An Overview of RFID Applications and Security

Ruchi Sharma, Associate Professor

Department of Electronics & Communication Engineering, Vivekananda Global University, Jaipur

Email Id -sharma.ruchi@vgu.ac.in

ABSTRACT: ***RFID is extensively utilized in a variety of settings, including logistics, supply chains, asset monitoring, and health care, among others, attracting the interest of numerous academics. This article provides an overview of the most often discussed RFID issues, with an emphasis on applications, security, and privacy. A total of 62,685 records were downloaded and processed from the Web of Science (WoS) and Scopus core databases, resulting in 40,677 unique items after reconciling the datasets to eliminate duplicates. Fundamental metrics such as the number of citations, average growth rate, and average number of papers each year were extracted and displayed. Using ScientoPy, a free Python program, we extracted the top themes and evaluated the pertinent indicators. The following sections discuss the findings: the Internet of Things (IoT), Supply Chain Management, Localization, Traceability, Logistics, Ubiquitous Computing, Healthcare, and Access Control; the second is the Security and Privacy section, which includes Authentication, Privacy, and Ownership Transfer; and finally, we discuss the implications. This article aims to provide the reader a broad picture of the current state of trending RFID issues and to offer various assessments from various angles, depending on the reader's objectives or background.***

KEYWORDS: ***Bibliometrics, Data Science, RFID, Scientometric, Scientopy.***

1. INTRODUCTION

Technology is supposed to work for us in increasingly visible and pervasive ways. RFID is used in a variety of settings, including logistics , supply chains , asset monitoring , healthcare, industrial business environments , and many more, to make our lives simpler and generate enormous amounts of data on a variety of levels. The most current research areas in RFID technology are described in this review article. Researchers will be able to use this data to discover research gaps and hot subjects[1]. It may also be helpful for those outside academics and other fields, since it provides a quick summary of the most current studies into RFID applications and security issues. Several reviews and surveys have been published that look at RFID from various angles. There were evaluations of the technology's uses, as well as academic literature and historical reviews, from 2007 to 2009. In addition, we came across a 2010 study on how RFID is utilized for tracking in the Internet of Things (IoT)[2].

In 2006, a review of specific applications, such as postal and courier services, was published. Similarly, work on its application in the aviation industry was published in 2010; work on its application in activities such as construction was published in 2015; healthcare-related publications were published from 2013 to 2018; work on supply chain management was published between 2010 and 2016; work on localization in the smart home paradigm was published in 2018; and finally, a paper on its application in the smart home paradigm was published in 2018. There was also a look at the function of RFID in transportation, which looked at the benefits and drawbacks of the technology. We noticed that each year's reviews tended to focus on a single topic. Based on the number of citations in papers published from 1996 to 2020 and activity in the selected topics between 2019 and 2020, this review compiles the most active topics to present the trends in RFID technology applications, contributing an updated overview similar to the reviews of the applications published before [10,11], but also creating eight groups based on the most active topics[3].

- *The Internet of Things (IoT)*: We can use RFID to track and protect specific items in a variety of settings all around the globe. Depending on the circumstances and needs, the technology provides a variety of pricing choices. RFID is often seen as a requirement for the Internet of Things for this reason and others. There have been many research on communication protocols to increase speed without sacrificing security or scalability; when utilizing mutual authentication between the reader and the tags, robust security and privacy are critical[4]. Existing security threats, privacy concerns, and countermeasures, as well as identifying limits, needs, and problems to work on for more secure deployment to satisfy security demands, are all being investigated[5]. Due to the constraints of processing, storage, and power on the RFID tag side, there is a need for more lightweight RFID authentication methods. Security and privacy communication models are being developed that are more resource-efficient while yet satisfying application security requirements. Furthermore, studies are focused on commercial tags in order to uncover common vulnerabilities and potential solutions for achieving secure applications. In addition to evaluating how to implement security via new policies for fine granularity and context-aware

information control, RFID–IoT studies are also looking into how to enforce security through new rules for fine granularity and context-aware information control [6].

- There is also a hardware and software suite for laboratories to test these new proposals, which includes emulating tags and readers and analyzing security schemes that aim to provide secure and untraceable communication for end-users, allowing flexibility and application in various environments while taking into account important IoT components like quality of service (QoS) or message queue telemetry. When considering the low-carbon economy, RFID plays a function in the industrial business environment[7]. However, its primary use is to aid in monitoring, traceability, and tracking, as well as to acquire more precise location data through ultra-wideband (UWB) technology[8] . It also helps to guarantee worker safety. For example, researchers want to develop an improved safety system for hazardous situations in industrial facilities utilizing wireless sensor networks (WSN) and RFID. Because of the importance of these activities, the industrial Internet of Things (IIOT) necessitates a high degree of trust and performance. As a result, research has been conducted into a general architecture for application program interfaces (APIs) that can handle the wide range of RFID equipment available for industrial environments , as well as improving communication speed and reliability for a large population of tags using an estimator to maximize channel usage efficiency[9] .
- *Managing the Supply Chain (SCM)*: RFID in supply chain management (SCM) connects the physical world with management systems; RFID gathers data to be evaluated and enhances management quality, which is a topic of particular interest for big corporations. For example, by implementing a framework for RFID development, the efficiency of operations may be improved, and competitive advantage can be increased. Researchers are also examining the effect of e-supply chains for grocery retailing; the benefits, challenges, and effects that RFID applications may bring to retail in the UK; the application in convenience stores in Taiwan and comparing RFID benefits for the United States and the Republic of Korea (South Korea) in their search for a smarter process . To deploy smart shelves [10], with identification at the item level in the retail supply chain, and decide how the cost should be shared among the partners, as well as its implementation on a sales floor ,a mean-variance analysis is required. Similarly, existing software solutions and information systems for supply chain coordination have been examined, with the performance obtained by incorporating RFID assessed using quantitative assessment or empirical evidence. Different factors in the supply chain, such as the impact of tag orientation and package contents on tag reading, are taken into account by investigators, resulting in discrepancies.
- *Geographical location*: The main purpose of RFID technology is to identify items, but researchers are pushing the technology's boundaries to extend its capabilities, enabling localisation information to be acquired from certain interior situations where GPS systems are usually ineffective. Real-time location tracking with high precision via RFID tags using commercial off-the-shelf (COTS) devices, a standalone positioning system using low-cost passive RFID tags installed to guide the path , the location of tags that are not in line of sight (NLOS) for the reader , and navigation for autonomous mobile robots using passive RFID tags are all examples of these applications. When RFID UHF tags are read on industrial mobile vehicles and robots, the signal strength indication from the vehicle's transponder causes the vehicle to move. Using the same concept, it allows the location and approach to a stationary target item. Another example is occupancy monitoring for smart buildings and indoor settings, which focuses on reducing energy use in these areas. In addition to enabling the locating and monitoring of people, equipment, and materials in realistic construction settings, RFID is utilized in the construction of structures to enforce management and safety.
- *Management of Logistics* : RFID technology is used in logistics to collect data that allows for the visualization and creation of analytics, such as on a shop floor where huge amounts of data are produced , and in material tracking for construction logistics . These applications need the use of intelligent network systems to gather data that can then be evaluated and distributed in real time. Furthermore, research in the retail industry has resulted in the development of a contingency model for identifying the most critical aspects of RFID supply chain projects for use in logistics and manufacturing settings. Researchers have also developed a methodology for evaluating RFID use in logistics. The use of a distributed simulation platform to develop sophisticated RFID-based freight transportation systems has been studied . This will also enable logistics truck management to interact with global positioning systems (GPS) and geographic information systems (GIS). There has also been a description of an architecture for enhancing terrestrial logistics.

1.1 Security and Privacy:

The security and privacy of data is a significant issue in many applications. The primary reason is the IoT and associated services' rapid growth and Internet diversity. As a result, there have been a number of concerns raised, including those about the security of already in use protocols like the mutual authentication protocol. In order to better secure the major technology users, it is also essential to examine existing threats and their remedies, as well as evaluate presently utilized standards such as the EPC Global C1G2. RFID scanners, tags, middleware, and backend systems are all being tested and new ways are being sought. The average number of security-related publications each year given in Figure 4, as well as the most significant indicators presented in Table 3, which offer values close to the IoT subject in the application part, indicate the importance of this scenario. As a result, the authentication subject exhibits the same pattern. The bulk of research are focused on reader-tag authentication, investigating novel ways for safeguarding this communication against various known threats while keeping a consistent AGR. Similarly, the ownership transfer issue investigates novel ways for ensuring security in the actual transfer of tags, safeguarding the privacy of the components, and determining the process's scalability to secondhand marketplaces and circular supply chains. The mutual authentication protocol, which has been studied in many ways, is one of the most researched subjects. Investigations have looked at potential mutual authentication protocol attacks and suggested changes to prevent them. Similarly, research into novel mutual agreement protocols to guarantee safe communication between mobile RFID-enabled devices and the main server has progressed. Similarly, enhancements to the hash-based RFID mutual authentication protocol to prevent denial of service (DoS) attacks have been investigated, as has cryptanalysis use in lightweight mutual authentication and ownership transfer for RFID systems . To address impersonation and replay threats, an RFID authentication technique based on quadratic residues has been developed, and novel approaches such as chaotic map use to ensure a mutually authenticated process utilizing a chaotic cryptosystem have been investigated . Due to the hardware constraints of the tags, however, researchers are looking for the most efficient ultra-lightweight authentication protocol. Finally, work is underway to validate GS1 EPC Class 1 Generation 2 RFID standards, which include mutual authentication and privacy protection in order to decrease database load and guarantee user privacy. All RFID settings, including low-cost RFID networks, need strong security and privacy. All of the aforementioned procedures and security precautions will ultimately make their way into daily life. One of the most common uses for these technologies is establishing frameworks to protect privacy in RFID-based healthcare systems. Furthermore, the increasing use of RFID makes security one of the most pressing issues in the IoT.

- *Authentication*: RFID tags' versatility in terms of shape and operating frequencies allows for a wide range of modifications for various and changing settings, such as solutions to provide secure and efficient medicine for patients. The development of protocols for authentication, such as Chien's protocol and other ultra-lightweight RFID, provides for advances in security against known weaknesses. Similarly, describes a lightweight authentication system for low-cost RFID with untraceability in mind. Cryptanalysis was used to examine the security level provided by protocols adhering to the EPC-C1G2 standard. Similarly, the security implications of RFID and authentication processing frameworks have been investigated, with researchers looking into a robust protocol based on error correction codes (ECC), as well as the inherent use of physical-layer authentication using integrated circuits to prevent device cloning. The development of effective methods for monitoring lost RFID tags has enhanced security. In response, a protocol has been developed to give coexistence proofs for RFID tags in order to identify tagged components that are shown at the same time and in the same location.

2. DISCUSION

Radio-frequency identification (RFID) utilizes electromagnetic fields to automatically detect and track tags attached to items. An RFID system comprises of a small radio transponder, a radio receiver and transmitter. When activated by an electromagnetic interrogation pulse from a nearby RFID reader device, the tag sends digital data, typically an identifying inventory number, back to the reader. This number may be used to track inventory items. Passive tags are fueled by energy from the RFID reader's interrogating radio waves. Active tags are powered by a battery and therefore can be read at a longer range from the RFID reader, up to hundreds of meters. Unlike a barcode, the tag does not need to be inside the line of sight of the scanner, thus it may be embedded in the tracked item. RFID is one form of automated identification and data capture (AIDC) (AIDC). RFID tags are utilized in numerous sectors. For example, an RFID tag affixed to a car during manufacturing may be used to monitor its progress through the assembly line, RFID-tagged medicines can be tracked via warehouses, and implanting RFID microchips in cattle and pets allows positive identification of animals. Tags may also be used in businesses to speed checkout, and to prevent theft by consumers and staff. Since RFID tags may be attached to real money, clothes, and belongings, or implanted in animals and humans, the potential of

accessing personally-linked information without permission has generated significant privacy issues. These concerns led in standard specifications creation addressing privacy and security problems.

3. CONCLUSION

RFID applications range from asset identification to tracking for industrial and general public environment applications, such as interior applications , robot navigation , and the placement of objects, including those that are not visible . Ultra-wideband has been utilized to solve some of the existing issues with narrowband frequencies. It also assists organizations with construction management and safety and pushes the boundaries of transmission signal quality enhancement in various frequencies .We discovered that privacy and authenticity were of the greatest importance . Based on scientometric factors, we divided the most active RFID applications into eleven categories in this study. The IoT is one of the applications highlighted for this technology, which supports the notion that RFID is a fundamental need for the Internet of Things . RFID was also used in supply chains , allowing for the detection of counterfeiting and the tracking of any asset. Testing current protocols for vulnerabilities and methods to fix them , as well as balancing privacy and performance for various situations , seem to be the most active security issues. Privacy and security are a major issue in nearly all apps, according to the findings. Furthermore, healthcare is a subject with a good AGR in the findings, and it incorporates RFID in a variety of associated activities . RFID is also utilized in access control, such as controlling access to places and systems , and its use in the human body has been investigated from many angles . Other recent papers have focused on specific topics, so this paper can serve as a jumping-off point, providing a global perspective to aid researchers in exploring the most active topics, trending applications, and security work in RFID, information that is useful to people with a variety of backgrounds and interests. During this study, it was discovered that the use of RFID is expanding, with security models and protocols managing the complexity. RFID is used in a variety of scenarios, as noted throughout the paper, and its applications and functionalities continue to expand, such as working with wireless sensors and IPv6, the new addressing system for the Internet of Things, and expanding its frequencies to allow for technological advancements (currently to ultra-wideband). As a result, this technology is finding new applications in RF, electronics, and security, and it is not an exaggeration to say that RFID will be the technology that enables any existing item to be linked to the Internet through the Internet of Things. Clarivate, WoS, and Scopus were utilized as centralized and main databases. Further study may look at databases that collect data quickly to get the most up-to-date information on RFID research and its relationship to new and trending technologies.

REFERENCES

[1] K. Singh and G. Kaur, “Radio frequency identification: Applications and security issues,” 2012, doi: 10.1109/ACCT.2012.94.

[2] M. Feldhofer and J. Wolkerstorfer, “Hardware Implementation of Symmetric Algorithms for RFID Security,” in *RFID Security*, 2008.

[3] K. Kasemsap, “Radio frequency identification and mobile ad-hoc network: Theories and applications,” in *Handbook of Research on Recent Developments in Intelligent Communication Application*, 2016.

[4] G. Thamilarasu and R. Sridhar, “Intrusion detection in RFID systems,” 2008, doi: 10.1109/MILCOM.2008.4753218.

[5] A. Souhail, “RFID based Automation system for garage parking,” *IEEE TENCON*. 2016.

[6] D. C. Wyld, “The chips are in: Enhancing sports through RFID technology,” *Int. J. Sport. Mark. Spons.*, 2008, doi: 10.1108/ijsms-09-02-2008-b008.

[7] J. M. Myerson, *RFID in the Supply Chain*. 2006.

[8] S. Piramuthu and W. Zhou, “RFID, sensor networks,” in *RFID and Sensor Network Automation in the Food Industry*, 2016.

[9] E. Vahedi, V. W. S. Wong, and I. F. Blake, “An Overview of Cryptography,” in *Advanced Security and Privacy for RFID Technologies*, 2013.

[10] D. Merli, G. Sigl, and C. Eckert, “Identities for embedded systems enabled by physical unclonable functions,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, 2013, doi: 10.1007/978-3-642-42001-6_10.