IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 4, April 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| A Monthly Peer Reviewed & Referred Journal |

||Volume 10, Issue 4, April 2021||

|DOI:10.15680/IJIRSET.2021.1004172|

A Detailed Survey of Radio Frequency Identification (RFID) Technology: Current Trends and Future Directions

Ujas Bhadani

Cybersecurity Expert, Gujarat Technological University, Ahmedabad, India

ABSTRACT: A radio frequency identification (RFID) system is a unique type of sensor network that uses radio frequency transmission to identify an object or a person. RFID tags may also communicate measurable environmental variables like temperature and relative humidity and other data like product and manufacturer specifics. Transponders (tags) and interrogators (readers) are two components of a standard RFID system. Tags are affixed to items or people, and readers use radio signals to communicate with tags within the readers' range. This research attempts to examine how RFID functions, various uses of RFID in various sectors, potential attacks and threats, and their defences and advancements. The goal of this study is to analyse some current developments in this area as well as discussion about upcoming work and research

KEYWORDS: RFID Tags, Security, Applications, Threats

I. INTRODUCTION

RFID (Radio Frequency Identification) is a wireless communication technique used to collect data that may be connected to various identification qualities of things carrying RFID labels (serial number, location, colour, date of purchase). RFID tags and RFID interrogators(readers) exchange electromagnetic waves as part of the data collecting process. When compared to other auto-detection technology, like barcodes, RFID offers more labelling specifically. For instance, RFID enables the assignment of several identification numbers for comparable objects as well as various levels of identification, improving visibility and traceability in logistical and manufacturing processes [1]. As the use of RFID systems increases, challenges to deploy, manage and control these devices also increase. Keeping an eye on the condition of RFID readers and ensuring that they are all configured uniformly is also a challenge. A big amount of data is also generated by a large number of RFID readers. The RFID reader data must be filtered and aggregated due to the existence of redundant and undesirable data. Most importantly, for data collection via RFID to be valuable in the first place, it needs to be interpreted in an application context [2]

II. HISTORY OF RFID

The research on RFID technology started during the second world war. Other RFID-related technologies include long-range transponder systems and IFF (Identification Friend or Foe) systems for airplanes. However, it took technology 30 years to catch up with the theory, as seen by the advancement of the integrated circuit, the microprocessor, and new business methods. During the 1950s and 1960s, researchers and inventors developed some prototype systems. A few theft-prevention tools were created. These devices, which were utilized in retail businesses and affixed to expensive goods and clothes, utilized 1-bit tags to detect the presence or absence of tags. This is likely the earliest and most prevalent commercial usage of RFID and has proven to be a successful anti-theft technique. RFID uses expanded into a variety of fields throughout the 1980s. Animal tracking systems became widely used in Europe, and RFID-equipped toll roads were installed in Italy, France, Spain, Portugal, and Norway. The widespread adoption of electronic toll collection in the United States during the 1990s was significant. There is now a lot of effort being done into standardization, the launch of several commercial applications, and the rationalization of frequency spectrum allotment across nations [3].

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| A Monthly Peer Reviewed & Referred Journal |

||Volume 10, Issue 4, April 2021||

|DOI:10.15680/IJIRSET.2021.1004172|

III. WORKING OF RFID

To set up an RFID system, three main components are required as shown in Fig. 1

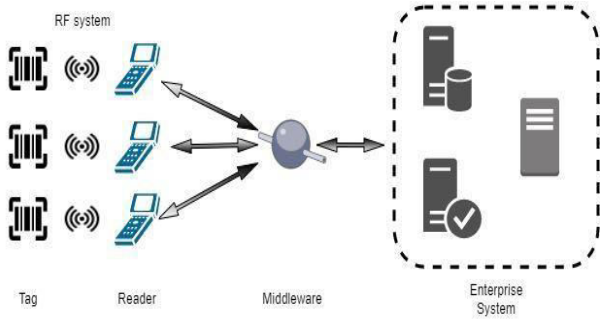

Fig. 1. Working of RFID

- *The tag*: the tag is the memory and antenna equipped chip that will be injected or adhered to an object (things, animals, etc.). Each tag contains a unique identification number that will be used to specifically identify the item it is attached to.
- *The reader*: The reader collects data from tags, filters it, and sends it to the processing unit.
- *The server/host*: The host is the processing component of an RFID system. The host is a computer that runs the corporate application as well as middleware, which is a program that acts as an interface between the application layer and the RFID RF (Radio Frequency) system, which is largely comprised of the reader. The host might be as simple as a single processor or as complex as an entire business system comprised of servers (web, databases, etc.). Future energy supply and consumption via smart grids will require more mobility, security, safety, and flexibility. These goals need a fundamental rethinking of the way power networks are organized and controlled, how cyber systems support grid operations, and how consumers engage with energy systems.

IV. CLASSIFICATION OF RFID

The RFID systems can be classified based on two criteria: Operating frequency of the system and power source of the tags.

A. Frequency allocation of the RFID

In RFID, frequency plays a significant role. From one band to the next, the electromagnetic wave's properties vary. Therefore, depending on the operation frequency, RFID systems may react differently. Applications of RFID technology is directly tied to the carrier selection depicted in Fig. 2

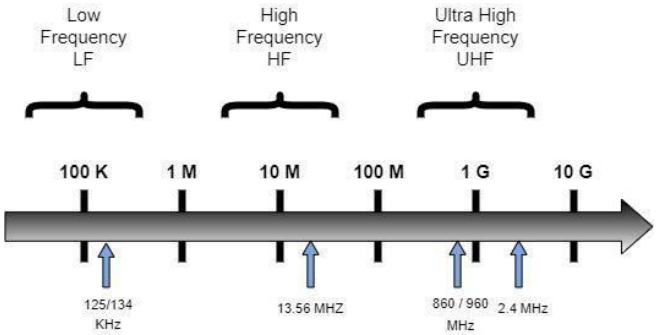

Fig. 2. Frequency allocation of the RFID

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| A Monthly Peer Reviewed & Referred Journal |

||Volume 10, Issue 4, April 2021||

|DOI:10.15680/IJIRSET.2021.1004172|

- *Low-Frequency RFID*: 125 kHz and 134.2 kHz are the most popular carriers utilized by low-frequency RFID systems. The fact that the signal is less influenced by metal is one of the primary properties of this RFID technology. The read range ranges from a few centimetres to roughly 2m and is mostly determined by the antenna of the tag. The data transmission rate is rather poor (about 70ms for read command). This inhibits the ability to scan many transponders at the same time.
- *High-frequency RFID*: RFID Passive HF (High Frequency) runs at an agreed global frequency of 13.56 MHz This means that an HF RFID system will be able to work everywhere in the world. However, some signal parameters, primarily power and bandwidth, are normalized by location. For instance, Industry Canada and the FCC in North America set a 3-Watt restriction on the reader's antenna power, but 4 Watts is the limit in Europe. When compared to LF, HF offers reduced expenses, the ability to read several labels at once, and faster transmission.
- *Ultra-High-frequency RFID*: The frequencies between 300 MHz and 3 GHz are included in UHF. 433 MHz, 2.45 GHz, and mainly the frequency 860 - 956 MHz are used for RFID UHF. Its use is more recent than those of HF and LF. Additionally, it utilizes a smaller antenna for long-distance transmission at higher speeds. Backscattering, an alternative to induction, is the method used by the UHF tag to deliver a signal after modifying the incoming signal from the reader.

The following table outlines a comparison between the LF, HF, and UHF.

TYPE	LF	HF	UHF
Range	Few centimetres	50 cm	6 m
Advantages	Non affected by water Non affected by metals Frequency use without restriction	Non affected by water - non affected by metals multiple tags read - non affected by electrical noise	Long range Standard High rate Easy to the product with low cost (5 cents)
Drawbacks	Expansive Noise Low rate (70 ms to read a tag)	Range < LF Less efficient than LF (water and metals)	Absorbed by water Reflected by metals Limited memory - interference with many applications
Applications	Animal tracking Identification	Credit card, access control card, passports	Industry Retail chain

Table. 1. Comparison LF, HF, and UHF

B. Tag power source classification

- *Passive RFID*: In passive RFID systems, the tag powers its integrated circuit and transmits the answer using the electromagnetic signal from the reader. This limited energy severely constrained both the integrated circuit's

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| A Monthly Peer Reviewed & Referred Journal |

||Volume 10, Issue 4, April 2021||

|DOI:10.15680/IJIRSET.2021.1004172|

processing power and the reading distance between the reader and tags. These tags typically cost between five cents and one dollar, making them more affordable.

- *Active RFID*: The battery-powered active tag's internal circuitry and signal response are both powered by the battery. Depending on the frequency employed, the transmission distance can rise and reach a few hundred meters. Its computation capacity is significantly more than that of passive tags. This kind of tag may be used in conjunction with a sensor and occasionally includes sophisticated functions that drive up the price of the tag to one hundred dollars per unit.
- *Semi-Active RFID*: The transmission module is still passive in this system since it is based on a semiactive tag that requires a battery to power the integrated circuit to perform processing (i.e., it draws energy from the reader signal for its power transmission module). The time required to transition from a dormant to an active state, however, is unsatisfactory and occasionally includes paying a penalty for waiting. Sensors and this kind of tag are frequently used together. It has improved over passive tags and is less expensive than active tags [4].

V. APPLICATION OF RFID

The capacity to identify things without a direct line of sight between the tag and reader, read/write functionality, security, programmability, and cluster reading are the three major characteristics of radio frequency tagging [6].

- *Recognition Without Direct Eye Contact*: Even if anything is in the way of the reader and the tag, it is still possible to identify people, things, and boxes.
- *Read & Write*: Certain RFID tags, as opposed to barcode identification technology, may retain data, enabling system designers to apply "handling codes" directly to the object as it moves through the system.
- *Group Reading*: Automated accounting processes can process more tags per second thanks to specially built readers.
- *Security*: Because tags are enclosed, they are far more difficult to manipulate. A lot of tag varieties now additionally include a serial identification number that is encoded into them and is guaranteed to be unique globally [7].
- *Programmability*: Rather than being read-only, many tags are read/write capable. This implies that information can be added to the tag, possibly to demonstrate that the object being identified has undergone a certain procedure or that its state or status has changed in some way. Or, in certain cases, to keep details on the tagged goods, such as the outcomes of any tests they have undergone [7].

These characteristics define how RFID technology is applied in every sector of business, industry, and service where data collection is required. The main application areas are as follows

A. Transportation and Distribution

The demanding railway environment is ideally suited for the usage of RFID technology. Field-programmable tags allow each vehicle to be uniquely identified by its kind, owner, and serial number using the industry standard of 12 characters. Tags are attached to the undercarriage of the vehicle; antennae are positioned between or near the tracks, and readers or display devices are usually situated 40 to 100 feet away in a roadside hut along with additional control and communications gear. Improved fleet utilization, which enables fleet size reductions and/or the postponement of investment in new equipment, is a key goal in rail applications.

RFID technologies are being used by commercial truckers to track entry into and exit from terminal buildings. From a terminal port in Hong Kong to a port in Japan, the first pilot test phase showed how RFID may be used in logistics and transportation [8]. The same systems can be used in conjunction with weigh-in-motion scales for transaction recording at garbage dumps, recycling facilities, mines, and other similar activities, as well as for credit transactions at truck stops or service stations.

B. Industrial

RF systems are perfectly adapted for the identification of high-unit-value items going through a demanding assembly process in a plant setting (such as the fabrication of agricultural or automotive equipment, where the product is cleaned, bathed, painted, and baked). Additionally, RF systems provide the longevity necessary for long-term detection of captive product carriers like:

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| A Monthly Peer Reviewed & Referred Journal |

||Volume 10, Issue 4, April 2021||

|DOI:10.15680/IJIRSET.2021.1004172|

- Tool carriers, monorail and power, free conveyor trolleys, tote boxes, containers, barrels, tubs, pallets
- Lift trucks, towline carts, and automatically guided vehicles.

Primary applications can be divided into two groups:

- Direct product identification, in which the tag directly identifies the object to which it is connected (for example, by part number or serial number, or, in the case of read/write systems, by assembly or process instructions for the object).
- Carrier identification in which the machine-readable RF "license plate number" of the carrier is given to the control system together with the content that has been manually (or using a barcode scanner) identified. Following load tracking is accomplished by strategically placed RF scanners.

C. Security and Law Enforcement

Using RF tags connected to equipment like tools and computers or built into security badges the movement and usage of expensive resources like persons and equipment may be tracked. In the event of an emergency evacuation, this form of monitoring also offers an additional layer of security for those operating in high-risk locations. Additionally, by using the idea of reference RFID tags, MSU's LANDMARC enhances the overall accuracy of finding items or people [9].

D. Nuclear Plant System

The Self-Diagnostic Monitoring System is being developed by the Pacific Northwest National Laboratory of the U.S. Department of Energy in Richland, Washington, to help plant operators. Radio-frequency tags are used in a prototype monitoring system to transmit performance information in nuclear power plant systems.

E. RFID-identification of waste bins

A data collecting and transmission solution with Memor2000 hand-held terminals has been provided by Mince Systems AB (www.minec.com) to identify trash cans or wastes with barcodes or RFID (Radio Frequency Identification) transponder tags. The HI tag 2 transponders chosen for this research have two portions of memory. The maker permanently encodes a unique code that cannot be copied, altered, or deleted into the read-only region. This offers a very high level of security. For detailed characterization and to make it easier to provide accurate purchase history, the read-write memory partition is programmed with a customer and/or bin number.

F. Animal identification

Livestock and animal control are two typical applications for RFID tags. A tag enclosed in a tiny glass capsule (approximately 4x30 mm in size) is inserted beneath the skin of an animal's neck using a device that resembles a giant hypodermic needle. The tag identifies the animal and may also contain other information. information, such immunization histories. Handlers simply need to "scan" the animal with a portable device at around 3 ft to identify it and save or retrieve information about it

G. Toll road control

Toll road control systems are designed to electronically identify passing cars to automatically debit their accounts for using the toll road without obstructing traffic. Lack of a national standard, which occurs when each manufacturer creates their own solution, is the main obstacle to establishing a national system. Amtech, an organization that tracks railroads, has long run a toll road on their property to advance their technology. Although many users of toll roads use the same section of road every day, many only use it sporadically, hence they are less likely to have transponders installed. Many users may pass toll booths operated by several corporations that employ various transponder protocols, necessitating the fitting of multiple separate transponders.

A minimum detection range of 4 meters is needed in these systems since the cars will be traveling at high speeds and because each manufacturer's vehicles vary in size and form. High reading speeds are preferred. This suggests that an electric field linked system, running at a frequency between 900 MHz and 5800 MHz, will be required for the toll road

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| A Monthly Peer Reviewed & Referred Journal |

||Volume 10, Issue 4, April 2021||

|DOI:10.15680/IJIRSET.2021.1004172|

system. Transponders are often fixed to a car's front glass. More than 1.8 million toll road transponders are said to have been in operation as of April 1997.

H. Healthcare

RFID labels and tags are starting to be used in the healthcare sector to track shared portable diagnostic equipment, medications, and supplies, including their expiration dates. As a result, healthcare facilities may better manage inventories and utilize their equipment to cut costs while providing the best possible patient care.

VI. SECURITY AND PRIVACY

Several privacy and security issues have been raised by the anticipated billion-fold growth of RFID tags. When businesses scan tags to obtain data about clients and then use data mining techniques to build individual profiles, privacy is often a problem [11]. A few scenarios were developed by anti-RFID campaigners to illustrate potential abuses if no safety measures are applied. The most typical is when someone scans tags without authorization to generate user profiles. Other situations include a thief scanning a gathering of people and spotting someone carrying a lot of valuable stuff or a mugger speculating about an individual's sickness by looking at the medications they are carrying (even money, if tagged as proposed). If tags start to take the place of credit cards, eavesdropping also becomes a concern that needs to be addressed. Although privacy is a problem, the difficulties outlined above are not the only concerns. As also, authentication is required. For instance, more recent tags include rewritable memory that can be used to store additional data during production. Stores must take precautions to prevent customers from switching the type of item to one that is less expensive if they use portable readers to calculate the sales price, for example. Additionally, access to the kill command, a feature that permanently disables a tag, needs to be restricted [11].

RFID is hampered by the limitations of constrained processing, constrained power, and unreliable connectivity. Below is a brief explanation of the necessary security requirements for an RFID system.

- *Data confidentiality*: It is the promise that the information being transferred will be kept private and that only parties with the proper authorization will have access to it.
- *Mutual Authentication*: Before any data is transferred, the tag and the reader must mutually authenticate one another.
- *Data integrity*: It is guarantee that an adversary has not modified the data while it is in transit.
- *Non-Repudiation*: This attribute makes sure that the tag and the reader cannot object to the data after it has been sent or received.
- *Availability*: This ensures that the security protocol between the tag and the server may be executed constantly and that it won't be prevented from being executed by the desynchronization of private data between the server and the tag [18].
- *Tag Anonymity*: The location, original identity, and other private information of the RFID tag are securely transferred.
- *Forward Secrecy*: This prevents an adversary from utilizing the current tag data to infer the previously sent tag information.
- *Scalability*: As the number of tags in the system grows, the security features of the protocol shouldn't be impacted

RFID users have two primary privacy concerns: inventorying and clandestine tracking. While being interrogated by a reader, RFID tags respond without allowing their owners or bearers know. Therefore, clandestine tag scanning is a real concern where read range allows. Even RFID tags that encrypt data with cryptographic algorithms typically radiate unique identifiers. As a result, someone wearing an RFID tag effectively broadcasts a fixed serial number to surrounding readers, creating an accessible platform for clandestine physical tracking. Even if the serial number on a fixed tag is random and contains no fundamental data, tracking is still possible [12].

RFID privacy is already a problem in several aspects of daily life:

- *Transponders for paying tolls*: Around the world, automated toll-payment transponders—small plaques installed in windshield corners—are typical. The data obtained from such a transponder was summoned by a court for use in a divorce case in at least one well-known incident, undermining the defendant's alibi [13].

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| A Monthly Peer Reviewed & Referred Journal |

||Volume 10, Issue 4, April 2021||

|DOI:10.15680/IJIRSET.2021.1004172|

- *Transponders for paying tolls*: Around the world, automated toll-payment transponders—small plaques installed in windshield corners—are typical. The data obtained from such a transponder was summoned by a court for use in a divorce case in at least one well-known incident, undermining the defendant's alibi [13].
- *Libraries*: A few libraries have RFID systems in place to make book checkout and inventory control easier while also lowering librarians' risk of repetitive stress injuries. The USA Patriot Act has in part sparked worries about book selection surveillance, which have exacerbated privacy worries regarding RFID [14].
- *Passports*: The International Civil Aviation Organization (ICAO), a global consortium, has published standards for RFID-enabled passports and other travel papers [10], [15].
- *Human implantation*: Like the VeriChip technology, few other RFID devices have ignited the passions of privacy activists [16]. VeriChip is an RFID chip that can be implanted into people, like those used for domestic pets. One intended use is medical record indexing, where a hospital can find a patient's medical record by scanning her identification tag. Hospitals have in fact started experimenting with these technologies [17].

There are numerous ways to ensure privacy. Typically, they are mechanisms that begin working once the client has purchased the product. Now of purchase, they are either enabled, or a user-owned device is in control of them [11].

- *Kill command*: a command that is accepted by EPC Class 1 and Class 2 tags. Once received, the command will make the tag useless. EPC Class 1 tags have 8-bit passwords, while EPC Class 2 tags have 32-bit passwords, preventing an attacker from calling those commands. A theoretical article explained how to upgrade the firmware on a cell phone to reprogram it to scan for tags and, once detected, to quickly enumerate all potential passwords.
- *Sleep command*: You cannot always kill a tag. Killing a library tag would necessitate retagging the book when it was returned, which would be counterproductive. However, it is important to safeguard library users' privacy. The kill command and the sleep command both functions similarly. The password-protected wakeup command is the only command that is recognized after being sent. The kill command has the same issues as the sleep command.
- *Split approach*: In this method, the data is spread across two tags, one of which the consumer can remove (for example a paper tag on clothing). While the removable tag has the serial number, the fixed tag just stores basic information about the device, such as its type, how to care for it, etc. With this method, products may be tracked using their unique identifiers while still allowing the consumer to keep track of their own items.
- *Blocking approach*: An extremely basic strategy is as follows: It uses a unique tag that deviates from the medium access protocol. A unique protocol used by RFID tags regulates access to the shared medium (air). When a reader enters a zone with several tags, it initially discovers all the tags within its range before asking each one. By spreading a random signal backward, the tag disables that mechanism and effectively jams the frequency. At the checkout counter, items are purchased in a supermarket, scanned, and then placed in a plastic bag with a blocker tag. No one can inspect the contents of the bag while it is being transported home. The products are taken out of the bag and put in the refrigerator at home. The products can then be scanned by the refrigerator and added to the inventory. Instead of including that functionality in a tag, it may instead be included in a device like a cell phone, which would enclose its carrier in a safe zone [11].

VII. FUTURE WORK AND RESEARCH

In RFID, frequency plays a significant role. From one band to the next, the electromagnetic wave's properties vary. There are several technical problems with RFID technology that need to be fixed, including cost management, energy efficiency, privacy concerns, interference from multiple readers, and security problems.

- *Cost management*: The adoption of RFID technology and systems worldwide is the ultimate objective of RFID proponents. The widespread development of RFID tags, readers, and applications has long been anticipated by RFID proponents. A few conditions, including willing participants and economically feasible RFID technology, are necessary for such widespread adoption. According to the research, bulk orders of RFID tags for chip tags may range in price from $0.3 to $0.5, while bulk orders of chapless tags can cost as little as $0.01 to $0.02. RFID tags are now more costly than barcodes. One of the key elements in restricting the use of RFID technology is this. According to estimates, RFID tags will have a cost benefit advantage over barcodes and will completely replace them if a price as low as ¢0.09 per tag is reached.
- *Energy Efficiency*: An RFID network has the following features: a very large number of tags per reader, for instance, each reader in a warehouse application handles thousands of tags; tags must be extremely tiny; and communication messages are often brief and straightforward.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| A Monthly Peer Reviewed & Referred Journal |

||Volume 10, Issue 4, April 2021||

|DOI:10.15680/IJIRSET.2021.1004172|

- *Privacy Issues*: There are several privacy concerns with RFID systems. Allowing remote access and data exchange indicates unauthorized use of personal data. Customers' privacy may be violated in a variety of ways when they purchase things with RFID tags: Because humans are unable to detect radio signals, tags could be read without a person's knowledge in the following ways: tags could be read by unauthorized parties; tags could be read by unauthorized parties; a database could be created to track relationships between tags and the owners of tagged items over time; information exchange between a tag and tag reader could be secretly monitored. Also, the possibility that the government could track citizens and eavesdrop on their personal habits using RFID tags has drawn more attention. Several researchers are engaged in this research. However, there are several privacy-related problems that merit more investigation and analysis.
- *Multiple Readers' Interference*: If there are many tags, anti-collision methods should be used to make each tag read-only only once. If they are in the same field, several readers may also interfere with one another. If two nearby readers communicate the same tag at the same time, it interferes. There are several algorithms that are used to overcome this issue. But this is indeed a research issue, which deserved further investigation [5]

VIII. CONCLUSION

The technology of Radio Frequency Identification (RFID) was surveyed in this research. A lot of people believe that RFID technology will soon be used everywhere. The article discussed RFID tags requiring three main components such as tag, reader, and server/host. RFID has become a crucial part of numerous computing applications, including transportation, industrial, record keeping, animal identification, document tracking, and healthcare. RFID security and privacy are interesting to study subjects that integrate a variety of fields, including privacy problems, read ranges, authentication, and privacy approach. This paper examined the RFID security requirements that must be put into practice to make the RFID system secure. With the widespread use of RFID technology, assaults on the system itself start to emerge. From common sniffing and eavesdropping to denial of service to new RFID viruses, this paper listed the most prevalent.

REFERENCES

1. X. Yu, C. Cecati, T. Dillon, and M. G. Simoes, "New frontier of smart grids," IEEE Ind. Electron. Mag., vol. 5, no. 3, pp. 49–63, 2011.
2. Department of Energy, "The future of the grid: Evolving to meet America's needs," Dec. 2014.
3. S. Xiao, "Consideration of technology for constructing Chinese smart grid," Autom. Electric Power Syst., vol. 33, no. 9, May 2009.
4. IEEE Grid Vision 2050 Reference Model, New York, NY, USA: IEEE, 2013.
5. Fazili, S., Grover, J. (2022). Smart Grid: A Survey. In: Agarwal, P., Mittal, M., Ahmed, J., Idrees, S.M. (eds) Smart Technologies for Energy and Environmental Sustainability. Green Energy and Technology. Springer, Cham.
6. X. Fang, S. Misra, G. Xue and D. Yang, "Smart Grid — The New and Improved Power Grid: A Survey," in IEEE Communications Surveys Tutorials, vol. 14, no. 4, pp. 944-980, Fourth Quarter 2012.
7. Hossain, Rahat Maung, Amanullah Than Oo, Aman Ali, Shawkat. (2013). Smart Grid.
8. P. Alcoy, P. Bowen, C. Chui, S. Bjarnason, K. Kasavchenko, G. Sockrider, and D. Anstee, (2018). Arbor's 13th Annual Worldwide Infrastructure Security Report.
9. D. Jin, Y. Zheng, H. Zhu, D. M. Nicol, and L. Winterrowd, "Virtual time integration of emulation and parallel simulation," in Proc. ACM/IEEE/SCS 26th Workshop Princ. Adv. Distrib. Simul., Jul. 2012, pp. 201–210. [Online]. Available: http://dl.acm.org/citation. cfm?id=2372596.2372597
10. V. Kolesnikov and W. Lee, "MAC aggregation protocols re- silient to DoS attacks," IEEE SmartGridComm, vol. 7, no. 2, pp. 226–231, 2011. [Online]. Available: http://inderscience.metapress. com/index/XW8541375106697V.pdf
11. Bhadani, U., 2020. Hybrid Cloud: The New Generation of Indian Education Society.
12. Cardenas, and J. G. Jetcheva, "AMI threats, intrusion detection requirements and deployment recommendations," in Proc. IEEE 3rd Int. Conf. Smart Grid Commun. (SmartGridComm), Nov. 2012, pp. 395–400.
13. X. Wang and P. Yi, "Security framework for wireless communications in smart distribution grid," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 809–818, Dec. 2011.
14. Huseinovic´, S. Mrdovic´, K. Bicakci, and S. Uludag, "A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid," in IEEE Access, vol. 8, pp. 177447-177470, 2020, doi: 10.1109/AC-CESS.2020.3026923.

|e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| A Monthly Peer Reviewed & Referred Journal |

||Volume 10, Issue 4, April 2021||

|DOI:10.15680/IJIRSET.2021.1004172|

15. Ukraine power grid cyberattack and US susceptibility: Cybersecurity Im- plications of Smart Grid Advancements in the US. Retrieved December 9, 2022, from https://web.mit.edu/smadnick/www/wp/2016-22.pdf
16. A. D. Maio, “Rao test for adaptive detection in Gaussian interference with unknown covariance matrix,” IEEE Trans. Signal Process., vol. 55, no. 7, pp. 3577–3584, Jul. 2007.
17. D. Gamerman and H. F. Lopes, Markov Chain Monte Carlo: Stochastic Simulation for Bayesian Inference. Boca Raton, FL, USA: CRC, 2006.
18. Tu`ng T. Kim, H. Vincent Poor (2011). Strategic Protection Against Data Injection Attacks on Power Grids.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details