sustainability

MDPI

Article

AIS Meets IoT: A Network Security Mechanism of Sustainable Marine Resource Based on Edge Computing

Han-Chieh Chao [1], Hsin-Te Wu [2] and Fan-Hsun Tseng [3,*]

[1] Department of Electrical Engineering, National Dong Hwa University, Hualien 974301, Taiwan; hcc@mail.ndhu.edu.tw
[2] Department of Computer Science and Information Engineering, National Ilan University, Yilan 260007, Taiwan; hsinte@niu.edu.tw
[3] Department of Technology Application and Human Resource Development, National Taiwan Normal University, Taipei 10610, Taiwan
* Correspondence: fhtseng@ntnu.edu.tw

Abstract: The sustainable utilization of marine resources is a vital issue to enrich marine life and to prevent species extinction caused by overfishing. Nowadays, it is common that commercial and smaller vessels are equipped with an Automatic Identification System (AIS) and GPS for better vessel tracking to avoid vessel collision as well as mayday calls. Additionally, governments can monitor vessels' sea activities through AIS messages, stopping them from overfishing or tracking if any vessel has caused marine pollution. However, because AIS devices cannot guarantee data security, they are susceptible to malicious attacks such as message modification or an illegitimate identity faking a distress signal that causes other vessels to change their course. Given the above, a comprehensive network security system of a sustainable marine environment should be proposed to ensure secure communication. In this paper, a stationary IoT-enabled (Internet of Things) vessel tracking system of a sustainable marine environment is proposed. The system combines network security, edge computing, and tracking management. It offers the following functions: (1) The IoT-based vessel tracking system tracks each aquafarmer's farming zone and issues periodic warning to prevent vessel collision for pursuing a sustainable marine environment; (2) the system can serve as a relay station that evaluates whether a vessel's AIS data is correct; (3) the system detects abnormal behavior and any irregular information to law enforcement; (4) the system's network security mechanism adopts a group key approach to ensure secure communication between vessels; and (5) the proposed edge computing mechanism enables the tracking system to perform message authentication and analysis, and to reduce computational burden for the remote or cloud server. Experiment results indicate that our proposed system is feasible, secure, and sustainable for the marine environment, and the tendered network security mechanism can reduce the computational burden while still ensuring security.

Keywords: automatic identification system; bilinear pairings; edge computing; internet of things; network security; sustainable marine environment

Citation: Chao, H.-C.; Wu, H.-T.; Tseng, F.-H. AIS Meets IoT: A Network Security Mechanism of Sustainable Marine Resource Based on Edge Computing. *Sustainability* **2021**, *13*, 3048. https://doi.org/10.3390/su13063048

Academic Editor: Ilsun You

Received: 26 January 2021
Accepted: 5 March 2021
Published: 10 March 2021

1. Introduction

The goal of the sustainable utilization of marine resources is to maintain marine life to a certain level and avoid severe marine pollution from aquaculture or vessels. Marine aquatic resources have, as a result of increased human population and climate changes, been on a steep decline. As of current, the global marine catch totals between 85 to 93 million metric tonnes per year [1], nevertheless, excessive fish catching can exhaust marine resources, which is why countries around the globe have, in recent years, been vehemently promoting aquaculture—especially because aquaculture might be the solution to creating an ample and reliable supply that will meet market needs. In the past, aquatic farms used to be land-based so as to lower costs, many sought out groundwater for water resources, and

the overpumping led to land subsidence problem, e.g., in Bangkok [2], in Shanghai [3], and in Mekong Delta [4]. With these in mind, many countries today are instead pushing for offshore aquaculture practices such as offshore cage farming. The practice of offshore aquaculture calls for zone management and cultivation monitoring so authorities can prevent aquafarmers from over-expanding their zone while monitoring whether a zone has been contaminated. Offshore aquafarmers, on the other hand, rely on radio communication and other forms of warning to prevent other vessels from colliding into their cultivation zone. For instance, in cage farming, when there is a typhoon, cages might get relocated to areas less impacted by the weather, which creates issues of zone management, moreover, warnings must be issued during said relocation for collision avoidance.

In light of all this, an offshore IoT-enabled (Internet of Things) vessel tracking system is much called for. Such a system can help keep track of each aquafarmer's cultivation zone at all times while monitoring whether any such zone has been expanding or relocating its cages, moreover, government officials can utilize the IoT platform to effectively track and monitor offshore aquaculture zones, all the while reducing marine pollution and vessel collision.

Most vessels nowadays come with an Automatic Identification System (AIS) communication system, which is mainly used to locate the position of nearby vessels via GPS for collision avoidance. An AIS system's GPS feature also helps the vessel with day-to-day navigation and specific procedures like entering a port. Nevertheless, because an AIS system is not encryption-protected in terms of data security [5] and identity authentication [6], it may fall prey to message modification attacks such as a launch of false distress signals or collision warnings. Moreover, a malicious party may initiate a denial-of-service attack to meltdown AIS communication while it carries out illegal activities. An AIS system downloads marine forecast information from the nearest marine authority however, if the AIS system and the facility in question fail to establish information security between them, this may give rise to various problems. For instance, if a hacker modifies weather forecast information, then vessels might be manipulated into taking detour or crowding a port for shelter. Hence, it is crucial for an AIS system to have a comprehensive network security mechanism that ensures message authentication, integrity, and non-repudiation.

The approach in [7] was to utilize multi-access edge computing for computation and storage purposes, reducing the burden on the cloud or fog computing. The authors in [8] constructed a computational model using mobile edge computing and cloud or fog computing that came with a security mechanism to ensure data security and in addition, the model requires the flexibility for future expansion. In [9], the authors applied fog and mobile-edge computing to a mobile networking framework for pursuing a sustainable and innovative cellular network. The paper utilized hesitant fuzzy soft sets to resolve the defined multi-criteria decision making problem. With AIS communication, the system receives a plethora of data on other vessels however, since these are data that have never undergone encryption or message authentication, the system needs edge computing for data validation, for instance, determining whether a vessel is traveling at a reasonable speed or whether it has malicious intentions. To vessels that exhibit malicious behavior, the system reports them to the authority and as for legitimate vessels, their data is stored via cloud or fog computing, but the edge computing can effectively relieve the computational burden on the cloud and fog computing with the added ability of processing real-time information.

This paper introduces an edge computing-based network security mechanism for AIS-enabled IoT devices. Our proposed scheme offers the following advantages: (1) Farming zone management can be accomplished using the offshore IoT vessel tracking system, which also warns vessels about nearby farming zones via AIS communication to help prevent collision; (2) the AIS-tailored network security mechanism safeguards message authentication, integrity, and non-repudiation during all AIS communication; and (3) our use of edge computing to filter messages blocks malicious messages from causing vessel collision or course manipulation. Under this mechanism, the system first applies IoT technology to authenticate any AIS communication and then encrypts the message with

bilinear pairing before sending it to the cloud server. If the system detects a maliciously modified message or fake message, it notifies the pertaining legal authority for further action. In the paper, message authentication covers two aspects: (1) Message integrity, for which we employ hash technologies to authenticate the integrity of a message, and (2) message validation, for which we examine GPS message contents to determine whether a vessel is issuing fake messages. For instance, if a vessel's anticipated course, distance, or speed does not match its corresponding data in GPS messages, then the system calls out this fake message. Our system adopts a group key approach in inquiring vessels whether they have truly engaged in collision. The experiment results indicate that our proposed mechanism is not only feasible but also practically applicable. The choice of applying lightweight cryptography in the network security mechanism is to reduce computational complexity for edge computing and lighten the load for cloud computing.

2. Related Works

One of edge computing's most appealing advantage is that it opens a door to better real-time service. Edge computing can offer users real-time service while easing the computational burden on fog computing. However, one challenge for edge computing is the potentially heavy load of computation, thus many researchers have devised solutions to improve computational capabilities [10–12]. In [10], the authors applied EdgeFlow in mobile edge computing for data offloading. When tasks are evenly distributed to individual edge devices, this not only prevents any single edge device from being overwhelmed with computational tasks but accomplishes real-time service at the same. In [11], the authors worked on integrating edge computing with IoT to reinforce trust between IoT devices. In the past, IoT devices were usually independent equipment that processed information services single-handedly, which put a cap on how much loading it could handle. By introducing edge computing and reinforcing the trust mechanism between devices, the IoT devices become able to process large amounts of computation and gain better computational capabilities. The paper [12] adopted many Small Cell Base Stations (SBS) for edge computing. SBS gives advantage because it is effective in data reception from different communication equipment and subsequent service computing and because it can perform distributed computing. These SBS features hugely improve edge computing's efficacy.

Several studies address the issue of framework compatibility. The work of [13] offers a comprehensive illustration of the differences in terms of framework and application among cloud, IoT, edge, and fog computing. The authors in [14] combined software-defined networking with edge computing technology. The problem of compatibility stems from facts such as cloud and fog computing work under different frameworks. The common users hold a myriad of communication devices that somewhat differ in network structure. The use of software-defined networking to accomplish network cloudification and integration with edge computing can effectively solve the problem of framework compatibility.

Some researchers [15–18] are dedicated to resolving issues in resource allocation and latency. The authors in [15] proposed a smart manufacturing computing framework. The paper applies a threshold greedy algorithm to determine resource requirements and computational capability, which significantly improves smart manufacturing's effectiveness in resource allocation. Meanwhile, the authors of [16] advocated that integrating edge computing into smart manufacturing yields a computational speed faster than that in fog or cloud computing. Additionally, edge computing can tailor task assignment individually for each smart device, increasing the efficacy of resource allocation. In [17], the authors analyzed resource allocation in edge computing and introduced a mobile edge computing intrusion detection system. The paper used Lyapunov functions to prove the system's stability, and the test yielded very promising results. The authors in [18] suggested integrating edge computing into IoT devices to improve the quality of service. The paper also proposed a novel idea concerning task allocation in edge computing that would elevate the IoT device's computational capabilities while reducing latency issues.

This work of [19] discussed data security protection in edge computing. The authors mentioned that edge computing currently lacks protection against security, making it susceptible to cyberattacks and data breaches. Hence, edge computing is in need of lightweight encryption to safeguard its data security. The authors in [20] adopted an ID-based distributed authentication of data. For any given party, they need only the other party's ID to apply bilinear pairings for an authentication of legitimacy, which would subsequently verify the data's integrity and authentication. Another proponent of ID-based cryptography, the paper [21] applied ID-based encryption to construct a privacy and data security mechanism for vehicular ad hoc networks. Through an ID-based mechanism, the system was able to effectively generate anonymous IDs for vehicles, and when a vehicle engages in illegal activity, the system is capable of tracing that vehicle's real ID. Meanwhile, the paper [22] uses bilinear pairings to generate data signatures that could effectively authenticate the data's accuracy. Also adopting pairing-based cryptography, the authors [23] used bilinear pairings to create a security mechanism that does not make use of public/private key authentication. It can counteract the processing time wasted in public/private key authentication while still providing comprehensive security.

In our proposed system, we adopt bilinear pairings to construct a network security mechanism that integrates edge computing for the purpose of verifying data authenticity. In addition, the system utilizes IoT devices to conduct farming zone management in offshore aquatic farms. Our proposed system can serve as a relay station that assists vessels in the open sea with message authentication, enhancing the security of AIS communication systems and safety at sea for vessels.

3. Background

In this section, we will discuss the cryptographic techniques and concepts featured in this paper, including bilinear pairings and group key, and introduce our proposed system model.

3.1. Bilinear Pairings

Suppose G_1 and G_2 are additive groups and multiplicative groups, and they are both of the same prime order q. P, Q is G_1's generator and the bilinear pairing function is $e : G_1 \times G_1 \rightarrow G_2$. Then the bilinear pairings are defined as follows [24,25]:

(1) Bilinear: $a, b, c \in Z_q^*$ and $S, Y \in G_1$; $e(ab \cdot P, c \cdot P) = e(abc \cdot P, P) = e(P, P)^{abc}$; $e(S + Y, P) = e(S, P)e(P, Y)$ for all $P \in G_1$;
(2) Non-degeneracy: $P \in G_1$ such that $e(P, P) \neq 1$;
(3) Computable: There exists an efficient algorithm to compute $e(S, Y)$, for $S, Y \in G_1$.

In [26], bilinear pairings were successfully applied as an encryption method. The work of [27] took a step further and accomplished fast encryption using bilinear pairings in an embedded system. In this paper, we employed ID-based Cryptography (IBC) [28] for identity authentication. IBC is created on the basis of bilinear pairings. Two parties must each have a private key that uses the same secret key and subsequently, one side needs only to obtain their counterpart's ID to generate a public key. Then, this party takes their own private key and their counterpart's public key to create a bilinear map, which establishes a common session key that both sides can use for Symmetric Encryption (SE) of data.

3.2. Group Key: Basic Concepts

Our proposed system uses group key to generate the public/private keys between a vessel within range and the IoT vessel tracking system. Furthermore, the public/private keys are then used for encryption in data transmission and generating a common session key.

Suppose the IoT vessel tracking system is $I_1 \sim I_n$. I_1's group public key is $\mathcal{PKG}_{\mathbb{ID}_{I_1}} = \mathbb{ID}_{I_1} \cdot P$; I_1's group private key is $\mathcal{PRG}_{\mathbb{ID}_{I_1}} = \mathbb{ID}_{I_1} \cdot r^s \cdot P$; I_1's group public value is $\mathcal{PUG}_{\mathbb{ID}_{I_1}} = r^{\frac{1}{s}} \cdot P$; I_1's group Hash-based Message Authentication Code (HMAC) public value is $\mathcal{PUHG}_{\mathbb{ID}_{I_1}} = e\left(r^{\frac{1}{u}} \cdot P, \mathbb{ID}_{I_1}\right)$. Following all this, the vessel AIS communication

systems are represented by $F_1 \sim F_n$. I_1 will generate, for $F_1 \sim F_n$, their public key $\left(\mathcal{PKG}_{\mathbb{ID}_{F_1 \sim F_n}} = \mathbb{ID}_{F_1 \sim F_n} \cdot P\right)$, private key $\left(\mathcal{PRG}_{\mathbb{ID}_{F_1 \sim F_n}} = \mathbb{ID}_{F_1 \sim F_n} \cdot r^s \cdot P\right)$, and group public value $\left(\mathcal{PUG}_{\mathbb{ID}_{F_1 \sim F_n}} = r^{\frac{1}{s}} \cdot P\right)$. $F_1 \sim F_n$ will send its secret key (v) to I_1 and it will serve as HMAC's key. Upon calculation, I1 will give $F_1 \sim F_n$ their group HMAC public value $\left(\mathcal{PUHG}_{\mathbb{ID}_{F_1 \sim F_n}} = r^{\frac{1}{uv}} \cdot P\right)$.

When I_1 and F_1 want to establish a common session key $\left(\mathcal{SK}_{\mathbb{ID}_{I_1 \leftrightarrow F_1}}\right)$, they only need their own private key and the other party's public key to generate it. The computation is $\mathcal{SK}_{\mathbb{ID}_{I_1 \leftrightarrow F_1}} = e\left(\mathcal{PRG}_{\mathbb{ID}_{I_1}}, \mathcal{PKG}_{\mathbb{ID}_{F_1}}\right) = e\left(\mathcal{PKG}_{\mathbb{ID}_{I_1}}, \mathcal{PRG}_{\mathbb{ID}_{F_1}}\right)$. The two parties can simply use $\mathcal{SK}_{\mathbb{ID}_{I_1 \leftrightarrow F_1}}$ to process symmetric encryption. If F_1 wants to broadcast a message (M) to other vessels, F_1 can use $\mathcal{PUG}_{\mathbb{ID}_{F_1 \sim F_n}}$ to compute a HMAC and then use $v = a * b$, a as HMAC's session key while it releases a, $b \cdot P$, and $\mathcal{PUHG}_{\mathbb{ID}_{F_1 \sim F_n}} = r^{\frac{1}{uv}} \cdot P$. Upon receiving the HMAC, other vessels can compute $e\left(\mathcal{PUHG}_{\mathbb{ID}_{F_1 \sim F_n}}, \mathbb{ID}_{I_1} ab \cdot P\right) = e\left(\mathbb{ID}_{I_1} r^{\frac{v}{uv}} \cdot P, P\right)$, followed by using $e\left(\mathbb{ID}_{I_1} r^{\frac{v}{uv}} \cdot P, P\right) = \mathcal{PUHG}_{\mathbb{ID}_{I_1}}$ to determine whether there is a match. If it is indeed a match, then it confirms that the message was sent by F_1 and that F_1 is a legitimate user. Table 1 is an illustration of the symbols employed in this paper.

Table 1. Summary of notations and symbols.

Notation	Representation of the Symbol or Symbol
P	the generator of G_1.
Q	the generator of G_1.
$\mathbb{ID}_u$	the real ID of the user u.
G_1	the additive group.
G_2	the multiplicative group.
s, v, c	A random number $s, v, c \in Z_q^*$ chosen as the master key where Z_q^* is a finite field of order q.
$\mathcal{SK}$	the common session key.
$\mathcal{SE}_{\mathbb{ID}_u}$	the symmetric encryption of user u.
e	the bilinear map.
H	the hash function.
M	the message or smart contract.
$\mathcal{PRG}_{\mathbb{ID}_u}$	the group private key of user u.
$\mathcal{PKG}_{\mathbb{ID}_u}$	the group public key of user u.
$\mathcal{PUG}_{\mathbb{ID}_u}$	the group public value of user u.
$\mathcal{PUHG}_{\mathbb{ID}_u}$	the group HMAC public value of user u.
$\mathcal{PR}_{\mathbb{ID}_u}$	the private key of user u.
$\mathcal{PK}_{\mathbb{ID}_u}$	the public key of user u.
$\mathcal{PU}_{\mathbb{ID}_u}$	the public value of user u.
$\mathcal{T}$	the timestamp of user u.

3.3. System Model

Figure 1 is an illustration of our proposed scheme. In this paper, we installed maritime positioning sensors ($R_{1,1} \sim R_{n,n}$) on the offshore aquafarm. These sensors utilize AIS communication to periodically broadcast messages that notify other vessels of the location of this stationary farm. Moreover, they help government units conduct offshore aquafarming management. Each of $I_1 \sim I_n$ represents one IoT vessel tracking system, which receives data via AIS communication and has access to 5G network. After $I_1 \sim I_n$ receives GPS data from $R_{1,1} \sim R_{n,n}$, the system judges whether there has been any change to the farming zone.

Meanwhile, $I_1 \sim I_n$ also collects AIS communication data from all vessels and proceeds to determine whether every piece of information is correct. If any anomaly is detected,

the system submits a warning to fog computing on the other hand, legitimate data is collected and then transmitted to fog computing. Our proposed communication method processes all message transmission using a network security mechanism. The proposed method utilized edge computing technologies to perform anomaly detection on the AIS communication data. Anomalies are reported to fog computing while managing authorities are notified for further actions. Our approach can effectively reduce the computational burden in fog computing. This paper judges a data packet's validity by the vessel's AIS system without the necessity of transmitting every packet to the cloud system or server for authentication, which will reduce the computing and communication workloads of the cloud system or server, enabling the AIS system to achieve the technical capacity that is comparable to edge computing. When the AIS system notices an abnormal packet, it will send the packet to the fog networking for storage and government agency reports and edge computing can reduce fog storage and distribute the calculation loading to each AIS system.

4. The Proposed Scheme

In this section, we will discuss five topics: Message signature and symmetric encryption (Section 4.1), group message broadcasting (Section 4.2), group key updates (Section 4.3), tracking management system (Section 4.4), and edge computing (Section 4.5).

4.1. System Initialization and Group Symmetric Encryption

By applying bilinear pairings, the paper constructed an all-around network security mechanism. Suppose TA is an impartial government unit. The system will first compute security coefficient of TA and $I_1 \sim I_n$, such as the public and private keys, using the following equations:

(1) TA chooses $c \in Z_q^*$ as the secret key; r represents the public value.
(2) TA's ID is $\mathbb{ID}_{TA}$ for which the public key is $\mathcal{PK}_{\mathbb{ID}_{TA}} = \mathbb{ID}_{TA} \cdot P$ and the private key is $\mathcal{PR}_{\mathbb{ID}_{TA}} = r^c \cdot \mathbb{ID}_{TA} \cdot P$.
(3) TA's public value is $\mathcal{PU}_{\mathbb{ID}_{TA}} = r^{\frac{1}{c}} \cdot P$.

Next, we compute the public key and private key of $I_1 \sim I_n$ using the following equation:

(1) In's public key is $\mathcal{PK}_{\mathbb{ID}_{I_n}} = \mathbb{ID}_{I_n} \cdot P$;
(2) In's private key is $\mathcal{PR}_{\mathbb{ID}_{I_n}} = r^c \cdot \mathbb{ID}_{I_n} \cdot P$.

$I_1 \sim I_n$ represents TA-authenticated, legitimate stationary IoT equipment. The next step for $I_1 \sim I_n$ is to configure security coefficient such as group public key. For $F_1 \sim F_n$. If F_n wishes to send private messages to I_1, then I_1's group public key can be deduced from I_1's ID. F_n can use its own $\mathcal{PRG}_{\mathbb{ID}_{F_1}}$ to compute a common session key using the equation:

$$\mathcal{SK}_{\mathbb{ID}_{I_1 \leftrightarrow F_1}} = e\left(\mathcal{PRG}_{\mathbb{ID}_{I_1}}, \mathcal{PKG}_{\mathbb{ID}_{F_1}}\right) = e\left(\mathcal{PKG}_{\mathbb{ID}_{I_1}}, s \cdot \mathcal{PKG}_{\mathbb{ID}_{F_1}}\right). \quad (1)$$

Following the above, F_1 applies Symmetric Encryption (SE) using $\mathcal{SE}_{\mathcal{SK}_{\mathbb{ID}_{I_1 \leftrightarrow F_1}}}(M||T_i)||H(M||T_i)$ before transmitting the message to I_1. Upon receiving the encrypted text, I_1 will first compute the common session key. Then, it will decrypt $\mathcal{SE}_{\mathcal{SK}_{\mathbb{ID}_{I_1 \leftrightarrow F_1}}}(M||T_i)$ and authenticate whether the decrypted contents $H(M||T_i)'$ and $H(M||T_i)$ are a match. If they are identical, it indicates message integrity. Since s is known only to I1, no other user can uncover s using their private key. In sum, $\mathcal{SK}_{\mathbb{ID}_{I_1 \leftrightarrow F_1}}$ is known only to F_1 and I_1.

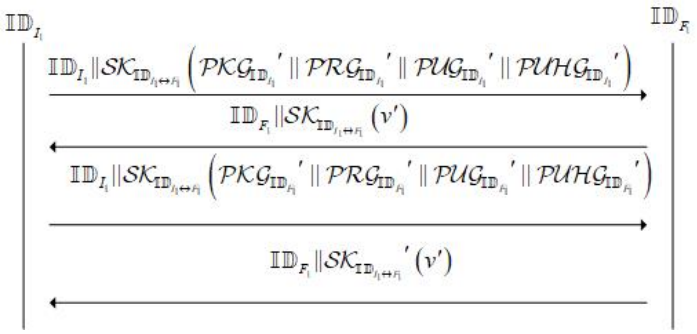
4.2. Group Message Broadcasting

The paper designed a group message broadcasting system for communication between stationary IoT devices or vessels in a group. Under our scheme, if, for instance, F_1 wants to relay vessel information to other vessels and devices in the group, then F_1 must first compute $b = \frac{v}{a}$ as well as the broadcast message $HMAC_a(M||T_i)||M||a||b \cdot P||T_i||\mathcal{PUHG}_{\mathbb{ID}_{F_1}}$.

Then, F_1 will broadcast the message to all the vessels in the group. Upon reception, the other vessels begin to authenticate whether the message indeed came from F_1 by computing $e\left(\mathcal{PUHG}_{\mathbb{ID}_{F_1 \sim Fn}}, \mathbb{ID}_{I_1} ab \cdot P\right) = e\left(\mathbb{ID}_{I_1} r\frac{v}{uv} \cdot P, P\right)$, in which $e\left(\mathbb{ID}_{I_1} r\frac{v}{uv} \cdot P, P\right) = \mathcal{PUHG}_{\mathbb{ID}_{I_1}}$. If the result is positive, then it confirms that the identity is authentic because only I_1 knows $r\frac{1}{u}$. Additionally, only F_1 knows v, which helps prove that the message was really relayed by F_1. Meanwhile, F_1 undergoes HMAC decryption to compute the integrity and if the result is correct then it is an indication that the message has not been modified.

4.3. Group Key Update

$I_1 \sim I_n$ regularly updates the key of each vessel in the group in order to prevent a secret key from overexposure and brute force attacks. Meanwhile, if a group member turns out malicious, engaging in false message relay, then in order to prevent this malicious vessel from flooding and interfering the system with a vast number of false messages, every member in every pair within $I_1 \sim I_n$ will use the common session key unique to themselves and another paired member in $I_1 \sim I_n$ to update its security coefficient using the following computation:



First of all, I_1 uses $\mathcal{SK}_{\mathbb{ID}_{I_1 \leftrightarrow F_1}}$ to encrypt the new security coefficient before submitting it to F_1, next, F_1 computes the new v', encrypts it using $\mathcal{SK}_{\mathbb{ID}_{I_1 \leftrightarrow F_1}}$, and sends it back to I_1. At this point, I_1 recalculates and generates F_1's new group key, which I_1 then encrypts using $\mathcal{SK}_{\mathbb{ID}_{I_1 \leftrightarrow F_1}}$ and transmits it to F_1. Upon reception, F_1 decrypts and uses that new group key to generate a new common session key, $\mathcal{SK}'_{\mathbb{ID}_{I_1 \leftrightarrow F_1}}$, which F_1 encrypts and sends to I_1. Once I_1 has successfully decrypted and confirmed the message's authenticity, the group key update is now complete.

4.4. Tracking Management System

The offshore aquaculture tracking system in this paper utilizes AIS communication and GPS sensors to track and position an aquatic farm. As shown in Figure 1, this work installed stationary IoT devices $I_1 \sim I_n$ by the shore. These devices carry two types of wireless communication technologies—one is AIS communication and the other one is 5G network. $I_1 \sim I_n$ obtains the GPS location of tracking devices $R_{1,1} \sim R_{n,n}$ via AIS communication. $R_{1,1} \sim R_{n,n}$ issues AIS notification messages to other vessels, helping them avoid collision or entering a farming zone. Additionally, $I_1 \sim I_n$ are also capable of calculating whether $R_{1,1} \sim R_{n,n}$ have been moved using the Algorithm 1.

Here, $GA'_{Ra_{i,i}}$ stands for the previously obtained GPS location while $GA_{Ra_{i,i}}$ represents the current GPS location. D represents the distance function of these two locations while $GA_{Ra_{i,i}}$ represents the speed as shown in the GPS data. Given the impact of wave motions in the sea, it may cause $R_{1,1} \sim R_{n,n}$ to move within a slight range. With help from our tracking management system, we first determine whether the difference between the GPS location and the current location is greater than the threshold. If yes, then it is indication that the aquafarmer is expanding their farming zone, which can lead to disputes between farmers over farming zones and fish products. Another issue that can benefit from the

tracking management system is that, during certain weather conditions, some aquafarmers will haul their farm to a zone less impacted by the weather. However, if they are to move their farm, they should notify the managing authority to prevent collision into other vessels. Last but not least, the managing authority can have knowledge of when and where a farm is being hauled to through our tracking system.

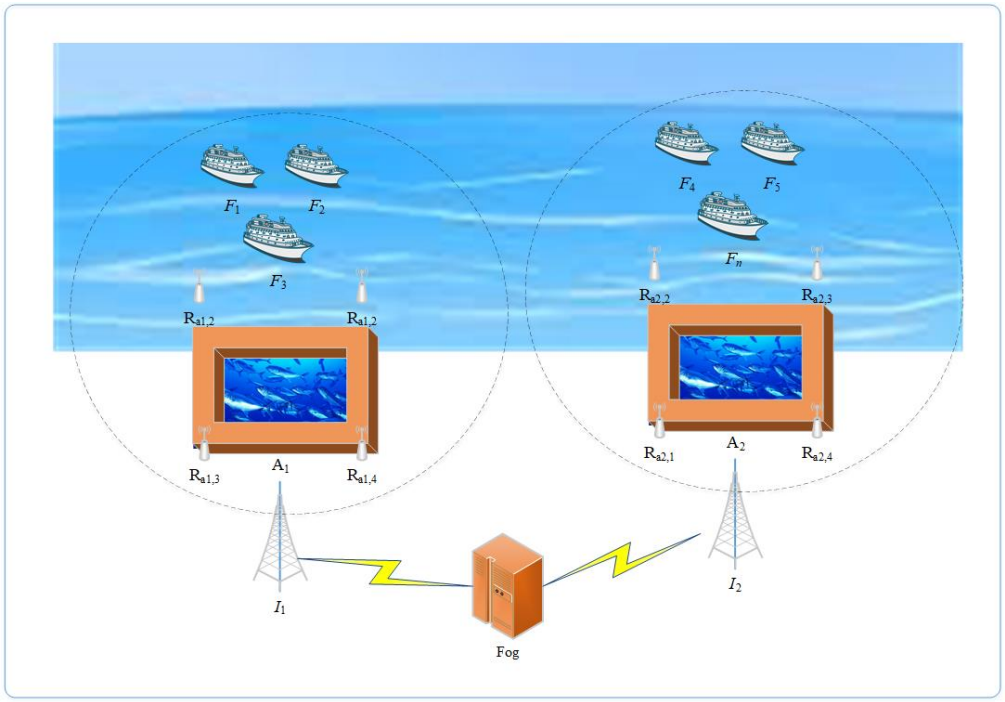


Figure 1. System illustration.

Algorithm 1 Determine whether the farming zone has shifted.

if $D\left(GA'_{Ra_{i,i}}, GA_{Ra_{i,i}}\right) > Threshold$ **then**
  Issue warning and notify the managing authority
else
  Safe
end if
Determine whether the speed in the GPS data is above the threshold value; if yes, then the aquatic farm is on the move
if $GS_{Ra_{i,i}} > Threshold$ **then**
  Issue warning and notify the managing authority
else
  Safe
end if

4.5. Edge Computing

The paper utilizes edge computing to determine whether any AIS communication data is trustworthy. An AIS system stores GPS data that serves mainly for the purpose of positioning a vessel. These GPS data include information such as vessel position, speed, and course. This work makes use of such GPS data as well as signal frequency as a referential tool to help identify and prevent malicious vessels from launching false signal attacks and interference. Our system will first identify the vessel's speed. This is because vessels generally travel at a fixed speed hence, if there exists a speed difference between earlier and later data, and that difference is greater than the threshold value, then the system judges it an anomaly. The system then issues warnings and notifies the authority. The determination is based on the Algorithm 2.

Algorithm 2 Determination of vessel speed.

Determine whether the difference between GPS-based speed from before and after is above the threshold value
if $\left(GS'_{F_1} - GS_{F_1}\right) > Threshold$ **then**
Issue warning and notify the managing authority
else
Safe
end if

Here, GS_{F_1} stands for vessel F_1's speed as per the GPS data. Next, the system determines the vessel's course. The rationale is that a vessel's course can hardly make a swift turn of a significant angle. The algorithm applied here is Algorithm 3.

Algorithm 3 Determination of GPS-based heading angles.

Determine whether the difference between the GPS-based heading angles is greater than the threshold value
if $\left(G\theta'_{F_1} - G\theta_{F_1}\right) > Threshold$ **then**
Issue warning and notify the managing authority
else
Safe
end if

Here, $G\theta_{F_1}$ stands for vessel F_1's speed as shown in the GPS data. If a vessel issues an abnormal distress signal, the system will compute the number of times that the vessel's AIS communication system has transmitted any data. If the number of times is scarce and yet it is calling for help, then the system issues a warning for the detection of anomaly. Under our proposed scheme, $I_1 \sim I_n$ will transmit data on $F_1 \sim F_n$ to TA, but TA only needs to store the data and not perform additional computation, which reduces computing in TA.

5. Performance

In this section, we will discuss edge computing and offer a performance analysis as well as network security analysis.

5.1. Edge Computing: Performance Analysis

Figure 2 presents the hardware equipment employed in our proposed system. Figure 2a shows the offshore aquaculture tracking system while Figure 2b shows the offshore data reception terminal. The offshore data reception terminal relies mainly on AIS communication and is also connected to an IoT development board for processing edge computing. The data along with the processing results are uploaded for fog computing. We can see from Figure 3 that our system's use of edge computing results in a lighter packet load than that in directly applying fog computing. When the number of offshore aquaculture tracking systems increases, as illustrated in Figure 2, it significantly raises fog computing's packet load. As seen from the above, by having the offshore data reception terminal help with computation, it reduces the computational burden in fog computing. Figure 4 is a demonstration of our proposed analysis system, which is capable of knowing whether a tracking system has been moved.

(**a**) Offshore aquaculture tracking system.

(**b**) Offshore data reception terminal.

Figure 2. Hardware model of the offshore tracking system.

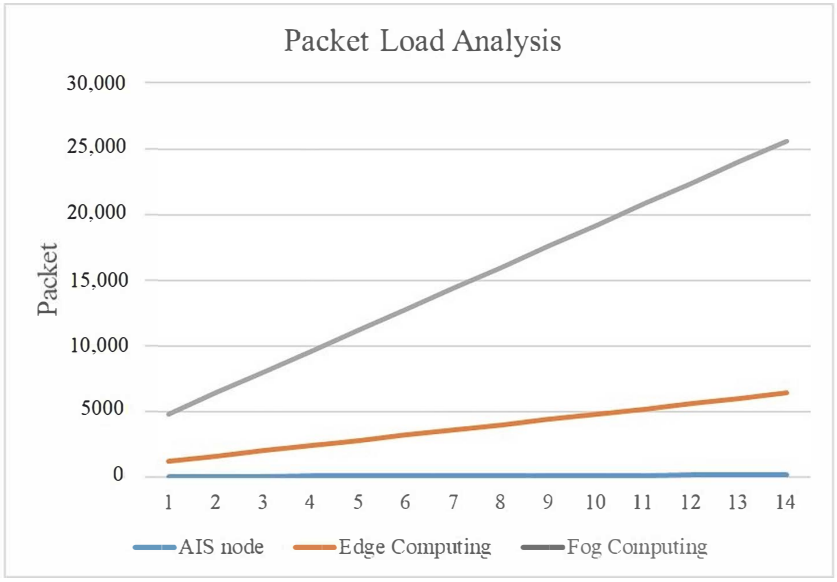


Figure 3. Edge computing: Packet load analysis.

Figure 4. Analysis platform.

5.2. Network Security Analysis

The network security analysis offered here is based on the encryption/decryption computation time listed in Table 2. The encryption/decryption computation time was calculated using the computational complexity approach mentioned in [29–31]. We also conducted a comparative analysis of different network security mechanisms in this work and in [22,23]. The analysis results are illustrated in Table 3. In terms of identity authentication, all three studies opted for non-symmetric bilinear pairings as the approach for authentication and transmission of security coefficients. In terms of private communication, the studies in [22,23] continue to employ non-symmetric bilinear pairings. By contrast, our proposed method chose to apply IBC for private communication and consequently, we used symmetric cryptography to encrypt the messages. As for message authentication in [22], users utilize digital signatures to run message authentication. A user generates signature using their private key and public value and afterwards, other users can use their public value to verify the signature. The paper [23] employs pairing operation and point multiplication to encrypt and verify signatures. This work uses field exponentiation and pairing operation to generate a HMAC key. Other users use the HMAC public value for key computation and if the verification is successful, then it verifies the data origin. HMAC can also be used to verify data integrity. Our proposed scheme uses $ab \cdot P$ to generate the HMAC key. Even if other users obtain knowledge of a and $\mathcal{PUHG}_{\mathbb{ID}_{F_1 \sim F_n}}$, they will still not have access to b, which is why our proposed system ensures the data origin, privacy, and integrity in AIS communication.

Table 2. Execution time in milliseconds.

Notation	Description	Execution Time (ms)
T_p	Pairing operation	≈4.5
T_m	Point multiplication	≈0.6
T_e	Field exponentiation	≈0.45
H	Hash-based message authentication code	0.002
S_e	Advanced Encryption Standard encryption	<0.19
S_d	Advanced Encryption Standard decryption	<4.65

Table 3. Effectiveness analysis.

Property / Method	[22]	[23]	The Proposed Scheme
Identity Authentication	Encryption: $T_p + T_e$ Decryption: $T_p + T_e$ Spending time: 10.08 (ms)	Encryption: $T_p + T_e$ Decryption: $T_p + T_e$ Spending time: 10.08 (ms)	Encryption: $T_p + T_e$ Decryption: $T_p + T_e$ Spending time: 10.08 (ms)
Private communication	Encryption: $T_p + T_e$ Decryption: $T_p + T_e$ Spending time: 10.08 (ms)	Encryption: $T_p + T_e$ Decryption: $T_p + T_e$ Spending time: 10.08 (ms)	Encryption: SE Decryption: Sd Spending time: 4.84 (ms)
Message Authentication	Signing: $2*T_p$ Verification: $2*T_p + 2*T_e$ Spending time: 18.9 (ms)	Signing: $3*T_p$ Verification: $3*T_p$ Spending time: 27 (ms)	Signing: T_p Verification: $T_p + T_e$ +H Spending time: 9.47 (ms)

6. Conclusions

With global population growth, the demand for fish products has been increasing gradually. For accomplishing the aspiration of the sustainable utilization of marine resources, many farmers have developed mariculture for growing fish yield. This article monitored vessels and mariculture areas by AIS. When vessels approach a farming zone, the farming zone requires warnings to prevent vessels from colliding into farms. To solve the above-mentioned problem, the paper provided an AIS-based warning mechanism of a sustainable marine environment.

The highlight of our proposed system is the network security mechanism that utilizes the GPS data available in an AIS system for message detection to determine the reasonability of a vessel's data. Our approach is to apply bilinear pairings in constructing a specific network security mechanism for sustainable marine. The advantages of our system include safeguarded authentication in terms of data origin, privacy, and integrity. Moreover, in order to relieve computational burden on fog computing, we introduced edge computing to help process and determine data accuracy, thus only if the data is accurate will it be uploaded in batches to fog computing. The upside is that fog computing now only needs to store the data and not conduct additional computing.

We put the proposed system to practice in actual operation, and the testing results proved that our system could effectively reduce fog computing's computational burden. Furthermore, our proposed network security mechanism is capable of successful processing within reasonable computation time for a secure and sustainable marine environment. For each piece of broadcast information, it only took the system 9.47 ms to complete signature and authentication. In sum, our system is a mechanism of lightweight security and it can effectively ensure secure communication with vessels for the sustainable marine.

Author Contributions: Conceptualization, H.-C.C.; validation, H.-C.C.; formal analysis H.-T.W.; writing—original draft, H.-T.W.; writing—review and editing, F.-H.T. All authors have read and agreed to the published version of the manuscript.

Funding: This work was financially supported from the Young Scholar Fellowship Program by Ministry of Science and Technology (MOST) in Taiwan, under Grant MOST109-2636-E-003-001, and was partly funded by the MOST in Taiwan, under grant MOST109-2511-H-259-004.

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

References

1. Food and Agriculture Organization of the United Nations. *The State of World Fisheries and Aquaculture 2020*; Sustainability in Action: Rome, Italy, 2020.
2. Phien-wej, N.; Giao, P.; Nutalaya, P. Land subsidence in Bangkok, Thailand. *Eng. Geol.* **2006**, *82*, 187–201. [CrossRef]
3. Shen, S.L.; Xu, Y.S. Numerical evaluation of land subsidence induced by groundwater pumping in Shanghai. *Can. Geotech. J.* **2011**, *48*, 1378–1392. [CrossRef]
4. Erban, L.E.; Gorelick, S.M.; Zebker, H.A. Groundwater extraction, land subsidence, and sea-level rise in the Mekong Delta, Vietnam. *Environ. Res. Lett.* **2014**, *9*, 084010. [CrossRef]
5. Arifin, B.; Ross, E.; Brodsky, Y. Data security in a ship detection and Identification System. In Proceedings of the 5th International Conference on Recent Advances in Space Technologies—RAST2011, Istanbul, Turkey, 9–11 June 2011; pp. 634–636. [CrossRef]
6. Su, P.; Sun, N.; Zhu, L.; Li, Y.; Bi, R.; Li, M.; Zhang, Z. A Privacy-Preserving and Vessel Authentication Scheme Using Automatic Identification System. In Proceedings of the Fifth ACM International Workshop on Security in Cloud Computing, Abu Dhabi, United Arab Emirates, 2 April 2017; pp. 83–90.
7. Taleb, T.; Samdanis, K.; Mada, B.; Flinck, H.; Dutta, S.; Sabella, D. On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 1657–1681. [CrossRef]
8. Shirazi, S.N.; Gouglidis, A.; Farshad, A.; Hutchison, D. The Extended Cloud: Review and Analysis of Mobile Edge Computing and Fog From a Security and Resilience Perspective. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 2586–2595. [CrossRef]
9. Rathore, S.; Sharma, P.K.; Sangaiah, A.K.; Park, J.J. A Hesitant Fuzzy Based Security Approach for Fog and Mobile-Edge Computing. *IEEE Access* **2017**, *6*, 688–701. [CrossRef]
10. Wang, P.; Yao, C.; Zheng, Z.; Sun, G.; Song, L. Joint Task Assignment, Transmission, and Computing Resource Allocation in Multilayer Mobile Edge Computing Systems. *IEEE Internet Things J.* **2019**, *6*, 2872–2884. [CrossRef]
11. Yuan, J.; Li, X. A Reliable and Lightweight Trust Computing Mechanism for IoT Edge Devices Based on Multi-Source Feedback Information Fusion. *IEEE Access* **2018**, *6*, 23626–23638. [CrossRef]
12. Chen, L.; Zhou, S.; Xu, J. Computation Peer Offloading for Energy-Constrained Mobile Edge Computing in Small-Cell Networks. *IEEEACM Trans. Netw.* **2018**, *26*, 1619–1632. [CrossRef]
13. Donno, M.D.; Tange, K.; Dragoni, N. Foundations and Evolution of Modern Computing Paradigms: Cloud, IoT, Edge, and Fog. *IEEE Access* **2019**, *7*, 150936–150948. [CrossRef]
14. Baktir, A.C.; Ozgovde, A.; Ersoy, C. How Can Edge Computing Benefit From Software-Defined Networking: A Survey, Use Cases, and Future Directions. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2359–2391. [CrossRef]
15. Li, X.; Wan, J.; Dai, H.N.; Imran, M.; Xia, M.; Celesti, A. A Hybrid Computing Solution and Resource Scheduling Strategy for Edge Computing in Smart Manufacturing. *IEEE Trans. Ind. Inform.* **2019**, *15*, 4225–4234. [CrossRef]
16. Qi, Q.; Tao, F. A Smart Manufacturing Service System Based on Edge Computing, Fog Computing, and Cloud Computing. *IEEE Access* **2019**, *7*, 86769–86777. [CrossRef]
17. Hui, H.; Zhou, C.; An, X.; Lin, F. A New Resource Allocation Mechanism for Security of Mobile Edge Computing System. *IEEE Access* **2019**, *7*, 116886–116899. [CrossRef]
18. Guo, M.; Li, L.; Guan, Q. Energy-Efficient and Delay-Guaranteed Workload Allocation in IoT-Edge-Cloud Computing Systems. *IEEE Access* **2019**, *7*, 78685–78697. [CrossRef]
19. Xiao, Y.; Jia, Y.; Liu, C.; Cheng, X.; Yu, J.; Lv, W. Edge Computing Security: State of the Art and Challenges. *Proc. IEEE* **2019**, *107*, 1608–1631. [CrossRef]
20. Wang, H. Identity Based Distributed Provable Data Possession in Multicloud Storage. *IEEE Trans. Serv. Comput.* **2015**, *8*, 328–340. [CrossRef]
21. He, D.; Zeadally, S.; Xu, B.; Huang, X. An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2681–2691. [CrossRef]
22. Tsai, J.L. A New Efficient Certificateless Short Signature Scheme Using Bilinear Pairings. *IEEE Syst. J.* **2017**, *11*, 2395–2402. [CrossRef]
23. Du, H.; Du, H.; Wen, Q. A Provably-Secure Outsourced Revocable Certificateless Signature Scheme Without Bilinear Pairings. *IEEE Access* **2018**, *6*, 73846–73855. [CrossRef]
24. Scott, M. Computing the Tate Pairing. In Proceedings of the Cryptographers' Track at the RSA Conference, San Francisco, CA, USA, 20–24 April 2005; pp. 293–304.

25. Boneh, D.; Franklin, M. Identity based encryption from the Weil pairing. In Proceedings of the Advances in Cryptology CRYPTO 2001, Santa Barbara, CA, USA, 19–23 August 2001; pp. 213–229.
26. Galbraith, S.D.; Harrison, K.; Soldera, D. Implementing the Tate Pairing. In Proceedings of the 5th International Symposium on Algorithmic Number Theory, Sydney, Australia, 7–12 July 2002; pp. 324–337.
27. Azarderakhsh, R.; Fishbein, D.; Grewal, G.; Hu, S.; Jao, D.; Longa, P.; Verma, R. Fast Software Implementations of Bilinear Pairings. *IEEE Trans. Dependable Secur. Comput.* **2017**, *14*, 605–619. [CrossRef]
28. Du, X.; Wang, Y.; Ge, J.; Wang, Y. An ID-based broadcast encryption scheme for key distribution. *IEEE Trans. Broadcast.* **2005**, *51*, 264–266. [CrossRef]
29. Wang, Q.; Li, X.; Yu, Y. Anonymity for Bitcoin From Secure Escrow Address. *IEEE Access* **2017**, *6*, 12336–12341. [CrossRef]
30. Scott, M. Efficient Implementation of Cryptographic Pairings. 2007. Available online: http://ecrypt-ss07.rhul.ac.uk/Slides/Thursday/mscottsamos07.pdf (accessed on 25 January 2021).
31. Devegili, A.J.; Scott, M.; Dahab, R. Implementing Cryptographic Pairings over Barreto-Naehrig Curves. In Proceedings of the International Conference on Pairing-Based Cryptography, Tokyo, Japan, 2–4 July 2007; pp. 197–207.