatos, E. P., & Trimintzios, P. (2006, June). A generic anonymization framework for network traffic. In *2006 IEEE International Conference on Communications* (Vol. 5, pp. 2302-2309). IEEE.

21. Shinzaki, T., Morikawa, I., Yamaoka, Y., & Sakemi, Y. (2016). IoT security for utilization of big data: Mutual authentication technology and anonymization technology for positional data. *Fujitsu Sci. Tech. J*, *52*(4), 52-60.

22. Jayaraman, P. P., Yang, X., Yavari, A., Georgakopoulos, D., & Yi, X. (2017). Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation. *Future Generation Computer Systems*, *76*, 540-549.

23. Jebril, N. A., & Al-Haija, Q. A. (2017). Review of Challenges in Embedded Systems Design: Robustness, Predictability, Security. *International Journal of Current Research in Embedded System & VLSI Technology [ISSN: 2581-5105 (online)]*, *2*(1).

24. Krumm, J. (2009). A survey of computational location privacy. *Personal and Ubiquitous Computing*, *13*(6), 391-399.

25. Shokri, R., Theodorakopoulos, G., Le Boudec, J. Y., & Hubaux, J. P. (2011, May). Quantifying location privacy. In *2011 IEEE symposium on security and privacy* (pp. 247-262). IEEE.

26. Ma, Z., Kargl, F., & Weber, M. (2009, March). A location privacy metric for v2x communication systems. In *2009 IEEE Sarnoff Symposium* (pp. 1-6). IEEE.

27. Szefer, J., Keller, E., Lee, R. B., & Rexford, J. (2011, October). Eliminating the hypervisor attack surface for a more secure cloud. In *Proceedings of the 18th ACM conference on Computer and communications security* (pp. 401-412).

28. Public Interest, Inc. (2014). Debian. Retrieved October 15, 2014 http://www.debian.org

29. Red Hat, Inc. (2014). Redhat. Retrieved October 15, 2014 http://www.redhat.com

30. Manadhata, P. K., & Wing, J. M. (2010). An attack surface metric. *IEEE Transactions on Software Engineering*, *37*(3), 371-386.

31. Garitano, I., Fayyad, S., & Noll, J. (2015). Multi-metrics approach for security, privacy and dependability in embedded systems. *Wireless Personal Communications*, *81*(4), 1359-1376.

32. Manadhata, P., Wing, J., Flynn, M., & McQueen, M. (2006, October). Measuring the attack surfaces of two FTP daemons. In *Proceedings of the 2nd ACM workshop on Quality of protection* (pp. 3-10).

33. Kurmus, A., Tartler, R., Dorneanu, D., Heinloth, B., Rothberg, V., Ruprecht, A., ... & Kapitza, R. (2013, February). Attack Surface Metrics and Automated Compile-Time OS Kernel Tailoring. In *NDSS*.

34. Mittal, S. (2016). A survey of techniques for approximate computing. *ACM Computing Surveys (CSUR)*, *48*(4), 1-33.

35. Kumar, R., Farkas, K. I., Jouppi, N. P., Ranganathan, P., & Tullsen, D. M. (2003, December). Single-ISA heterogeneous multi-core architectures: The potential for processor power reduction. In *Proceedings. 36th Annual IEEE/ACM International Symposium on Microarchitecture, 2003. MICRO-36.* (pp. 81-92). IEEE.

36. Verma, M., Petzold, K., Wehmeyer, L., Falk, H., & Marwedel, P. (2005, September). Scratchpad sharing strategies for multiprocess embedded systems: A first approach. In *3rd Workshop on Embedded Systems for Real-Time Multimedia, 2005.* (pp. 115-120). IEEE.

37. Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment: from error visibility to structural similarity. *IEEE transactions on image processing*, *13*(4), 600-612.

38. Sathishkumar Karupusamy; Ramalingam, M., Eswaran, Boopathi Kumar and Thiagarasu, V. (2021). “Guest Editorial: Big Data Analytics and Management in Internet of Things”. Journal of Information Technology Management, Special Issue, 1-5.

39. M. Ramalingam, K. Sathishkumar [2020], "Design And Development of Cluster Based Stretch And Shrink Scheme For Topology Stability And Load Balancing In Mobile Ad Hoc Network Using Weighted Clustering Algorithm", International Journal of Scientific & Technology Research Volume 9, Issue 01, pp. 574-578, ISSN 2277-8616.

40. Sathishkumar , Dr.V.Thiagarasu, Dr.E.Balamurugan, Dr.M.Ramalingam, [2018], "An Competent Artificial Bee Colony (ABC) and Fuzzy C Means Clustering Using Neuro-Fuzzy Discriminant Analysis from Gene Expression Data", International Journal of Science & Engineering Development Research, ISSN:2455-2631, Vol. 3, No. 4, pp. 24 - 28, April.

41. Sathishkumar Karupusamy [2019], “Standard Weight and Distribution Function Using Glowworm Swarm Optimization for Gene Expression Data”, International Conference on Sustainable Communication Network and Application [ICSCN 2019] (Springer LNDECT), held at Surya Engineering College, Tamil Nadu, India during 30-31 July 2019. Vol. 39, pp. 604-618.

42. Sathishkumar Karupusamy [2019], “Gene Expression Analysis Using Clustering Methods: Comparison Analysis”, International Conference on Sustainable Communication Network and Application [ICSCN 2019] (Springer LNDECT), held at Surya Engineering College, Tamil Nadu, India during 30-31 July 2019. Vol. 39, pp. 633-644.