electronics

MDPI

Article

Survey: An Overview of Lightweight RFID Authentication Protocols Suitable for the Maritime Internet of Things

Glen Mudra [1,*], Hui Cui [2,*] and Michael N. Johnstone [3]

[1] School of IT, Murdoch University, Perth, WA 6150, Australia
[2] Faculty of IT, Monash University, Melbourne, VIC 3800, Australia
[3] Security Research Institute, School of Science, Edith Cowan University, Perth, WA 6207, Australia; m.johnstone@ecu.edu.au
* Correspondence: 33683512@student.murdoch.edu.au (G.M.); hui.cui@monash.edu.au (H.C.)

Abstract: The maritime sector employs the Internet of Things (IoT) to exploit many of its benefits to maintain a competitive advantage and keep up with the growing demands of the global economy. The maritime IoT (MIoT) not only inherits similar security threats as the general IoT, it also faces cyber threats that do not exist in the traditional IoT due to factors such as the support for long-distance communication and low-bandwidth connectivity. Therefore, the MIoT presents a significant concern for the sustainability and security of the maritime industry, as a successful cyber attack can be detrimental to national security and have a flow-on effect on the global economy. A common component of maritime IoT systems is Radio Frequency Identification (RFID) technology. It has been revealed in previous studies that current RFID authentication protocols are insecure against a number of attacks. This paper provides an overview of vulnerabilities relating to maritime RFID systems and systematically reviews lightweight RFID authentication protocols and their impacts if they were to be used in the maritime sector. Specifically, this paper investigates the capabilities of lightweight RFID authentication protocols that could be used in a maritime environment by evaluating those authentication protocols in terms of the encryption system, authentication method, and resistance to various wireless attacks.

Keywords: RFID; IoT; MIoT; cyber security; maritime

Citation: Mudra, G.; Cui, H.; Johnstone, M.N. Survey: An Overview of Lightweight RFID Authentication Protocols Suitable for the Maritime Internet of Things. *Electronics* **2023**, *12*, 2990. https://doi.org/10.3390/electronics12132990

Academic Editors: Marios Avgeris, Dimitrios Dechouniotis, Konstantinos Tsitseklis and Vitoropoulou Margarita

Received: 30 April 2023
Revised: 29 June 2023
Accepted: 5 July 2023
Published: 7 July 2023

1. Introduction

The maritime industry contributes significantly to civilisation and the global economy by facilitating passenger travel and the transport of goods worldwide. As a "green" option, marine transport is attractive because it is economical and best-suited for large volumes of cargo [1]. The value of the shipped cargo is significant. For example, in Australia, it is estimated that the value of cargo shipped annually is AUD$592.9 billion and that the maritime industry provides revenue of AUD$6.88 billion annually [2]. Australia ranks fifth globally for the volume of goods shipped annually with 80% of Australia's trade being facilitated by seaborne travel, thereby providing a boost of more than AUD$2 billion dollars to the Australian economy [2].

The Organisation for Economic Cooperation and Development (OECD) estimates that the volume of maritime freight will triple by 2050 [3], which presents several challenges for the maritime industry, as it needs to increase its capacity to meet growing demands and ensure sustainability. Whilst the overall objective of the maritime sector remains the same, maritime industries are required to expand and adapt by modernising processes to align with Industry 4.0 [4]. Industry 4.0, also known as the fourth industrial revolution, refers to the digital transformation of the industry, forcing organisations to review their strategies on how they operate and think outside the box—organisations need to revolutionise how they operate by leveraging technology to improve their performance and increase efficiency to

maintain their competitive advantage. As such, the maritime industry continues to adopt technology (e.g., the IoT) to evolve and meet these demands.

Technology has played a positive role in transforming the maritime industry by improving its performance and addressing real-world issues with innovative solutions; however, these advances have also introduced new risks with new threat avenues for notable cyber attacks that have steadily increased in recent years, which poses significant instability to the industry [5], which causes significant concerns. A recent cyber security survey conducted by Ports and Terminals revealed that 74% of the respondents had been the target of an attempted or successful data breach within the past year [6]. A single cyber attack across major ports in the Asia–Pacific region has the potential to cause $110 billion dollars worth of damage, and a virus-infected computer carried by a vessel could scramble database records causing a major disruption to port operations [7].

1.1. Maritime Internet of Things

In 2006, a (then) new concept, e-navigation, was presented to the Maritime Safety Committee (MSC), which is now governed by the International Maritime Organisation (IMO). The core functionalities of the IMO include maritime safety, security, and protecting the environment. The e-navigation concept specifically focuses on MIoT devices, both at sea and ashore, that communicate via electronic means. In addition to traditional challenges associated with IoT, such as privacy and security concerns caused by limited resources, the MIoT also inherits additional risks that are specific to its nature [8]. Considering that the oceans make up 70% of the Earth's total surface area, the maritime industry, or shipping in particular, is a global operation that reaches some of the most remote areas in the world and requires ubiquitous connectivity to facilitate communication across organisational, regional, and national boundaries over the MIoT network to ensure service continuity. The vast surface area of the sea, combined with long distances and multiple routes between destinations means that traffic control (data transmission) is somewhat uneven—whilst many vessels take routes close to shore using various channels and waterways (and thus are in almost constant communication), other vessels are required to travel across deep seas (so MIoT communication often occurs in bursts). MIoT networks must cater for this uneven distribution.

Furthermore, the maritime industry relies on communication and information exchange between several systems and devices that are heterogeneous. IoT devices are used onboard vessels or land-side operations for data collection, reporting, and monitoring as well as automation. To harness the full potential, devices must be able to communicate often via a gateway that provides interconnections for several systems and devices. For example, sensors that monitor the environment, such as wind, weather, water depths, etc., are all utilised to analyse conditions to assist in maritime operations (navigation routes, berthing vessels). Whilst the maritime environment is complex, a simple design approach for MIoT systems is preferred. Not only are simple systems cheaper to manufacture and maintain, they are also often found to be robust and capable of handling harsh conditions, such as extreme weather or exposure to elements, with minimal to no user intervention [9]. This is because many MIoT systems use remote monitoring and control capabilities from onshore locations; therefore, the reliability of MIoT systems must be assured. Security is also of high importance to the maritime industry, as it is susceptible to various targeted attacks, some specific to maritime and others more generic to IoT systems. These attacks include Automatic Identification System (AIS) Spoofing, Global Positioning System (GPS) Spoofing, Remote Access Attacks, Radio Frequency Jamming, Sensor Manipulation, and Malware or Ransomware attacks.

- AIS Spoofing—Vessels are mandated to use an AIS system for vessel tracking and situational awareness to assist with collision avoidance. AIS Spoofing is the manipulation of AIS data to broadcast false vessel location, identity, or other information. AIS Spoofing can create confusion, increase safety risks, and be used to hide illegal activity [10].

- GPS Spoofing—Vessels rely on GPS systems for positioning and navigation. GPS Spoofing broadcasts false information to interrupt GPS receivers and can lead to potential collisions, access to restricted areas, and misdirection of vessels [11].
- Remote Access Attacks—Exploit the use of the remote access and control functionality to gain unauthorised access. Adversaries use this access to manipulate systems, cause disruption, and even steal sensitive information [12].
- Radio Frequency Jamming—The maritime industry relies on radio frequency (RF) to communicate between sensors, vessels, and other MIoT devices. Jamming is the intentional disruption or degradation of these communication channels, which negatively impacts operations [13].
- Sensor Manipulation—The maritime sector uses a variety of sensors that monitor the equipment status, cargo integrity, and environmental conditions. These sensors assist with predictive maintenance, improving safety and the impact on the environment by monitoring emissions. Adversaries may target these sensors to provide false or misleading data readings that have a flow-on effect to integrated systems [14].
- Malware and Ransomware—Compromised devices or systems with malware or ransomware are used by adversaries as entry points to launch attacks, disrupt operations, and steal data or demand ransom payments (ransomware) [15].

A popular subsystem of the MIoT is Radio Frequency Identification (RFID) technology [16]. To the best of our knowledge, minimal work has been conducted within the area addressing the security around RFID protocols utilised in the maritime domain. Research typically focuses on the application or use cases where the technology is applied but does not cover the security component [17–22]. This paper summarises applications of RFID technology in the maritime sector and explores its vulnerabilities in realistic use cases. We focus on passive-RFID technology that is used to improve supply chain management and logistics through object identification and tracking. The objective is to provide a guide on lightweight protocols that are suitable for passive-RFID systems within the MIoT that are crucial for ensuring system security, improving resiliency, and providing long-term sustainability for our maritime industry.

1.2. Organization

The rest of this paper is organised as follows. In Section 2, we describe the principles of RFID and the attendant security issues arising from the implementation of those principles. In Section 3, we review current applications of RFID technology within the MIoT domain. In Section 4, we provide an overview of lightweight RFID authentication protocols suitable for passive RFID technology. Section 5 describes the parameters of the real-world scenario we intend to use to validate selected authentication protocols. Section 6 discusses the findings. This is followed by Section 7, which highlights the research gap and requirements for future work. Finally, Section 8 summarises the contributions of this paper.

2. Preliminaries

This section provides a brief overview of RFID principles, describes some issues regarding RFID security and privacy, and notes a range of attacks to which RFID technology is susceptible.

2.1. RFID Definition

RFID technology facilitates communications between IoT devices by providing a wireless channel between a transponder (tag) and a receiver (reader). An RFID system typically contains three components, a tag, a reader and a back-end server or database in which data are stored, as per Figure 1. A tag contains an integrated circuit (IC) attached to an antenna that is used to transmit a signal and communicate with a reader when in its proximity. RFID provides the ability to identify objects in the neighbourhood of a reader, unlike barcodes [23] which must be in direct sight of a barcode scanner. RFID systems operate by affixing a small tag to an object so that the object can be identified when it

comes within the range of a reader. RFID technology also allows additional information regarding the object to be stored within the tag's onboard memory chip, which can provide extra functionality. Rather than simply containing an object's generic type (as in bar code systems), RFID tags can contain object-specific information, such as a unique serial number, status, location, or product information. This information can be modified as the tag travels from place to place.

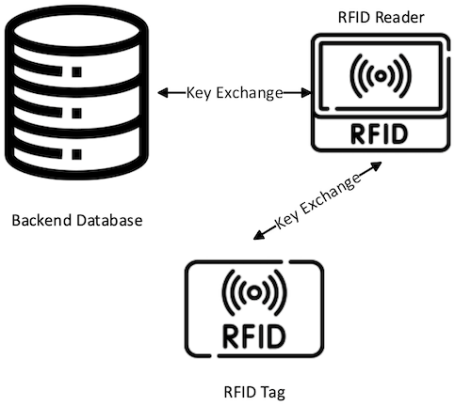

Figure 1. RFID system principles.

The proximity or distance within which an RFID tag can be identified by a reader depends on the frequency of the radio waves. Lower frequencies provide weaker signals (i.e., have less energy than higher frequency waves) reducing the distance over which a reader can communicate with a tag, but lower frequencies are more resilient to signal disruptors, such as liquids and metals. Higher frequencies provide a stronger signal, increasing the distance over which a tag and reader can communicate but requiring more power.

RFID technology can be categorised into three types, depending on their range and simplicity of construction, viz., passive, semi-active, and active RFID tags. Passive RFID tags are the simplest and most common tags. They contain only an integrated circuit board and an antenna. As such, a passive tag relies on the power (known as backscatter) generated from RFID readers, thus requiring the tag to be in close proximity to a reader in order to operate. Therefore, passive RFID tags are compact and cheap to manufacture, making them a popular choice. The RFID backscatter allows a nonpowered RFID tag to utilise the energy transmitted from an RFID reader to activate the tag IC through the antenna and provide a response, and the remaining power is modulated or converted within the tag's onboard chip and returned via the tag's antenna to the reader's antenna. Semi-active RFID tags contain their own power source that can be used to power additional sensors or components connected to the tag, yet lack an antenna and rely on backscatter to communicate and distribute signals, making them similar to passive RFID tags but providing an extended range compared to passive RFID tags. Active RFID tags contain their own power source along with an onboard transmitter that broadcasts their signal, making them larger in size and more expensive to manufacture than the other types (but they have a much larger range than the other types). This paper focuses on passive RFID tags, as they are widely utilised within the maritime sector due to their price and form factor.

2.2. RFID Security and Privacy

Concomitant with the IoT [24], the MIoT also inherits the associated security risks [23] that come with an interconnected world of more than 12 billion devices, as of 2021 [25]. As a result, the security landscape has drastically changed and continues to do so. As more devices connect to the IoT, the volume of attacks has (unsurprisingly) increased, but also, the attacks have grown in complexity [26]. Generally, the level of effort adversaries invest into an attack is directly related to the impact that they can have, whether it be monetary, malicious damage, or sabotage. The risk associated with each threat is dependent on

the application or nature of IoT systems, and thus, IoT system architects should design and build solutions that protect the confidentiality, integrity, and availability of the data contained within these systems using appropriate security controls [27,28].

As the maritime environment is dynamic, its systems' design is a crucial component and must be considered in relation to the type of application. Maritime IoT systems designed for at-sea operation must consider the limited resources, i.e., no direct access to power sources or constant network connectivity and the exposure to the elements. For example, smart buoys with IoT sensors and data collection capabilities must contain their own power sources in order to operate, often through the use of batteries [29]. In order to prolong the lifespan of the device, efficient operations must be utilised to avoid the consumption of available resources. This can be achieved by using lightweight computational functions and communicating with other IoT devices at less frequent intervals to save power. MIoT devices may also use alternative power sources, such as waves, to generate power [29]. MIoT devices must consider special hardware considerations, such as water resistance, circuit board hardening, and shock resistance, to handle the elements of the maritime environment [9].

Whilst the benefits of the IoT are significant, there are several areas of concern that need to be considered when employing RFID technology. The security controls most relevant to RFID technology are encryption, authentication, and physical security. Encryption is the process of converting data into a new format that cannot be easily read by an unauthorised entity. Authentication is the act of validating an entity's identity to determine if the entity is authorised before providing access or sharing information. Physical security relates to appropriate measures put in place to prevent an entity from physically damaging, stealing, or gaining access to systems, information, or hardware components. This paper focuses on security from a technical perspective—as such, physical security is outside its scope.

Since RFID technology relies on electromagnetic waves to communicate between a tag and a reader, the technology is susceptible to attacks common to other wireless protocols which include, but are not limited to, cloning, spoofing, Man-in-the-Middle (MitM), replay, forward security, brute force, Denial of Service (DoS), and desynchronisation attacks [30,31]. Whilst adversaries must be in close proximity to a tag, the frequency of movement of most RFID tags provides opportunities for adversaries to intercept communications—an authentication protocol is one of the first measures used to defend against such attacks.

2.3. Confidentiality in RFID

As mentioned previously, RFID tags contain an onboard memory chip that can contain sensitive data in addition to a tag's unique identifier. As such, cryptographic methods, such as encryption, are a common solution to ensure the confidentiality of the data stored on a tag. Although the principle of data encryption is straightforward, the use of encryption in RFID technology faces some challenges. Many RFID devices are incapable of performing complex cryptographic functions in real-time due to power and memory limitations; thus, some cryptographic methods are not recommended for resource-limited IoT devices, such as passive RFID tags [32]. Therefore, complex encryption techniques are generally enacted server-side. The two general types of encryption techniques used are as follows:

- Symmetric Encryption. The symmetric encryption mechanism uses a single secret key for both encryption and decryption. Popular symmetric algorithms include the Data Encryption Standard (DES), Triple DES (3DES), and the Advanced Encryption Standard (AES). In addition to secret keys, passwords are used as secrets in some symmetric schemes to encrypt and decrypt data—a process known as password-based encryption.
- Asymmetric Encryption. Asymmetric encryption schemes use public and private key pairs to conduct encryption and decryption. The public key is applied to data encryption and a private (secret) key is used for data decryption (e.g., the Rivest–Shamir–Adleman encryption algorithm).

Passive RFID tags often employ the use of symmetric encryption techniques, because they can require less computation compared to asymmetric schemes. As symmetric encryption uses a single key for both encryption and decryption, the key must be shared between multiple devices and or parties. The necessity of key sharing makes symmetric encryption schemes less secure than asymmetric schemes, as the latter utilises two separate, yet mathematically-related, keys. In asymmetric schemes, the private key must be kept secret to give only the intended or authorised person the ability to decrypt the data (e.g., the RSA algorithm [33] is a commonly used asymmetric encryption scheme that allows any sender to encrypt a message using a receiver's public key, whilst the private key remains known only to the receiver). Not having to expose a decryption key via over-the-air (wireless) transmission channels reduces the risk of key theft. A key can be compromised via a brute-force attack in which an adversary repeatedly attempts to guess the correct key until the correct key is determined. Of course, if the key space is large enough, this can take some time [34].

2.4. Hash Functions

Another cryptographic technique widely used to ensure integrity and, as a side effect, confidentiality, is a hash function, or simply, a hash. A hash is a one-way mathematical function that converts a numeric input into another compressed numeric value to maintain the integrity/confidentiality of the data. Whilst the input to a hash function can be arbitrary, the output (hash value) is always of a fixed length. Examples of hash functions are message-digest algorithms, including the MD5 developed by Rivest in 1992 [35] and the Secure Hashing Algorithm (SHA) [36]. The MD5 outputs a 128-bit hash value, but several vulnerabilities have been identified in this algorithm. SHA variants (e.g., SHA-1, SHA-2, and SHA-3) are more complex hash functions that support the output of hash values of different sizes, making them more secure and thus harder to compromise [36].

2.5. RFID Authentication

The authentication of trusted entities is a problem for all systems. It is usually solved by something you know (e.g., a password), something you have (e.g., a token), or something you are (e.g., a biometric signature) [37] For RFID-based systems, the limited computation and memory resources available to RFID tags present a challenge for authentication. Thus, choosing a suitable encryption scheme to be utilised is often driven by the aforementioned constraints. As RFID systems broadcast their signals to communicate with devices, they are potentially at risk from the actions of adversaries, at least within the proximity of the broadcast signal. Processes such as mutual authentication can act as an additional security control to allow a reader to confirm the identity of a tag and vice versa. Additionally, as previously mentioned, since RFID technology uses electromagnetic waves to communicate, it is susceptible to wireless attacks, such as

- Cloning Attacks, in which an adversary duplicates an authorised tag to gain unauthorised access.
- Spoofing Attacks, in which an adversary takes on the identity of an authorised tag to gain access.
- Man-in-the-Middle Attacks, where an adversary eavesdrops on communication between authorised devices.
- Replay Attacks, in which an adversary re-uses information, such as session keys, to gain access to the system.
- Brute Force Attacks, where an adversary repeatedly guesses passwords until access is obtained.
- Denial of Service (DoS) Attacks, where an adversary attempts to overload a system so that the system becomes unresponsive or unavailable to legitimate users.
- Desynchronisation Attacks, in which an adversary disables communication between authorised devices so that authentication cannot be performed.

3. Maritime RFID Applications

This section provides an overview of various RFID solutions used throughout the maritime sector. The maritime sector currently employs RFID technology to address various issues and improve the efficiency of routine operations relating to maritime development, protection, and sustainment. RFID technology continues to be deployed in novel ways in which a significant benefit continues to be realised, both on land and at sea. RFID devices are used on unmanned ships to collect environmental data, the internal states of the ship, and the working states of equipment via RFID and intelligent systems. The data are then utilised to provide insights and feedback via intelligent systems to inform key stakeholders [17]. For example, sensors onboard the vessel can automatically identify an issue and inform the ship's maintenance crew so the issue can be addressed early, minimising the potential damage and impact. As noted previously, these devices use electromagnetic waves to communicate; thus, they are susceptible to attacks from potential adversaries within the proximity of the ship—upwards of 100 m for active RFID tags. This can be problematic for classified vessels, such as naval ships that wish to remain undetected. Another military example is the application of RFID technology combined with biometrics to track and maintain an inventory, such as personal infantry weapons. The solution involves military personnel authentication via biometrics, including fingerprints and iris scans. A reader can read the tag affixed to the weapon and update its status, e.g., Returned or Checked-Out [19]. As RFID technology is susceptible to spoofing and tracking attacks, the same technology can be utilised by adversaries, as items (such as weapons) can be tracked, thereby recording the location and movement of each item if not secured properly. Therefore, RFID protocols should implement appropriate security measures to preserve the confidentiality and integrity of the data being exchanged between MIoT devices.

A common application of RFID technology within the maritime sector is its use in container ports [38]. Sea containers are standard storage units/containers that are used to transport a variety of goods efficiently. The standardised size/format allows for container ports to easily plan for, move, and manage large cargo volumes, shifting containers between rail, road, and sea easily using universal gantry cranes. This type of operation is automated in ports, such as the Port of Melbourne and the Port of Rotterdam [20]. Crane operators remotely control the cranes, whilst automated terminal trucks transport the containers to designated areas within the port compounds. Additionally, automated stacker cranes unload/load a container from the terminal truck into the yard for stowage before being transported to its next location. This technology increases productivity and safety by reducing human involvement. Instead, humans are tasked with the job of monitoring and resolving issues within the system to minimise disruption. RFID is one of the technologies used within a port ecosystem to achieve this functionality, allowing the machines to communicate with each other to identify the objects and determine the destination location. RFID tags affixed to objects allow each object to be identified for an array of purposes, assisting with supply chain management to improve the inventory tracking and management of assets. This speeds up port operations by allowing macro objects, such as containers, to be easily identified and can also contain information such as the cargo manifest, source, and destination and even shipping agent/freight forwarder information, providing tracking information to multiple parties along the way (importers, exporters, shipping agents, and freight forwarders). Platforms such as the eSeal [16], record each time a container is opened (unlocked) and can alert officers at a checkpoint if the seal has been tampered with to deter criminal activities such as theft, drug, and people smuggling, which are threats to national security.

Furthermore, RFID solutions are one of the underpinning technologies within Port Community Systems (PCS), a term used to define informational platforms built using technology that connects stakeholders and allows information exchange between parties, bringing significant value to those involved. The primary goal of a PCS is to improve the efficiency and gain competitive advantages within ports. As ports are often compared to one another based on performance metrics, each port strives to be the best. The implementation

of automation technologies and cooperative PCS platforms can benefit all involved with improved delivery accuracy and efficiency [18]. RFID readers are also used as navigational aids around a port. The location at which an RFID tag is read and recorded assists with logistics and tracking cargo on its journey to the end destination.

Finally, RFID tags are frequently used for the purposes of personnel identification and act as keys in access control systems. RFID-enabled identification cards are issued to maritime workers. Access rights or roles are encoded on the tags, and the tags permit access to security gates and doors, thus providing a simple method of authorisation and authentication. An example is the use of Maritime Security Identification Cards (MSIC) within Australia. All maritime workers are required to hold and present a valid MSIC when working within land-side restricted areas to verify that they have the necessary security clearances. MSIC cards are only issued once background checks on the worker have been completed. A commercial example of this technology occurs on cruise ships. Passengers are issued with RFID tags that provide access to different services and amenities on-board—the tag acts as a key to access their room, restaurants, and even payments whilst on-board [39]. The tag may also be used in emergency situations. RFID readers installed on lifeboats can track which passengers have successfully disembarked from the vessel [40].

4. Overview of Existing Lightweight RFID Protocols

In this section, we provide an overview of RFID authentication protocols, focusing on those that are compatible with the constraints described for passive RFID tags (lightweight/ultralightweight protocols). We used various key searches, such as 'Maritime RFID security, Maritime RFID authentication protocols, RFID security maritime', to identify current literature related to our research using various repositories, viz., Google, Google Scholar, and the university library. The search results covered how the technology is utilised within the maritime sector. However, they did not produce work that specifically focused on the overall security aspects, such as the encryption methods utilised and how the devices are authenticated. From the literature, we discovered that low-cost passive RFID technology is commonly used. Therefore, we shifted our focus to the security associated with lightweight authentication protocols that would be compatible with the maritime use cases presented in Section 3. The maritime sector uses RFID technology for personnel identification as well as cargo tracking in the supply chain life cycle [9,14,18].

The following literature review was conducted using a systematic review process. We used keyword searches such as 'lightweight RFID protocols, RFID authentication protocols, RFID security', as our focus was on lightweight and ultralightweight authentication protocols that are suitable for low-cost RFID deployments (passive tags). Due to the resource limitations of passive RFID technology, lightweight/ultralightweight authentications must be used [41]. Other fully-fledged protocols were excluded from this research. In total, 29 lightweight and ultralightweight RFID authentication protocols were evaluated based on their methods of authentication and encryption and their ability to defend against known wireless attacks.

4.1. Protocol Overview

IoT security is one of the top priorities of organisations that wish to leverage this technology. Security mechanisms, such as data encryption, authentication, and the ability to defend against known attacks, are some of the characteristics that are assessed when determining whether a system is secure against potential adversaries. The limited resources available on MIoT devices raise challenges when implementing these security mechanisms without affecting the overall performance and usability of these systems where MIoT devices are embedded. Specific to RFID technology, in over two decades, there have been many approaches proposed to manage the security and privacy of data contained within RFID tags which use a range of both one-way authentication and mutual authentication schemes.

4.2. One-Way Authentication Protocols

The earliest protocol, a Triple DES RFID Authentication Protocol, was proposed in 1997 [42]. The protocol employs three main cryptographic techniques, where plaintext is encrypted using Triple Data Encryption Standard (3DES) 112-bit keys to provide additional security above that of standard DES and double-DES schemes and provide security against brute-force and Man-in-The-Middle attacks. The symmetric key used is obtained from the MD5 (hash-function) generation, which is then encrypted using the RSA method that utilises PKE, providing three levels of defence against potential adversaries, as data are also encrypted during the communication.

An early approach from 2005 is the "kill tag", which has the intent of disabling a tag contained within a product once it has been purchased, therefore rendering the tag unresponsive to RFID readers [43]. Whilst potentially protecting the data, disabling the tag removes its RFID capabilities, which may be an undesirable outcome for some applications.

Choi et al. [44] proposed OHLCAP in 2005 which is a one-way hash-based protocol that uses basic addition and exclusive-or (XOR) operations, making the protocol lightweight and suitable for low-cost RFID solutions. A reader sends a random value to a tag, which is used to perform the computation on the tag. The tag then returns the response to the reader, where additional computation is performed against the data in the back-end database in which the tag's validity is verified. The tag must be authenticated before sensitive information is exchanged. Refreshing the randomly generated value and hash-based encryption protects against possible replays and eavesdropping attacks from potential adversaries.

The Semi-Randomised Access Control (SRAC) Protocol from 2005 described in [43] utilises a hash function to communicate a tag's ID to a reader. If the hashed ID is found in the back-end database, the tag is authenticated, and the tag ID is updated. The back-end system retains a copy of the updated ID and the previous one to prevent desynchronisation attacks; however, it opens the protocol to potential replay attacks. An Advanced SRAC (A-SRAC) Protocol is proposed in [43] to address the concern of a replay attack by implementing a challenge-response process.

The RFID Access Control Protocol, proposed in 2011 [45], builds on the existing hash-based protocols proposed in [46,47] whilst addressing concerns regarding the limitations of previous protocols where tag identification is sent via plaintext, making it susceptible to eavesdropping.

The Slender PUF Protocol 2005 [48] uses physically unclonable functions (PUFs) that are lightweight and compatible with RFID. A strong PUF is incorporated into an RFID tag's circuit board when presented with a challenge; the onboard PUF generates a physically defined output, which serves as the unique identifier. The protocol does not send the full message at once, but rather, sends it in bits in which the verifier is expected to know the response, providing verification and preventing eavesdropping. The protocol is resilient against all known machine-learning attacks.

The Efficient RFID Authentication Protocol (ERAP) proposed by Shen et al. in 2016 [49] is a low-cost RFID protocol that claims to defend against known attacks at a lower cost compared to other protocols [50]. However, a review of the protocols [51] showed that the protocol is also not secure against DOS, MITM, and eavesdropping attacks.

4.3. Mutual Authentication Protocols

Early work in 2003 by Juels et al. proposed a selective blocking protocol [52] that presents the actual value of a tag based on a particular subset of ID codes. They also addressed several "mart" methods for protecting security, including a hash-lock mechanism that hides the tag's identity until a successful PIN or key is presented. Jules proposed the concept of a yoking-proof RFID [53] authentication scheme in 2004 in which two tags are paired together; both entities, in which the keys are pre-shared, must be presented simultaneously to the verifier. If the verifier does not receive the correct information within the allocated time period of 400 ms, authentication is not achieved, and the protocol drops the communication. The Lightweight Mutual Authentication Protocol (LMAP) proposed

by Peris-Lopez et al. in 2006 [54] uses an indexed pseudonym (IDS) to mask the identity of the tag, which is known by authorised readers. If the IDS is identified in the system, the protocol proceeds to generate two encrypted messages using a random number generator (RNG). The tag then attempts to decrypt the encrypted messages. If successful, the IDS is then updated with the new keys created as part of this transaction for the future. The authors note that, due to the tag being re-writable, it is susceptible to data integrity issues. In the event that an attacker is able to modify the tag data, the IDS will no longer be valid, as it would be unknown to the reader, thus, making the protocol susceptible to desynchronisation attacks and forward security attacks [55].

Chien et al. [47] proposed an ultralightweight protocol in 2007 consisting of three stages: tag identification, mutual authentication, and pseudonym/key updating. A tag's ID, pseudonym, and keys are pre-shared with the back-end database. A reader initiates communication in which the tag returns the pseudonym. If the pseudonym is found, the tag proceeds with the mutual authentication step; otherwise, the session is terminated. Once authenticated, the pseudonym and keys are updated, providing robust security against desynchronisation attacks.

In the Chen and Deng protocol [56], RFID tag information remains static on the tag itself and the back-end database, which transfers information to the reader. The use of static information means that the protocol is susceptible to various impersonation and cloning attacks, as identified in [57].

The Mutual Authentication Protocol (MAP), proposed in [58], builds upon the existing pad generation (PadGen) function developed in [59,60] that utilises a tag's access and kill passwords for the foundations of the encryption scheme, which are not encrypted and can be retrieved by eavesdropping. MAP incorporates mutual authentication to improve the security of EPCglobal C1G2 tags [56]. The Cho et al. [61] protocol is based on mutual authentication and a hash function incorporating the use of a 96-bit secret key, and it claims to defend against both privacy and forgery. A cryptanalysis of the protocol by [62] proved that the protocol is susceptible to desynchronisation and impersonation. An ultralightweight authentication protocol proposed by Gao et al. in 2013 [63] aims to reduce the risk of desynchronisation attacks using Cyclic Redundancy Code (CRC) as a lightweight checksum to validate the integrity of the data stored on the tag. As well as permutation, a cryptographic technique re-arranges the characters within a string to hide the source data. The checksum is used to validate the value of the encrypted message against that stored locally on the tag. If incorrect, the tag will not respond and will close communication with the unauthorised reader. A review of RFID protocols shows that this protocol is susceptible to a number of known attacks [51].

The Improved Three-Pass Mutual Authentication (ITMAP) [64] Protocol moves away from PRNG and bitwise logical operations due to the inherent risk of using a single PRNG on a tag. It partners with more robust cryptographic functions on the back-end, which allows for higher computation and can facilitate digital signatures and password-based encryption (PBE). ITMAP is the only protocol that claims to be secure against all known RFID attacks. Additionally, the protocol employs secure controls, such as mutual authentication and asymmetric encryption, which are known standard practices in system security.

The Two-Way Authentication Protocol (TWAP), defined in [65], uses mutual authentication using a hash function between a tag, reader, and database. It is noted that its rapid development will improve overall computation speeds, and the system performance will not be affected. A revised Double PUF-Based Authentication Protocol was proposed in 2017 in [66]. This has similar characteristics to the initial PUF protocol whilst having improved security by utilising a two-stage multiple-choice arbiter (TSMCA). The TSMCA approach uses a string-matching technique during the authentication process that removes the need to share the PUF response with the verifier directly. The Extended Tiny Encryption Algorithm (XTEA) Mutual Authentication Protocol defined in [67] is built using cipher block chaining (CBC) encryption and decryption schemes, primarily using lightweight

XOR operations. When requested by a reader, a tag will generate a pseudo-random number, which is used as the security identifier for the purposes of authentication. The identifier is then encrypted using the XTEA function, which is then transmitted to the reader, where it is decrypted. If the data output matches, the reader and tag are considered to be mutually authenticated. The XTEA function is a block-cipher encryption algorithm similar to DES; however, it uses a much larger key size of 128 bits, using 32-bit arithmetic. The protocol uses a relatively weak formula for encrypting the data; however, the risk of brute-force decryption is mitigated by the number of rounds completed using this method—the larger the number of rounds, the harder it is to decrypt the data.

The findings identified throughout the literature review are summarised in Table 1. We used the following metrics to evaluate each mutual authentication.

- Encryption method(s)s used by the protocol;
- Whether the protocol is susceptible to attack(s);
- Type(s) of authentication employed by the protocol.

The authors of the authentication protocols reviewed in Section 4 used a number of approaches to address security risks associated with passive RFID technology with a common goal of improving the overall performance and security risks associated. Out of the 29 protocols evaluated, only the ITPMAP [64] protocol claims to be able to defend against all known attacks. Given the limitations of the technology, all researchers were faced with similar challenges. Whilst the protocols improved periodically, the majority of the protocols are still susceptible to a number of attacks. A timeline of the protocols evaluated is shown in Figure 2. Given the security risks and issues presented, further work is required to address these shortfalls.

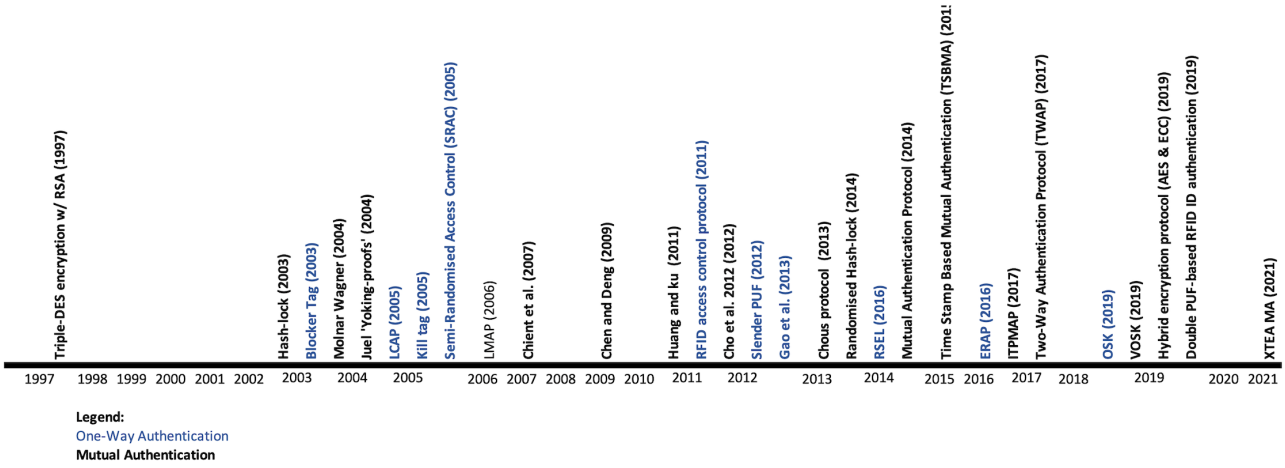

Figure 2. RFID Protocol Development Timeline [30,32,42–45,47–50,52–54,56,58,62–72].

The RFID authentication protocols evaluated in this paper form the foundations of the overall system security in which they are utilised; therefore, the trade-offs and benefits of each protocol must be considered carefully. For example, passive RFID tags are lightweight, cheap to manufacture, and require minimal resources, and hence, they are often considered as a "value for money" option in RFID applications. The trade-off is that these devices have several limitations, namely regarding computing power (resources), which may adversely affect the performance or ability to perform core functions. In essence, it is not always practical to completely eliminate technology based on its setbacks. Instead, focus can be shifted to addressing these risks via alternative controls. To our knowledge, passive RFID continues to be utilised within the area of MIoT after considering the benefits of automation, efficiency, and safety advantages it brings to the maritime industry. As such, our focus is to find the balance between performance and security to improve the security of these systems.

Table 1. RFID Protocol Evaluation. Here "Y " denotes the authentication and encryption types used by the protocol or, whether it is susceptible to each wireless attack.

	Encryption						**Wireless Attacks**										**Authentication**				
	Hash	**Asymmetric**	**Password**	**Symmetric**	**DOS Attack**	**Machine Learning**	**Cloning Attacks**	**Forward Security**	**Desynchronisation Attacks**	**Man-in-the-Middle (MITM)**	**Spoofing Attacks**	**Disclosure Attacks**	**Eavesdropping Attacks**	**Physical Attacks**	**Impersonation**	**Replay Attacks**	**Mutual Authentication**	**Authentication**	**Private Authentication**	**Lightweight**	**Ultralightweight**
One-Way Authentication																					
Blocker Tag [52]			Y				Y	Y						Y		Y					
LCAP [68]								Y	Y							Y		Y			
Kill Tag [43]			Y				Y														
Semi-Randomised Access Control (SRAC) [43]									Y				Y			Y					
RFID Access Control Protocol [45]							Y	Y							Y						
Slender PUF [48]											Y							Y			
Gao et al. [63]							Y		Y	Y			Y		Y			Y			Y
RSEL [50]	Y				Y					Y			Y					Y		Y	
ERAP [49]	Y	Y		Y	Y					Y			Y					Y			
OSK [30]	Y				Y											Y					
Mutual Authentication																					
Triple-DES Encryption w/ RSA [42]		Y						Y								Y		Y			
Hash-Lock [52]	Y									Y	Y						Y				
Molnar Wagner [69]										Y			Y						Y	Y	
Juel 'Yoking-Proofs' [53]	Y															Y					
LMAP [54]				Y				Y	Y											Y	
Chien et al. [47]															Y	Y					
Chen and Deng [56]															Y		Y				
Huang and Ku [58]					Y											Y					
Cho et al. 2012 [44]	Y						Y	Y		Y							Y				
Chou's Protocol [70]								Y													
Randomised Hash-Lock [71]	Y				Y								Y								
Mutual Authentication Protocol [62]					Y		Y	Y									Y				
Time-Stamp-Based Mutual Authentication (TSBMA) [72]	Y				Y												Y				
ITPMAP [64]		Y	Y																		
Two-Way Authentication Protocol (TWAP) [65]	Y								Y				Y				Y				
VOSK [30]	Y				Y																
Hybrid Encryption Protocol (AES & ECC) [32]		Y		Y	Y			Y					Y				Y				
Double PUF-Based RFID ID authentication [66]						Y											Y				
XTEA MA [67]				Y	Y					Y							Y			Y	

4.4. MIoT Suitable Protocols

As alluded to in previous sections of this paper, passive RFID technology is widely used within the maritime sector and is susceptible to the aforementioned attacks. Considering the criticality and dependencies on these systems, this presents a significant threat to the industry. An authentication protocol is the core component of first-layer defence and is paramount to ensuring the confidentiality, integrity, and availability (C.I.A.) of the data and information. Whilst it is nearly impossible to remove all risks entirely, effort should be expended to reduce risk as much as possible. As passive RFID tags do not require direct power, they are small in size, which allows them to be affixed to mobile objects in a way that is not obtrusive and does not impact functionality. Additionally, they are relatively cheap to manufacture, making them cost-effective for large-scale deployments for the purposes of inventory tracking and supply chain logistics within the maritime industry and have additional functionalities above traditional identification practices such as barcodes. However, these attributes also present several disadvantages or trade-offs associated with these low-cost devices. Namely, the lack of power means that the tags must be in close proximity to the reader to be detected. Limited resources hinder their performance and reduce the ability to perform standard security functions, such as AES encryption, that are used in traditional IoT systems. Furthermore, despite these constraints, the technology still has a valid use case within the field; however, further work needs to be undertaken to find the right balance between performance and efficiency without compromising security, specifically for use in MIoT, where the impact of a compromised system has the ability to cause a significant impact.

Therefore, our focus is to strengthen the security landscape for this technology so that the same benefits can be gained without compromising security or performance. Using the information identified as building blocks, we identified the following salient points for MIoT.

1. A tag must be able to identify legitimate and trusted readers to ensure secure communication (e.g., mutual authentication);
2. The authentication protocol must use multiple keys for the encryption and decryption process to improve security between multiple entities (e.g., public-key encryption) to handle several actors (e.g., manufacturers, shipping agents, cargo owners, port authorities, customers, etc.).
3. The authentication protocol must be suitable for passive RFID technology that is commonly used for the above-mentioned scenarios.
4. The authentication protocol must be resistant to known attacks, as covered in Table 1.
5. Data stored on a tag must be encrypted and accessible by trusted sources only.
6. The system should be able to detect and prevent compromised RFID tags from communicating with the network.

From the evaluated RFID protocols summarised in Table 1, there are two protocols in particular that could be considered as potential options to be utilised for maritime RFID solutions, the Improved Three Pass Mutual Authentication Protocol (ITPMAP) [64] and the Triple DES (3DES) with RSA Protocol of Lim et al. [42], with the exception of substituting the 3DES encryption component with a suitable symmetric key encryption, since the DES encryption scheme has been deprecated for some time and has been confirmed to be insecure against a variety of attacks. These two protocols were selected and considered as they best align with the criteria of using mutual authentication and public-key encryption. Mutual authentication is required to validate that each device is legitimate. Devices that are unable to authenticate will be unable to communicate with legitimate devices, increasing the security. Additionally, public-key encryption is essential for communicating with devices owned and managed by different entities, which is often the case in maritime settings, as described in Section 5.2. Additionally, the ITPMAP also claims to defend against all known RFID attacks. Whilst the Triple-DES with RSA Protocol claims to only be susceptible to replay attacks and is unable to provide forward security due to its vulnerability as a

result of using an outdated encryption scheme. We also recommend replacing the 3DES component with a more robust encryption scheme.

5. Our Approach

In this section, we cover our approach to validate that the aforementioned protocols are suitable for the MIoT. From our survey, we observed that the majority of the authentication protocols are susceptible to attacks in one form or another. To improve the security pertaining to maritime logistics and supply chain management, we used the following scenario to examine security issues identified in several authentication protocols and to answer our research question. Do these protocols meet the above conditions, making them suitable for the MIoT?

As alerted to in previous sections of this paper, passive RFID technology is commonly used to collect information about maritime logistics and supply chain management. Several case studies have been presented where RFID tags are affixed to various objects for tracking and object identification. On route to its destination, the RFID tag communicates with several readers. To ensure security, the RFID tag should only interact with legitimate readers to protect the C.I.A of the data using mutual authentication.

5.1. MIoT Scenario

A maritime shipping company (MSC) wants to improve its performance and align the company with Industry 4.0. To achieve this goal, the MSC plans to exploit the use of the IoT to optimise core operations through automation, reducing the administrative overhead and improving the accuracy. The MSC is only one actor in the overall supply chain assisting with the global trade for Australian ports and needs to work with other actors in the supply chain to achieve its goal. In order to understand the current constraints within the supply chain, the MSC plans to use RFID technology for the tracking and identification of global trade (goods and cargo). Due to the large-scale operation, the MSC has decided to opt for passive RFID technology based on its cost and versatility. These RFID tags will be affixed to various objects, such as shipping containers and the inventory of the contents within trucks, trains, and other mobile equipment used, as well as issuing personnel with RFID-enabled identification tags.

The intent is to collect data about the supply chain's life cycle, such as the type of cargo being imported/exported for the automation of manifests and other regulatory reports, such as the origin and destination of cargo. The MSC also intends to track the location of the cargo to confirm that the cargo has met its intended recipient and to measure the dwell times in which the trade is delayed/held up longer than expected. As a result, it also plans to track other actors within the ecosystem, such as trucks, trains, and vessels that are used to transport the material between locations e.g., ports, holding yards, etc. The RFID-enabled ID cards issued to personnel will be used to track and monitor workers and act as keys, linked to the Port Access Control System. Additionally, access may be managed by different entities, depending on the site/location that staff require access to.

For the reasons stated above, the system must be robust and secure against unauthorised access and inappropriate use of the data collected by these systems. The system must also allow data to be used by all relevant actors involved in supply chain management. For example, government and regulatory bodies must monitor the types of cargo for purposes of import/export rules, as per the customs act. Port authorities must manage and control the access linked to the personnel's security identification card to protect the interests of national security. Other entities, such as the shipping agents and freight forwarders, must also be able to read and manage the data stored on these tags.

5.2. Proposed Framework

The implementation of RFID-based solutions for the maritime sector is complex due to the involvement of multiple entities (actors) and the pivotal roles they play within the supply chain. To achieve efficiency, the data and information used within these PCS systems

must be shared for the benefits to be realised. At present, systems in this domain appear to be managed and owned by a single entity. In contrast, our, perhaps more realistic, MIoT scenario focuses on devices owned by multiple entities that need to safely and securely communicate amongst themselves, adding to the complexity. The authentication protocol must be able to meet the core requirements mentioned in Section 4.4 (Salient Points). For example, RFID-based access control systems are currently utilised in Australian ports. RFID-enabled ID tags are issued to personnel and act as a method for authentication. Once authenticated, the tag holder will be permitted to access secure areas if authorised. At present, these ID tags are managed and maintained by a single entity. Our proposed approach will allow multiple entities (such as different companies) to manage and maintain their ID tags and still allow access to various locations managed by separate entities, permitting the ID holder to access multiple locations, whether they are managed by the same entity or not.

Another approach, based on assets rather than people, is object-based tags. In this approach, RFID tags are affixed to physical objects, such as cargo or shipping containers, or mobile plant equipment, such as trucks, trains, and cranes, that may be used to transport cargo in and around port environments. These tags may be required to be read and accessed by multiple port entities as part of the core operations between the departure and arrival destinations and any interim locations visited during the journey.

Thus, the need for a robust and secure authentication protocol that allows a single RFID tag to securely communicate with multiple managed readers is to be established. Essential requirements that should be met for RFID-based systems within the MIoT include the following:

The following diagram, Figure 3, summarises the core requiremenst for an RFID tag to be read and managed by multiple entities from our MIoT use-case scenario presented in Section 5.1. The diagram shows a single, passive RFID tag communicating with multiple RFID readers owned and managed by multiple entities, divided by a wall to represent a secure zone between each entity, as the entities and/or their readers may not communicate with one another directly but communicate with the RFID tag itself as it moves between the zones.

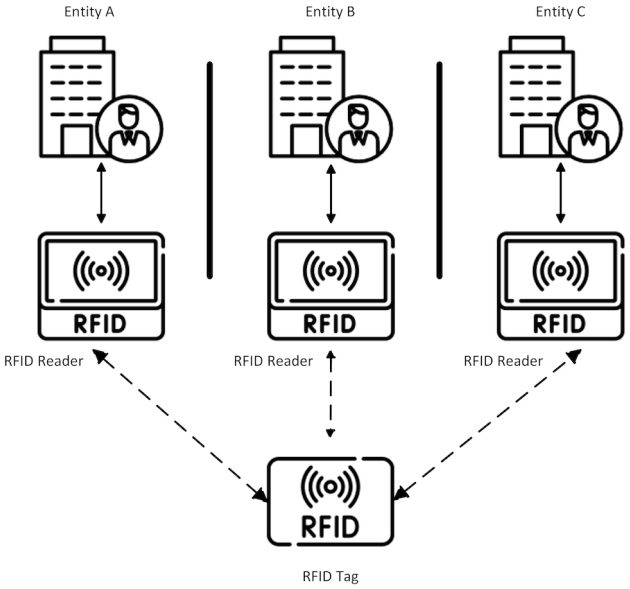

Figure 3. Proposed Port Access Control System.

The solution must implement mutual authentication between the tag and the readers to ensure that communication only occurs between authorised devices. As sensitive information will be embedded within the tag's RFID memory chip, the encryption and

authentication schemes utilised must be secure and protect the information, whilst also being efficient and lightweight.

6. Discussion

RFID technology plays a pivotal role within the maritime sector and is used in several areas to improve the efficiency of daily operations through data collection and automation [40,73]. Given the analysis in Table 1, it is obvious that there are security concerns with current RFID authentication protocols, which have a flow-on effect for data processed within MIoT systems. A compromised RFID system can provide adversaries with access to sensitive information or can disrupt port and maritime operations, leaving a lasting impact that can severely affect the global economy and cause a threat to national security. Unfortunately, previous work surrounding the implementation of RFID technology within the maritime domain specifically focused on the technology itself, the system architecture, or how the system can be utilised without taking the security aspects of the overall system into consideration. A comprehensive review of RFID protocols was completed by [51]. This paper extended that work by focusing specifically on lightweight protocols suitable for passive RFID. Additionally, some extant research addresses security [30,74,75]. The focus is on RFID systems built for a singular entity using encryption methods, such as password-based encryption. These types of encryption scenarios are not suitable for real-world implementations (e.g., shipping containers where data must be read by third parties, such as port authorities and customs, as they require sensitive information, such as the password/encryption keys, to be shared with all stakeholders. As such, the sharing of secrets is not an effective or secure way of permitting access to the data, and these tasks cannot be achieved at this level whilst maintaining appropriate security controls. Nonetheless, the research shows that these protocols are still susceptible to several known attacks.

7. Future Work

This paper highlights the current security concerns related to RFID security protocols and the additional concerns for critical infrastructure use cases, such as those operating in the maritime domain. Extensive efforts are needed to strengthen the current security protocols for widely used RFID technologies, namely, passive RFID tags. A strong, secure, and robust Mutual Authentication Protocol for RFID technology is mandatory to protect the sensitive data currently transmitted by these systems to eliminate or mitigate the threat from potential adversaries. The authentication protocol must also include the ability to detect compromised tags communicating with trusted devices to prevent backdoor access and possible malicious damage. Significant work is also required to implement a secure authentication protocol for RFID systems shared by multiple parties.

To determine whether the selected protocols are viable options for the MIoT specifically, we intend to use the above Port Access Control System presented in Section 5.2 to evaluate the protocols based on performance and their ability to defend against known RFID attacks from potential adversaries. The performance will be assessed based on the computation cost, communication cost, and storage requirements of the protocol.

8. Conclusions

The primary objective of this paper was to improve the security around RFID technology currently used within the MIoT. The present security issues identified in several of the authentication protocols cause great concern in terms of the overall risk of the data captured and utilised by these systems. The maritime industry continues to leverage RFID technology in efforts to optimise and improve core operations. As shown, many of the existing RFID protocols are susceptible to various types of attack; yet, the technology still continues to be used in a variety of applications. Security threats raise major concerns in MIoT implementations where data security and privacy is of the utmost importance due to the disastrous outcomes that could be caused by exploiting known vulnerabilities. For example, compromised RFID systems could lead to unauthorised access to secure areas,

thereby facilitating disruptions and impacting the global economy, especially since 90% of the world's freight moves by sea. In summary, we identified an imperative need to improve security for RFID-based systems used by the maritime industry and intend to do so by adapting these protocols to address a real-world use case. This will be followed by a security review and analysis of the protocols.

Author Contributions: Conceptualization, G.M. and H.C.; methodology, G.M.; literature review, G.M.; formal analysis, G.M.; writing—original draft preparation, G.M.; writing—review and editing, G.M., H.C. and M.N.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research project (Investigating the Practicability of RFID Protocols for Secure Communications in Maritime IoT) was supported by the Defence Science Centre, an initiative of the State Government of Western Australia under grant (DSCID 2223R4RHDSG004).

Data Availability Statement: All data is included in this paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Carnarius, J. Modes of Transportation Explained: Which Type of Cargo and Freight Transportation is the Best? *Freighthub. Blogi.* **2018**. Available online: https://freighthub.com/en/blog/modes-transportation-explained-best (accessed on 29 April 2023).
2. Shipping Australia Report. Factsheet on the Transport of Australian Import & Export Cargoes by Shipping Australia. 2020. Available online: https://shippingaustralia.com.au/wp-content/uploads/2020/11/SAL20048-FACT-SHEET-ON-AUSTRALIAN-TRADE-by-SAL-1.pdf (accessed on 29 January 2023).
3. Corbett, J.J.; Winebrake, J.; Endresen, E.; Eide, M.; Dalsøren, S.; Isaksen, I.S.; Sørgård, E. *International Maritime Shipping: The Impact of Globalisation on Activity Levels*; Globalisation, Transport and the Environment; OECD Publishing: Paris, France, 2010; pp. 55–79.
4. Hahn, G.J. Industry 4.0: A supply chain innovation perspective. *Int. J. Prod. Res.* **2020**, *58*, 1425–1441. [CrossRef]
5. Alifragki, M.E. Cyber—Attacks: The New Type of Piracy in the Maritime World. Ph.D. Thesis, University of Piraeus, Pireas, Greece, 2019.
6. Jones Walker. *2022 Ports and Terminals Cybersecurity Survey*; Jones Walker: Columbia, FL, USA, 2022.
7. Daffron, J.; Ruffle, S.; Coburn, A.; Copic, J.; Quantrill, K.; Strong, K.; Leverett, E. *Shen Attack: Cyber Risk in Asia Pacific Ports*; Cambridge Centre for Risk Studies: Cambridge, MA, USA, 2019.
8. Xia, T.; Wang, M.M.; Zhang, J.; Wang, L. Maritime Internet of Things: Challenges and Solutions. *IEEE Wirel. Commun.* **2020**, *27*, 188–196. [CrossRef]
9. Jones, E.C.; Chung, C.A. Marine RFID Security Applications. In *RFID and Auto-ID in Planning and Logistics*; CRC Press: Boca Raton, FL, USA, 2011; pp. 345–354. [CrossRef]
10. Kelly, P. A novel technique to identify AIS transmissions from vessels which attempt to obscure their position by switching their AIS transponder from normal transmit power mode to low transmit power mode. *Expert Syst. Appl.* **2022**, *202*, 117205. [CrossRef]
11. Spravil, J.; Hemminghaus, C.; von Rechenberg, M.; Padilla, E.; Bauer, J. Detecting Maritime GPS Spoofing Attacks Based on NMEA Sentence Integrity Monitoring. *J. Mar. Sci. Eng.* **2023**, *11*, 928. [CrossRef]
12. Cankar, M.; Stanovnik, S. *Maritime IoT Solutions in Fog and Cloud*; IEEE: Piscataway Township, NJ, USA, 2018; pp. 284–289. [CrossRef]
13. Standifer, C. RF a struggle for unmanned systems: Cargo UAV Will Likely Face Problems with Radio Jamming in Theater. *Inside Pentagon Inside Navy* **2011**, *24*, 3.
14. Plaza-Hernández, M.; Gil-González, A.B.; Rodríguez-González, S.; Prieto-Tejedor, J.; Corchado-Rodríguez, J.M. *Integration of IoT Technologies in the Maritime Industry*; Advances in Intelligent Systems and Computing; Springer International Publishing: Cham, Germany, 2020; pp. 107–115. [CrossRef]
15. Pakistan Gulf Economist. *Ransomware Attack Takes US Maritime Base Offline*; Pakistan Gulf Economist: Karachi, Pakistan, 2020; Volume 39.
16. Xiaoning, S.; Dongkai, T.; Stefan, V. RFID Technology and its Application to Port-Based Container Logistics. *J. Organ. Comput. Electron. Commer.* **2011**, *21*, 332–347. [CrossRef]
17. Wang, J.; Xiao, Y.; Li, T.; Chen, C.L.P. A Survey of Technologies for Unmanned Merchant Ships. *IEEE Access* **2020**, *8*, 224461–224486. [CrossRef]
18. Dowgiewicz, K. How Technology Can Advance Port Operations and Address Supply Chain Disruptions. Ph.D. Thesis, Pepperdine University, Malibu, CA, USA, 2022.
19. Bogićević, D.; Tot, I.; Prodanović, R.; Todorović, B. Identification of soldiers and weapons in military armory based on comparison image processing and RFID tag. *Vojnoteh. Glas.* **2021**, *69*, 179–195. [CrossRef]
20. Swash, D.R. Port Automation: The Route to the Future. *E-J. Ports Termin.* **2021**, *10*, 8–10.

21. Supply Chain Market. US Naval Supply Systems Command (NAVSUP) expands supply chain use of passive RFID at Pearl Harbor Naval and Marine Corps Hawaiian bases. *RFID (Radio Freq. Identif.) Newsl.* **2008**, *5*, 1. Available online: https://www.supplychainmarket.com/doc/us-naval-supply-systems-command-navsup-expand-0001 (accessed on 5 February 2023).
22. Yau, K.A.; Peng, S.; Qadir, J.; Low, Y.; Ling, M.H. Towards Smart Port Infrastructures: Enhancing Port Activities Using Information and Communications Technology. *IEEE Access* **2020**, *8*, 83387–83404. [CrossRef]
23. Kumar, A.; Jain, A.K.; Dua, M. A comprehensive taxonomy of security and privacy issues in RFID. *Complex Intell. Syst.* **2021**, *7*, 1327–1347. [CrossRef]
24. Baig, Z.; Szewczyk, P.; Valli, C.; Rabadia, P.; Hannay, P.; Chernyshev, M.; Johnstone, M.; Kerai, P.; Ibrahim, A.; Sansurooah, K.; et al. Future challenges for smart cities: Cyber-security and digital forensics. *Digit. Investig.* **2017**, *22*. [CrossRef]
25. Satyajit Sinha. Number of Connected IoT Devices Growing 9% to 12.3 bn Globally. 24 May 2023. Available online: https://iot.electronicsforu.com/content/tech-trends/number-of-connected-iot-devices-growing-9-to-12-3-bn-globally/ (accessed on 1 June 2023).
26. Talwana, J.C.; Hua, H.J. Smart World of Internet of Things (IoT) and Its Security Concerns. In Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, 15–18 December 2016.
27. Tewari, A.; Gupta, B.B. Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. *Future Gener. Comput. Syst.* **2020**, *108*, 909–920. [CrossRef]
28. Khwaja, M.; Ghani, A.; Shehzad Ashraf, C.; Shamshirband, S.; Shahbaz Ahmed Khan, G.; Mosavi, A. Securing IoT-Based RFID Systems: A Robust Authentication Protocol Using Symmetric Cryptography. *Sensors* **2019**, *19*, 4752. [CrossRef]
29. Wang, Y.; Liu, X.; Wang, Y.; Wang, H.; Wang, H.; Zhang, S.L.; Zhao, T.; Xu, M.; Wang, Z.L. Flexible Seaweed-Like Triboelectric Nanogenerator as a Wave Energy Harvester Powering Marine Internet of Things. *ACS Nano* **2021**, *15*, 15700–15709. [CrossRef]
30. Liu, D.; Yang, G.; Huang, Y.; Wu, J. Inductive Method for Evaluating RFID Security Protocols. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 2138468. [CrossRef]
31. Yousuf, Y.; Potdar, V. A Survey of RFID Authentication Protocols. In Proceedings of the 22nd International Conference on Advanced Information Networking and Applications—Workshops (Aina Workshops 2008), Gino-wan, Japan, 25–28 March 2008; pp. 1346–1350. [CrossRef]
32. Farooq, U.; Ul Hasan, N.; Baig, I.; Shehzad, N. Efficient adaptive framework for securing the Internet of Things devices. *EURASIP J. Wirel. Commun. Netw.* **2019**, *2019*, 210. [CrossRef]
33. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
34. Wang, S.; Zhang, B. Research on Security Protocol of RFID System Based on Public Key Cryptography. *J. Phys. Conf. Ser.* **2019**, *1237*, 22134. [CrossRef]
35. Rivest, R. RFC 1321: The MD5 message-digest algorithm, April 1992. In *Status: Informational*; RFC Editor: Marina del Rey, CA, USA, 2014.
36. Gupta, P.; Kumar, S. A comparative analysis of SHA and MD5 algorithm. *Architecture* **2014**, *1*, 4492–4495.
37. Gope, P.; Hwang, T. A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system. *Comput. Secur.* **2015**, *55*, 271–280. [CrossRef]
38. Fraga-Lamas, P.; Varela-Barbeito, J.; Fernandez-Carames, T.M. Next Generation Auto-Identification and Traceability Technologies for Industry 5.0: A Methodology and Practical Use Case for the Shipbuilding Industry. *IEEE Access* **2021**, *9*, 140700–140730. [CrossRef]
39. Royal Caribbean. Royal Caribbean Cruise Ship Adopts RFID Technology to Enhance Comfort and Security. 26 July 2015. Available online: https://www.rfidsolutionsonline.com/doc/royal-caribbean-cruise-ship-adopts-rfid-technology-enhance-comfort-security-0001 (accessed on 15 May 2022).
40. Andreadakis, A.; Sloane, T.F.; Dalaklis, D. An Automated Lifeboat Manifesting Embarkation System (ALMES): Optimizing Evacuation and Passenger Manifestation Via RFID/NFC. *TransNav* **2021**, *15*, 215–221. [CrossRef]
41. Gao, M.; Lu, Y. URAP: A new ultra-lightweight RFID authentication protocol in passive RFID system. *J. Supercomput.* **2022**, *78*, 10893–10905. [CrossRef]
42. Lim, G.C.L.; Arada, G.P.; Abad, A.C.; Magsino, E.R. RFID Tag Data Encryption Using Triple DES and RSA Algorithms. *J. Phys. Conf. Ser.* **2021**, *1997*, 012028. [CrossRef]
43. Lee, Y.K.; Verbauwhede, I.M.R. Secure and Low-cost RFID Authentication Protocols. In Proceedings of the 2nd IEEE Workshop on Adaptive Wireless Networks, Lake Vista, FL, USA, 24 August 2005.
44. Choi, E.Y.; Lee, S.M.; Lee, D.H. Efficient RFID Authentication Protocol for Ubiquitous Computing Environment. In *Embedded and Ubiquitous Computing—EUC 2005 Workshops*; Enokido, T., Yan, L., Xiao, B., Kim, D., Dai, Y., Yang, L.T., Eds.; Springer Berlin/Heidelberg, Germany, 2005; pp. 945–954.
45. Chen, Y.Y.; Tsai, M.L.; Jan, J.K. The design of RFID access control protocol using the strategy of indefinite-index and challenge-response. *Comput. Commun.* **2011**, *34*, 250–256. [CrossRef]
46. Weis, S.A.; Sarma, S.E.; Rivest, R.L.; Engels, D.W. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In *Security in Pervasive Computing*; Springer: Berlin/Heidelberg, Germany, 2004; Volume 2802.

47. Chien, H.Y. SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity. *IEEE Trans. Dependable Secur. Comput.* **2007**, *4*, 337–340. [CrossRef]
48. Majzoobi, M.; Rostami, M.; Koushanfar, F.; Wallach, D.S.; Devadas, S. Slender PUF Protocol: A Lightweight, Robust, and Secure Authentication by Substring Matching. In Proceedings of the 2012 IEEE Symposium on Security and Privacy Workshops, San Francisco, CA, USA, 20–23 May 2012; pp. 33–44. [CrossRef]
49. Shen, J.; Tan, H.; Moh, S.; Chung, I.; Wang, J. An Efficient RFID Authentication Protocol Providing Strong Privacy and Security. *J. Internet Technol.* **2016**, *17*, 443–455. [CrossRef]
50. Fan, K.; Li, J.; Li, H.; Liang, X.; Shen, X.; Yang, Y. RSEL: Revocable secure efficient lightweight RFID authentication scheme. *Concurr. Comput. Pract. Exp.* **2014**, *26*, 1084–1096. [CrossRef]
51. Ibrahim, A.; Dalkılıç, G. Review of different classes of RFID authentication protocols. *Wirel. Netw.* **2019**, *25*, 961–974. [CrossRef]
52. Juels, A.; Rivest, R.; Szydlo, M. The blocker tag: Selective blocking of RFID tags for consumer privacy. In Proceedings of the CCS03: Tenth ACM Conference on Computer and Communications Security 2003, Washington, DC, USA, 27–30 October 2003; pp. 103–111. [CrossRef]
53. Juels, A. Yoking-proofs for RFID tags. In Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, Orlando, FL, USA, 14–17 March 2004; pp. 138–143. [CrossRef]
54. Peris-Lopez, P.; Hernandez-Castro, J.; Tapiador, J.; Ribagorda, A. LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags. In Proceedings of the 2nd Workshop on RFID Security, Graz, Austria, 12–14 July 2006.
55. Raju, M.H.; Ahmed, M.; Ahad, M.A.R. MUMAP: Modified Ultralightweight Mutual Authentication protocol for RFID enabled IoT networks. *J. Inst. Ind. Appl. Eng.* **2021**, *9*, 33–39. [CrossRef]
56. Chen, C.L.; Deng, Y.Y. Conformation of EPC Class 1 Generation 2 standards RFID system with mutual authentication and privacy protection. *Eng. Appl. Artif. Intell.* **2009**, *22*, 1284–1291. [CrossRef]
57. Kapoor, G.; Piramuthu, S. Vulnerabilities in Chen and Deng's RFID mutual authentication and privacy protection protocol. *Eng. Appl. Artif. Intell.* **2011**, *24*, 1300–1302. [CrossRef]
58. Huang, Y.J.; Jiang, C.H.; Wu, H.H.; Hong, Y.H.; Liu, K.J. Mutual Authentication Protocol for RFID System. In Proceedings of the 2011 14th IEEE International Conference on Computational Science and Engineering, Dalian, China, 24–26 August 2011; IEEE: Piscataway Township, NJ, USA, 2011; pp. 73–80. [CrossRef]
59. Huang, H.H.; Ku, C.Y. A RFID Grouping Proof Protocol for Medication Safety of Inpatient. *J. Med. Syst.* **2008**, *33*, 467. [CrossRef]
60. Konidala, D.M.; Kim, Z.; Kim, K. A Simple and Cost-effective RFID Tag-Reader Mutual Authentication Scheme. In Proceeding of the 2007 IEEE International Conference on RFID, Gaylord Texan Resort, Grapevine, TX, USA, 26–28 March 2007; IEEE: Piscataway Township, NJ, USA, 2007; pp. 141–152.
61. Cho, J.S.; Yeo, S.S.; Kim, S.K. Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value. *Comput. Commun.* **2011**, *34*, 391–397. [CrossRef]
62. Safkhani, M.; Peris-Lopez, P.; Hernandez-Castro, J.C.; Bagheri, N. Cryptanalysis of the Cho et al. protocol: A hash-based RFID tag mutual authentication protocol. *J. Comput. Appl. Math.* **2014**, *259*, 571–577. [CrossRef]
63. Lijun, G.; Maode, M.; Yantai, S.; Yuhua, W. An ultralightweight RFID authentication protocol with CRC and permutation. *J. Netw. Comput. Appl.* **2014**, *41*, 37–46. [CrossRef]
64. Younis, M.I.; Abdulkareem, M.H. ITPMAP: An Improved Three-Pass Mutual Authentication Protocol for Secure RFID Systems. *Wirel. Pers. Commun.* **2017**, *96*, 65–101. [CrossRef]
65. Yu, W.; Jiang, Y. Mobile RFID Mutual Authentication Protocol Based on Hash Function. In Proceedings of the 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Nanjing, China, 12–14 October 2017; pp. 358–361. [CrossRef]
66. Liang, W.; Xie, S.; Long, J.; Li, K.C.; Zhang, D.; Li, K. A double PUF-based RFID identity authentication protocol in service-centric internet of things environments. *Inf. Sci.* **2019**, *503*, 129–147. [CrossRef]
67. Anusha, R.; Shastrimath, V.V.D. RFID-MA XTEA: Cost-Effective RFID-Mutual Authentication Design Using XTEA Security on FPGA Platform. *Int. J. Electron. Telecommun.* **2021**, *67*, 623. [CrossRef]
68. Su-Mi, L.; Young Ju, H.; Dong Hoon, L.; Jong In, L. Efficient Authentication for Low-Cost RFID Systems. In Proceedings of the Computational Science and Its Applications—ICCSA 2005: International Conference, Singapore, 9–12 May 2005.
69. Molnar, D.A.; Wagner, D.A. Privacy and security in library RFID: Issues, practices, and architectures. In Proceedings of the 11th ACM Conference on Computer and Communications Security, Washington, DC, USA, 25–29 October 2004.
70. Chou, J.S. An efficient mutual authentication RFID scheme based on elliptic curve cryptography. *J. Supercomput.* **2014**, *70*, 75–94. [CrossRef]
71. Dehkordi, M.H.; Farzaneh, Y. Improvement of the Hash-Based RFID Mutual Authentication Protocol. *Wirel. Pers. Commun.* **2014**, *75*, 219–232. [CrossRef]
72. Changlun, Z.; Wenqi, Z.; Haibing, M. A Mutual Authentication Security RFID Protocol Based on Time Stamp. In Proceedings of the 2015 First International Conference on Computational Intelligence Theory, Systems and Applications (CCITSA), Ilan, Taiwan, 10–12 December 2015; pp. 166–170.
73. Fu, H.; Sun, F. Benefit and Cost of RFID Technology to Container Ports A Competitive Perspective. *J. Coast. Res.* **2020**, *106*, 494–497. [CrossRef]

74. Mohamad Noor, M.B.; Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. *Comput. Netw.* **2019**, *148*, 283–294. [CrossRef]
75. Pateriya, R.K.; Sharma, S. The Evolution of RFID Security and Privacy: A Research Survey. In Proceedings of the 2011 International Conference on Communication Systems and Network Technologies, Katra, India, 3–5 June 2011; IEEE: Piscataway Township, NJ, USA, 2011; pp. 115–119. [CrossRef]