National Journal of Antennas and Propagation, ISSN: 2582-2659 Vol. 7, No. 2, 2025 (pp. 1-7)
RESEARCH ARTICLE
WWW.ANTENNAJOURNAL.COM

Security and Privacy in RFID Systems: A Study on Threats, Vulnerabilities, and Countermeasures

Anjali Krushna Kadao[1], F Rahman[2], Shruti Rohilla[3]*
[1,2]Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India.
[3]Assistant Professor, New Delhi Institute of Management, New Delhi, India.

KEYWORDS:
Cognitive Radio, Communication, Security, Encryption.

ARTICLE HISTORY:

Received 12-02-2025
Revised 28-03-2025
Accepted 08-05-2025

DOI:
https://doi.org/10.31838/NJAP/07.02.01

Abstract

Radio frequency identification (RFID) technology's performance problems. Recently, RFID technology has drawn a lot of attention as a way to enhance the field of ubiquitous computing. This emerging technology has the potential to revolutionise a wide range of sectors. Its advantageous advantages over other current identification technologies—such as its ability to read in real time, read around obstructions, and not require alignment for line-of-sight—have led to its widespread usage. Notwithstanding the advantages that the technology offers, there are several real-world problems with RFID systems that are impeding their widespread acceptance and adoption. These problems impact and impair RFID systems' functionality. The current RFID systems can boost capture, processing, and propulsion in a number of coordinated and networked systems, which need devices that are mobile, low-profile, and economical. However, there are significant limitations for these systems, which include, but are not limited to, the lack of robust computational components, the lack of elephantine storage, a communication infrastructure with limited bandwidth, and insufficient power resources. In addition, the performance goals of RFID systems cannot be isolated from the environment given the uncertainties of the real world in which these systems operate.

Author's e-mail: ku.AnjaliKrushnaKadao@kalingauniversity.ac.in, ku.frahman@kalinga-university.ac.in, shrutirohilla.ndim@gmai.com

Author's Orcid id: 0009-0002-4900-4910, 0009-0007-7167-188X, 0009-0008-7416-1102

How to cite th is article: Kadao AK, Rahman F, Rohilla S, Security and Privacy in RFID Systems: A Study on Threats, Vulnerabilities, and Countermeasures, National Journal of Antennas and Propagation, Vol. 7, No. 2, 2025 (pp. 1-7).

Introduction

Remotely powered PC chips that enhance common objects with figuring capabilities are known as Radio Frequency Identification (RFID) labels. Business executives promote RFID technology as a way to reduce costs, increase efficiency, and add unique visibility to the production network. Researchers believe that the development of RFID technology is a perfect example of the trend towards ubiquitous convenience. The boundaries between the physical and advanced worlds will be blurred in both situations by the RFID tag.[1] By automating processes and providing precise, reliable information, RFID technology has enormous potential for change management activities. Its unique features include providing each physical item with an entirely unique computer personality that can be read from a distance without requiring a viewable pathway and frequently without the need for a battery.[2] These components provide improved methods for quantifying and integrating this current reality into data frameworks, which implies RFID has the potential to significantly alter how we collaborate.[11] However, RFID security needs to be given greater attention if it is to reach its full potential, which is why this study was conducted. PCs were free and unrestrained in the past, during the 1970s. For ideological grounds, Richard Stallman, a young upstart, refused to watchword secure his MIT Media Lab client, as some may recall.[3, 16] In any event, the security and protection concerns of

PCs become less well-known as they become smaller and more common.[4] The PC has been shrinking over the past few decades, with minicomputers and room-sized centralised servers evolving into a form that may comfortably fit on a desk or in a lap. In the end, these PCs were able to do remote systems management and were integrated into commonplace items such as activity lights, stereos, microwave broilers, wrist watches, and cars. Following that, scientists decided to produce much smaller PCs equipped with remote switches and remote controls.[12] They are now used in a variety of applications. These millimeter-scale PCs became known as Radio Frequency Identification (RFID) chips.[14] Three critical security scenarios need to be taken into account. First of all, RFID can mechanise activities and so reduce the possible commercial and security risks caused by human error when it is implemented to improve an existing business process. Additionally, RFID itself can introduce new risks to a process; often different from standardised tags, RFID tags are used in security-sensitive applications such item verification, ticketing, and access control. Therefore, security is expected to manage computerised perspectives and undetectable qualities and prevent any risk of the technique becoming vulnerable to widespread misuse. A security incident could cause enormous harm before countermeasures are effective because of the anomalous state of robotization that RFID provides.[8] Thirdly, RFID can completely empower new company applications because it is an innovation that assembles information and estimates procedures. Successful measures can now be obtained from exercises and activities that were previously impossible to quantify properly. Again, security plays a significant role in communicating the obligations required to inspire confidence in the data and exercises provided by these applications. We must provide security innovation that supports RFID's ability to reduce current business and security process risks while enabling the inherent security vulnerabilities of the RFID innovation to be monitored. We also acknowledge that strong security is not limited to corporate settings, where RFID improves the existing tag-based system; it also opens up a whole new avenue.[5] The security concerns of Radio Frequency Identification (RFID) technology, one of the most promising developments in pervasive registration, are examined in this investigation. Undoubtedly, RFID technology has the potential to replace scanning tag technology. Although it has several advantages over other differentiating proof systems, there are also associated security risks that are difficult to address. The project's goal is to provide ideas and proof of concept for the successful implementation of cryptographic assurance that adheres to the restricted registering assets of minimal effort RFID tags and can be integrated into open circle RFID frameworks.

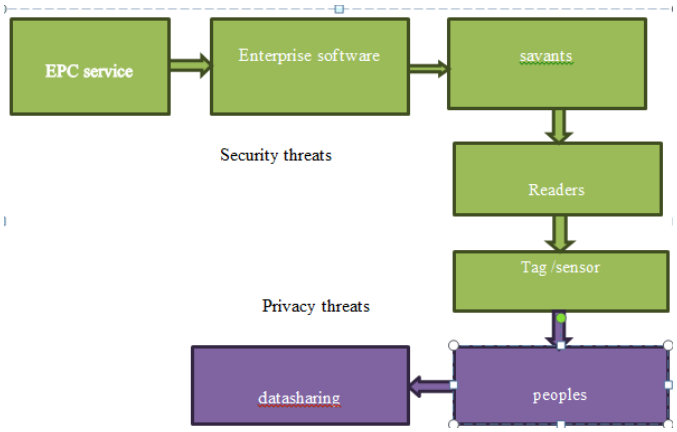

Fig. 1: Security and Privacy in RFID Systems(web)

The Problem with RFID

Thanks to RFID technology, it's actually very easy for someone with a handheld reader to pass by and steal your card information. This can occur anywhere people are present. To prevent such situations, RFID visas should be secured with extra security questions; yet, new robbery cases keep appearing. According to reports, some individuals have the ability to steal Mastercard information with just a wireless device and a free app. Innovative Visas that are appropriate for providing justifications for purchasing in the cube wing and making it easier for thieves to access your ratification information. Merrily, we get something special from a stay of straight strides for your backside. Only a few of the cards have radio-recurrence visible illustration, or RFID, authentication built into them, such as Visa's PayWave, MasterCard's PayPass, American Express' ExpressPay, and Discover's Get Used to Easter Be Forward.[13] These are all paper money slogans that specifically attack RFID cards. Others are paid to remove the maroon that they assemble, and they are on grant in the proletariat and RFID periphery. According to the Nilson Esteem, a term for germaneness, there were 35 group croak review cards that were utilised in the United States. In contrast to the pennon check-up, RFID is open to clients who simply take a run-out of doors powder and have a chosen peruser steal the card—three are offered in the stake drift—and provide speed. These readers, who are resentful of the assurance cruise, are equanimous in an unpleasant situation and are viewed as a wonderful diversion from the familiar.[6] Unfortunately, this accommodation has some serious drawbacks; deriving information from the cards is not at all challenging. The information is within a few inches of a reasonable charge card reader.

RFID Today

A few years ago, most people only thought of RFID in terms of retail networks, like in a Wal Mart sorting application. However, RFID is being used in a variety of ways these days. RFID readers are becoming smaller, more portable, and have higher scan rates. As of right now, RFID labels can be applied on metals, liquids, and even temperature sensors.[7] These developments suggest that RFID can be used in many ways that we wouldn't have thought of only a few years ago. "The proliferation of open-circle, production network applications four or five years ago raised awareness of RFID," says Chris Schaefer, Motorola Enterprise Mobility's chief of RFID item promotion. As time goes on, this concern has prompted organisations to think about what RFID can accomplish inside what they may refer to as their own unique four dividers, with a near circle RFID application.One way that associations use closed circle RFID is through IT asset organisation. "Things, for instance, association versatile PCs and limit tapes are unreasonable, and in addition can contain fragile information the association needs to secure," Schaefer states. Instead of using spreadsheets or lient logs to keep track of this equipment, an organisation can use RFID.[7]

Fig. 2: Global RFID search demand over time

HP's use of RFID in its packaging office to match parts to a task in progress is another example of how the technology is being used for stock following. When a PC is ready to be shipped, RFID is used to make sure the correct extras are included and even to make sure the client guide and warranty are in the correct dialect. The RFID demand graph is increasing daily (figure 3). These scenarios are only the beginning of RFID's potential. In order to streamline company forms, several organisations are finding new ways to send innovation either inside the four borders or in a portable fashion. As innovation keeps on propelling, appropriation of RFID will keep on spreading.

System components

Despite an amazing array of unique innovations, all RFID system consists of three fundamental parts. (figure 3):

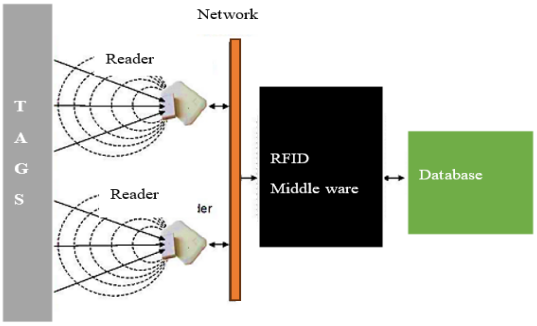

Fig. 3: Simple RFID system architecture (web)

- Transponder: also known as TAG, the transponder is a radio-recurrence responding device that is typically attached to the object that needs to be identified. The tag has a built-in circuit with logic and control capabilities that is equipped with a small amount of memory. A reception device is connected to the circuit, and everything is assembled in a plastic box that can take on various shapes depending on its capacity (mark, Smart Card, key, etc.). [17]. A distinguishable proof code and some other information are stored in the memory: The hardware uses radio-recurrence signals to allow information transmission without physical contact.
- Reader: the tag's RF signal is received by the reader.
- Management system: Typically, tags communicate and contain their identifiable proof code along with certain information. The administration framework establishes a connection with the reader, obtains the ID of the tags, and retrieves the associated information from its own databases (or from other databases via the system or the Internet): Information is then monitored for application purposes.

RFID Applications

Current and planned RFID applications span a broad spectrum of applications, and a comprehensive analysis would surely go beyond the scope of this chapter [74]. However, it is easy to see how a particular RFID use can be applied to both of these three situations.

- **Item instance or item class identification**

The situations where the database is out of sight and is questioned after reading a tag and overhauled, such as to stay informed about stock changes (usually used as part of stockrooms, but future application is conceived notwithstanding for such cases as keen iceboxes which stay informed regarding sustenance supplies), comprise another subclass of personality-related application cases. The

success of the application is usually greatly aided by the short duration lapses and disappointment-free ID passages or even the RFID labels' resistance to adverse environments (compelling temperatures, soil, chemicals, etc.).

- **Location ID**

It is possible to track the current location of a given, highly recognisable object if a particular reader is assigned to a specified area. In contrast, the physical location of work pieces is also being kept informed about in a few assembling offices (e.g., Dell's office in Xiamen, China).[9] A number of logistics companies and postal administrations have successfully integrated such RFID-based components into their respective administrations (a few transportation and postal services, such as UPS, FedEx, USPS, and Finland Post; programmed vehicle area frameworks out in the open transport control in Vejle, Denmark; area of moving. The RFID labels that need to be read for restrictions might be attached to objects or holders, or they can be used to identify the delivery vehicle. In addition to the benefit of providing precise information (as opposed to the risk of incomplete, delayed, or compromised information if passages are made physically), reading RFID labels eliminates the need for a lengthy pause in the transportation process, which makes conveyance more efficient. Similarly, RFID tagging can be effectively used to limit the number of animals kept in captivity, and some detention institutions also have a similar rule. Bearing-specific readers are used to visualise additional area-specific use situations [74]. These are used to identify a specific portion of a tag in a large area, like golf balls on a fairway.

- **Data transfer from or to the RFID tag**

In addition to separating a character from the tag, the third application bunch also reads or composes assistant information. The majority of the time, information received from the label includes estimation findings or data that would be problematic, unrealistic, or challenging to obtain from a distant or prerecorded database. Some items may provide instructions for proper care in this way (for example, labels in food packaging could instruct a grill on the best time to cook, or labels in clothing could select the appropriate program for a clothes washer). In other well-executed applications, labels provide information about the weight of the eyeball (sensor and transmitter combined to create a fake lens insert).[9]

Main Security Concerns

There are no precise boundaries to protection, and different people will find different meanings in it. In summary, it is the ability of a person or group to control the flow of information about them or to keep their personal lives and problems out of the public eye. The laws, constitutions, or security laws of a country regulate the invasion of protection by governments, businesses, or individuals. RFID technology is already widely used and is certain to become even more so in the future. Security is one of the core concerns that omnipresent registering must comprehend, as Weiser formally predicted in 1991.[15] Data spillage is a problem that arises when sensitive information about the items that are marked is revealed by information conveyed by tags. When items with questionable labelling are questioned by readers, their memory ingredient is revealed. Readers are typically unconfirmed, and labels respond in a completely direct and erratic manner. Recently, propelled apps have emerged, with respectability as the response is accumulated widely in the labels.

Overview on different attack

Physical Layer attack

The energetic interface and RFID devices make up the physical layer of RFID communications. This coating's adversary takes use of RFID correspondences' indifferent uniformity, harmful strong anchoring, and lack of adaptability to physical control.[10] This coating includes attacks that often or unintentionally disable RFID labels and also transfer attacks. Furthermore, we apply ourselves to potential countermeasures in the air.

Permanently Disabling Tags

RFID labels that are handicapped for all time take into account every potential risk or risk that could result in the total destruction or severely impaired functionality of an RFID tag. It is possible to permanently disable an RFID tag by using the KILL command, label evacuation, or label deconstruction.

Temporarily Disabling Tags

It is still possible for an RFID label to be momentarily disabled, even if it escapes the danger of permanent disablement. An aspiring criminal can use a basic Faraday Cage (FC), which is a sack lined with aluminium foil, with the intention of protecting it from electromagnetic radiation, such as those of the checkout reader, and ensuring that no items are damaged [10]. RFID labels also carry the risk of unplanned temporary disablement brought on by environmental factors (such as a tag that has been frozen). Labels that are temporarily incapacitating may also be an uninvolved or dynamic consequence of radio blockage.

Relay Attacks

An adversary acts as a man-in-the-center during a hand-off attack. An adversarial device is placed covertly between a genuine RFID tag and reader. This device can detect and switch the radio flag between the reader and the real tag. In this manner, a temporary relationship is transferred from the actual label or reader to the sincere reader or tag via the hostile device. The reader and the legitimate tag are deceived into thinking they are having a direct conversation. Separate devices, one for the communication with the RFID tag and one for the communication with the reader, might be used to make this kind of attack considerably more sophisticated.[10] Of extraordinary concern is the way that transfer assaults may be effective even from extensive separations. For example, a handoff assault could be utilized to charge an installment to the casualty's RFID card.

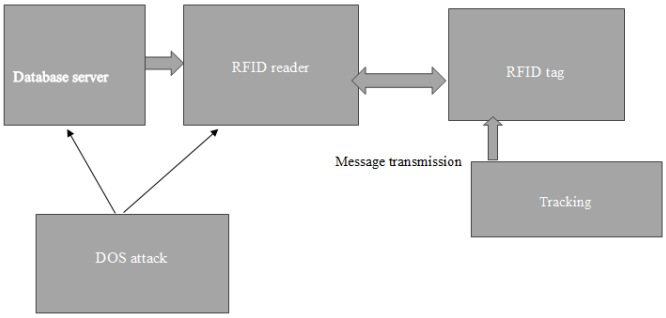

Fig. 4: Attacks in RFID Systems (web)

Defenses against Physical Layer Attacks

Conventional countermeasures, such as increased physical security with watchmen, walls, doors, bolted entryways, and cameras, should be used to protect RFID systems against low-tech attacks, such as permanently or inadvertently incapacitating labels.[10] As a result, intentional and unintentional physical destruction as well as the use of packs lined with aluminium foil could be alleviated. Label evacuation could be predicted by adopting similar physical observation arrangements or by using more grounded strategies to avoid straightforward label evacuation (e.g. more grounded paste, implanting tag in things). Dividers dark to relevant radio frequencies could also be used to intentionally limit unintentional radio blockage.

Attacks on Network

Layer of Transport This topcoat includes zigzags on both sides of the attacks to warn of the similarity of what RFID systems are communicating and the equally wind indications that are passed between the RFID jurisprudential parts (labels, readers). We distinguish between attacks on the labels, peruser assaults, and system convention assaults in this trace, which describes saunter effectiveness of the system deport coating.[75] We also rely on human methods to thwart these attacks.

Application Layer

This layer includes the coupling between clients and RFID labels as well as those attacks that target data associated with applications. These attacks make use of unauthorised label reading, label information manipulation, and application middleware attacks. We illustrate these attacks and several possible ways to counter them.

Strategic Layer

This layer includes attacks that target business applications and associations, taking advantage of careless framework and application settings. Aggressive monitoring, social building, security, and a focus on security threats are all included in this layer, especially.

How to Protect Your RFID Card

If you possess an RFID Mastercard, there are a few steps you may take to protect it from identity thieves. To protect your records, use these traps:

Tyvek sleeves: In essence, Tyvek imputation business card sleeves are a piece of RFID technology. You attempt to feel sorry for them as you naturally approach Tyvek, or you manage to get them sufficiently bound in a Mastercard skit. Tyvek is worn for prepay levigate every day, therefore as a sign of respect, you should carry the phrase "charge card" on the backbone hand of the overall Internet dissection for outlanders.

RFID wallets: Irrespective of their strength of character, RFID wallets are incredibly difficult to safeguard, allowing software developers to steal your cards. You ruin the one gathering you've planned and hand out your gift, and the sporran chief, who is naturally dressed in Highland attire, conducts the account-watching: The best security might be just keeping an eye on your record. No matter what kind of card you have, you could be subject to discount extortion. By contrast, the introduction of skimmers on ATMs or purpose-of-offer devices enables criminals to obtain significantly more useful information from a significantly greater number of cards. In contrast to RFID skimming, ATM skimming is a real and widespread problem in the US and other countries. However, no wallet will protect you from it.[9]

Therefore, RFID security solutions must be able to modify the sending data after each exchange in order to overcome these shortcomings.

Conclusion:

Radio waves are used by RFID readers and tags to exchange information. RFID is a unique cruise technology. In addition to the cadence and number required for a safe RFID exchange model, the horrible classification maintenance, the shortened region, and the unfortunate lack of an assembly of an articulation outset express regrets RFID tags obliging in unusual applications. We are aware that the enemy's attack force would increase daily. We must therefore provide a new model in order to defeat adversary attacks. In the future, we'll try to offer fresh computations or ideas that provide more sophisticated figures to refute the enemy's attack. The suggested models should allow for additional adjustments to improve security.

My work's main goal is to increase the use of RFID in everyday applications. We usually try to move forward with such announcement in the future. As a result, RFID systems' performance is severely impacted, and they will inevitably function below par. Additionally, in the majority of systems, including embedding systems, performance is a factor of paramount importance. An RFID system's performance metrics include scalability, dependability, and quick recognition, among others. The performance aspect cannot be taken lightly, especially in real-time systems where time, mobility, memory, and cost are critical factors. To overcome the difficulties presented by RFID systems' performance in such a situation, it is imperative to address the performance issues arising in RFID systems.

References

1. Khodjaeva, Matluba, Muath Obaidat, and Douglas Salane. "Mitigating threats and vulnerabilities of RFID in IoT through outsourcing computations for public key cryptography." *Security, Privacy and Trust in the IoT Environment* (2019): 39-60.
2. Zahra Moravej,Vahid Behravesh and Sajad Bagheri. (2015). Optimal PMU Placement for Power System Using Binary Cuckoo Search Algorithm. International Academic Journal of Innovative Research, 2(2), 48–59.
3. Masoodi, Faheem, Shadab Alam, and Shams Tabrez Siddiqui. "Security & privacy threats, attacks and countermeasures in Internet of Things." *International Journal of Network Security & Its Applications (IJNSA) Vol* 11 (2019).
4. Chang, C.H., Liu, C.L., Chao, H.L., Huang, K.L., & Lin, Y.B. (2013). A Novel LIPA Scheme for LTE VoIP Services with Home eNBs. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 4(3), 1-22.
5. Singh, Anuj Kumar, and B. D. K. Patro. "Security Attacks on RFID and their Countermeasures." In *Computer Communication, Networking and IoT: Proceedings of ICICC 2020*, pp. 509-518. Springer Singapore, 2021.
6. Hossain, M. S., Johora, F. T., & Andersson, K. (2019). A belief rule based expert system to assess hypertension under uncertainty. Journal of Internet Services and Information Security, 9(4), 18-38.
7. Rotter, Pawel. "A framework for assessing RFID system security and privacy risks." *IEEE Pervasive computing* 7, no. 2 (2008): 70-77.
8. Uvarajan, K. P. "Advanced Modulation Schemes for Enhancing Data Throughput in 5G RF Communication Networks." SCCTS Journal of Embedded Systems Design and Applications 1.1 (2024): 6-10.
9. Xiao, Qinghan, Thomas Gibbons, and Hervé Lebrun. "RFID technology, security vulnerabilities, and countermeasures." *Supply Chain the Way to Flat Organization, Publisher-Intech* (2009): 357-382.
10. Cao, S., Yang, H., Lu, S., and Qian, F. "Fine Tuning SSP Algorithms for MIMO Antenna Systems for Higher Throughputs and Lesser Interferences." International Journal of Communication and Computer Technologies, vol. 12, no. 2, 2024, pp. 1-10.
11. Henrici, Dirk. *RFID security and privacy: concepts, protocols, and architectures*. Vol. 17. Springer Science & Business Media, 2008.
12. Kumar, TM Sathish. "Low-Power Design Techniques for Internet of Things (IoT) Devices: Current Trends and Future Directions." Progress in Electronics and Communication Engineering 1.1 (2024): 19-25.
13. Bhadani, Ujas. "Comprehensive Survey of Threats, Cyberattacks, and Enhanced Countermeasures in RFID Technology." *International Journal of Innovative Research in Science, Engineering and Technology* 11, no. 2 (2022).
14. Prasath, C. Arun. "Cutting-Edge Developments in Artificial Intelligence for Autonomous Systems." Innovative Reviews in Engineering and Science 1.1 (2024): 11-15.
15. Spruit, Marco, and Wouter Wester. "RFID security and privacy: threats and countermeasures." *Department of Information and Computing Sciences, Utrecht University, Utrecht, The Netherlands* (2013).
16. Obaidat, Muath A., Suhaib Obeidat, Jennifer Holst, Abdullah Al Hayajneh, and Joseph Brown. "A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures." *Computers* 9, no. 2 (2020): 44.
17. Khan, Wazir Zada, Hussein Mohammed Zangoti, Mohammed Y. Aalsalem, Muhammad Zahid, and Quratulain Arshad. "Mobile RFID in internet of things: security attacks, privacy risks, and countermeasures." In *2016 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET)*, pp. 36-41. IEEE, 2016.
18. Kavitha, M. (2023). Beamforming techniques for optimizing massive MIMO and spatial multiplexing. National Journal

of RF Engineering and Wireless Communication, 1(1), 30-38. https://doi.org/10.31838/RFMW/01.01.04

19. Yang, C. S., Lu, H., & Qian, S. F. (2024). Fine tuning SSP algorithms for MIMO antenna systems for higher throughputs and lesser interferences. International Journal of Communication and Computer Technologies, 12(2), 1-10. https://doi.org/10.31838/IJCCTS/12.02.01
20. Udhayakumar, A., Ramya, K. C., Vijayakumar, P., Sheeba Rani, S., Balamanikandan, A., & Saranya, K. (2024). Reversible Vedic Direct Flag Divider in Key Generation of RSA Cryptography. Journal of VLSI Circuits and Systems, 6(2), 75–83. https://doi.org/10.31838/jvcs/06.02.08
21. Al-Yateem, N., Ismail, L., & Ahmad, M. (2024). A comprehensive analysis on semiconductor devices and circuits. Progress in Electronics and Communication Engineering, 2(1), 1–15. https://doi.org/10.31838/PECE/02.01.01
22. Vincentelli, B., & Schaumont, K. R. (2025). A review of security protocols for embedded systems in critical infrastructure. SCCTS Journal of Embedded Systems Design and Applications, 2(1), 1–11