J Inf Process Syst, Vol.15, No.1, pp.217~232, February 2019
https://doi.org/10.3745/JIPS.04.0105

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Digitalization of Seafarer's Book for Authentication and e-Navigation

Jun-Ho Huh* and Kyungryong Seo**

Abstract

Currently, the crew working on a ship is required to carry a seafarer's book in most countries around the world, including the Republic of Korea (ROK). Yet, many fishermen working in the international waters of the ROK do not abide by this rule as the procedure of obtaining it is rather inconvenient or they do not understand the necessity or the benefits of having it. Also, as the regulation of carrying the certificate has been strengthened, it is important for them to avoid making a criminal record unintentionally. This study discusses the digitalization of the seafarer's book based on several security measures in addition to BLE Beacon-based positioning technology, which can be useful for the e-Navigation. Normally, seamen's certificates are recorded by the captain, medical institution, or issuing authority and then kept in an onboard safe or a certificate cabinet. The material of the certificates is a cloth that can withstand salinity as the certificate could be contaminated by mold. In the past, the captains and their crews were uncooperative when the ROK's maritime police tried to inspect several ships simultaneously because of the time and cost involved. Thus, a system with which the maritime police will be able to conveniently manage the crews is proposed.

Keywords

Android Application, Authentication, Digitalization, e-Navigation, Parallel Computing, Seafarer's Book, Seaman Service Book, System Architecture

1. Introduction

This research discusses the method of digitalization of ID cards for identification and authentication. Currently, many firms are using digitalized ID cards for their security or monitoring purposes.

The executive officers on a ship are required to individually carry seafarer's books, which used to be recognized as a passport [1–5]. However, the fisherman or the crew who are working in the ROK's coastal waters do not need to carry the certificate, but the captain and the chief engineer have to get an official approval from the Regional Office of Maritime Affairs and Fisheries prior to sailing.

Since the Seafarers' Identity Documents Convention (ILO), seaman's certificates are to record crew's work history/employment record, qualifications, contract contents and other necessary items. Nevertheless, these certificates are not recognized as a formal passport by the Republic of Korea (ROK) immigration authority such that all foreign crews are required to submit their individual seafarer's

Manuscript received June 20, 2018; first revision August 20, 2018; accepted September 16, 2018.
Corresponding Author: Kyungryong Seo (krseo@pknu.ac.kr)
* Dept. of Software, Catholic University of Pusan, Busan, Korea (72networks@cup.ac.kr)
** Dept. of Computer Engineering, Pukyong National University, Busan, Korea (krseo@pknu.ac.kr)

identification when they enter or leave Korean waters.

The reason that seaman's certificates have not been digitized earlier is that, different from electronic passports, they are constantly exposed to moisture and humidity so that waterproofing the embedded batteries has not been easy. However, Bluetooth systems are suited to seaman's certificates as the batteries last longer and are resistant to moisture. Fig. 1 shows the design of the current (2016–2018) Korean seafarer's book.

Fig. 1. The design of the current (2016–2018) Korean seafarer's book.

One of the major difficulties of not being able to digitize the seaman's certificate was that the RFID chips were sensitive to extreme weather conditions involving very high (low) temperatures or humidities when they are embedded in the electronic passports.

Fig. 2 is a lost seafarer's book found in the Mokpo region (ROK). Once it falls into the sea, its condition becomes much worse and it becomes moldy quickly. In this sense, if they are digitized, it will be possible to know how many of them need to be rescued and where and who they are when the ship is sinking or stranded.

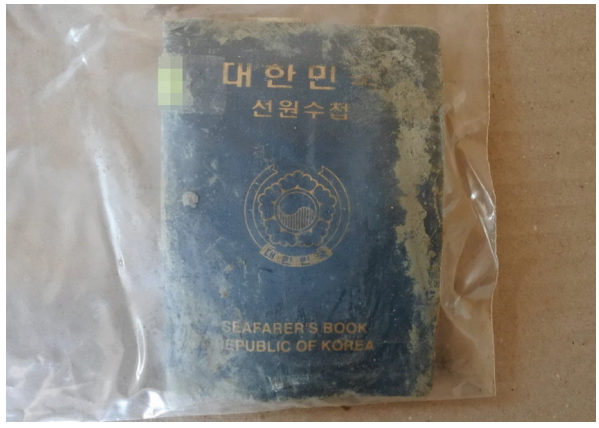

Fig. 2. A lost seafarer's book found in the Mokpo region (ROK).

2. Related Research

2.1 Electronic Passport (e-Passport)

Often referred to as an e-Passport, the electronic passport is embedded with an RFID chip containing the personal and biometric information of a holder and a communication antenna. Such a digitized passport makes it difficult to counterfeit or duplicate so that the holder's personal data can be protected while he/she travels abroad, making immigration procedure more convenient.

The embedded RFID chip holds the same information as the hand-written passports but it also contains the biometric information as well. Further, the e-Passports are applied with enhanced security measures which can effectively protect the information from forging or making copies. Also, as the holder's original information is being recorded in the central server, such malicious attempts can be detected immediately. Most of the nations around the world are issuing e-Passports currently and the government of the ROK has started to issue this type of passports to their citizens and government officials since 2008 [6,7].

Despite the convenience and the enhanced security offered by these e-Passports, they still have some problems. That is, the embedded RFID chip and antenna are vulnerable to pressure generated by excessive torsion or weight and the cover of these passports can become thicker than the old ones. The possibility of hacking of personal data using some advanced communication technologies has always been another major issue. As the information in the e-Passport can be hacked remotely after it is scanned, it could be transferred to another RFID chip for duplication. There have been many such incidents and so far, there seem to be no perfect countermeasures on this issue, even though a series of technological approaches have been introduced or proposed. All of these problems were anticipated and discussed before e-Passports were introduced globally [8–10].

Under the regulation of ICAO, a communication technology known as BAC has been adopted to the ROK e-Passports along with EAC and CA, which are to prevent skimmings or frequency eavesdroppings. Such a measure was deemed to be successful but to enhance the security level further, the government is taking further steps by centralizing the e-Passport issue system through their own closed administrative network. It was once reported that the Nicaraguan passports are the most secure ones as they have been using about 89 indicators as one of their security measures but the cat-and-mouse situation between governments and hackers are yet to be resolved as long as current communication technologies are used without improving their respective security levels. An attempt to replace the RFID chips as an alternative measure is being discussed currently.

A passport is a type of official document which proves one's identity, and the people who intend to travel out of their respective nations are required to carry it. This applies to ROK citizens as stated in Article 1 of the Passport Act. According to the act, passports are categorized into general passports, official passports, and diplomatic passports, as well as single-use passports, which allow a one-time trip to a foreign country, and multiple passports, which a person can use to travel abroad an unlimited number of times until the expiration date. The electronic passport or e-Passport is a machine-readable passport which contains an antenna and a chip that contains the holder's personal information along with their biometric information. The electronic passports in the ROK bear a serial number starting with the letter M [11–13].

The objective of introducing electronic passports is to maximize the security of passports through the prevention of forgery and illegal use, ultimately improving the convenience and safety of Korean

nationals traveling abroad. The holder's existing information is registered in the chip embedded in the electronic passport and it is protected with multiple types of security technologies. This makes it very difficult to manipulate the front page, where personal information is printed, or the chip. Even if the manipulation is successful, there is a significant chance that the tampering will be exposed during the immigration process.

The government of the ROK started issuing official and diplomatic electronic passports on March 31, 2008 and the general electronic passports on August 25 of the same year. It is true that there is a concern about remote information leaks for the reason that a contactless chip has been embedded in each electronic passport. However, there were ample discussions and studies by professionals on the security of the chips prior to when the electronic passport established itself as the new international standard.

Meanwhile, to explain about the personal information leak, a security technology called BAC (basic access control) is being applied to the ROK's electronic passports to prevent 'skimming', which is to illegally and stealthily approach the passport holder to steal his/her personal information. This is in accordance with ICAO regulations. To read the information on the chip, one needs to know the passport number first and then the birth date and the expiry date. However, skimming becomes impossible when the passport is folded so the data is not shown in the open [14–17].

Also, the ROK passports are encrypting communications between chips and readers with strong security technologies such as BAC, EAC (extended access control), and CA (chip authentication) to prevent eavesdropping. Finally, the personal information recorded in the chip includes the information printed on the first page with the holder's photo as well as other information, such as biometric data. In addition to above-mentioned technologies, the government of the ROK is doing everything possible to ensure complete personal information protection at an administrative level by adopting a centralized passport issuing system based on a unified closed network.

2.2 The Intent of the Introduction of Electronic Passports

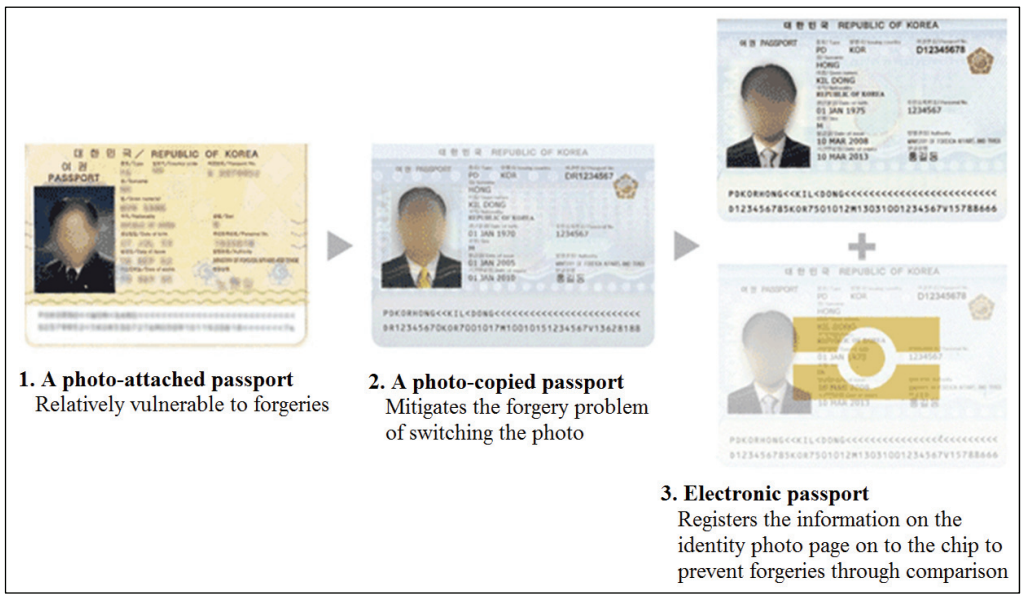

Fig. 3. Comparison between the registered fingerprint and the passport holder's fingerprint.

Ultimately, the introduction of electronic passports aims to promote the convenience of Korean citizens traveling abroad by maximizing the security of passports containing forgeries or being used illegally. The existing information recorded on a non-electronic passport is re-registered on the chip embedded in the electronic passport to which various types of security technologies have been added. Thus, manipulating the identity photo page and the chip simultaneously become almost impossible and, even if it is successful, the manipulations will be automatically detected during the immigration process [18–23]. Fig. 3 shows a comparison between the registered fingerprint and the passport holder's fingerprint. Photo replacement attempts, which happen frequently, can be prevented by this double-registration, and the passport holder verification and the illegal-use containment functions have been strengthened since 2010 by issuing electronic passports that include fingerprint information.

Meanwhile, various types of security technologies are applied to electronic passports to protect personal information or to prevent forgeries (Table 1).

Table 1. The security technologies for electronic passports

Technology	Description
Personal info. protection	
Basic access control (BAC)	Blocks remote information. Leaks: Ensuring that the information on the chip can only be read when the passport is submitted.
Extended access control (EAC)	
Terminal authentication (TA)	Fingerprint info. Protection: Ensuring that only the readers approved by the ROK government can read the information. Even the passport was submitted.
Chip authentication (CA)	Eavesdropping prevention: Creating a security communication channel stronger than BAC between the chip and the reader.
Forgery prevention	
Extended access control (EAC)	
Chip authentication (CA)	Verification of chip duplication (Alternative to AA function)
Passive authentication (PA)	Checking the contents alteration: Preventing chip and identity page manipulations.
Containment of illegal use	
Biometric data registration	Comparing the registered biometric information between the holder and the chip for identification.

2.3 Seafarer's Book

There was a plan to include seaman's biometric information in his/her certificate in between 2004 and 2005 but it was not realized as there were some issues as well. This idea was first brought forward at the Seafarer's Identity Documents Convention and the Ministry of Maritime Affairs & Fisheries (MOF) of the ROK was willing to go forward with it. The government's plan was to include the biometric information in seaman's certificate after computerizing it [24–27].

The September 11 attack on US soil was the main cause of the US government's decision on enforcing more strict requirements on seaman's certificates. After the attack, they announced that only the passports containing the holder's biometric information will be accepted when seafarers wish to come on US shores. Following the announcement, the ILO advised all the shipping companies and nations to replace their seaman's certificates accordingly. Despite the advice, the changes were slow because of the issues pertaining to the physical vulnerabilities of the RFID chips and the technological problems involved with digitalization. One interesting thing about the US's requirements was that the holder's voice data was not compulsory.

In the ROK, the seafarer's book was used as a passport before freeing overseas travel but, due to the problem of forgery, it was separated from the passport function. Prior to this action, the crews were able to travel abroad and the standard and the authentication methods of the certificate were similar to those of the passport.

This document certifies that the person holding the certificate is a seaman as per the International Convention on Standards of Training, Certification and Watch-Keeping for Seafarers (STCW), 1978. A Seaman Book is one of the compulsory documents for applying for crew transit visas. The record of employment on board of a merchant ship (sea service) is recorded in a Seaman Service Book. Seafarers in different countries are issued similar service books with different names (e.g., Seaman Record Book, Seaman Discharge Book, etc.). Pakistan's Government Shipping Office issues this book under section 120 of Merchant Shipping Ordinance, 2001 [28,29]. It is mandatory for all seafarers serving onboard a ship, whether they are on the Minimum Safe Manning Certificate or not, to hold a "Seaman Service Book and Seaman Identity Document (SID).

3. Seafarer's Book Digitalization Design for Authentication and e-Navigation

Compared to the e-passport, the seafarer's book is more detailed (Fig. 4). That is, Fig. 4(a) includes a crew member's diagnostic information, such as anemia, syphilis, AIDS, and urine test results along with the hospital name and the doctor's name [30]. The contents of the employment contract are then entered in Fig. 4(b) whereas the history of contract renewals or changes in contract terms are recorded in Fig. 4(c). Crew's licenses and their acquisition/expiry dates, etc., are to be included in Fig. 4(d) and, finally, in Fig. 4(e), the certificate holder's signature, address, and the requirements or the instructions given by the relevant authority(s) are entered. The items used in the author's preceding research The Medicine(s) Intake Notification System [1,2] are relevant to the items to be listed in Fig. 4(a).

As the new certificate includes more valuable information, improved security measures and storage capacity are essential. Although the certificates are usually kept in an onboard safe or cabinet, their safety cannot always be guaranteed.

This study discusses the method of distinguishing the damaged/unusable certificates due to contamination, humidity, or salinity. The study also aims to construct a system that tracks a seafarer's book through triangulation using the signals transmitted by multiple BLE beacons acting as GPS satellites. Although the principle is still the same, it is important to note that BLE technology was used to prolong battery life. Fig. 5 shows a whole system design of a seafarer's book.

Fig. 4. Parameters in the seafarer's book compared to the e-Passport: (a) a crew member's diagnostic information, (b) the contents of the employment contract, (c) the history of contract renewals or changes in contract terms, (d) Crew's licenses and their acquisition/expiry dates, and (e) the certificate holder's signature, address, and the requirements or the instructions given by the relevant authority(s).

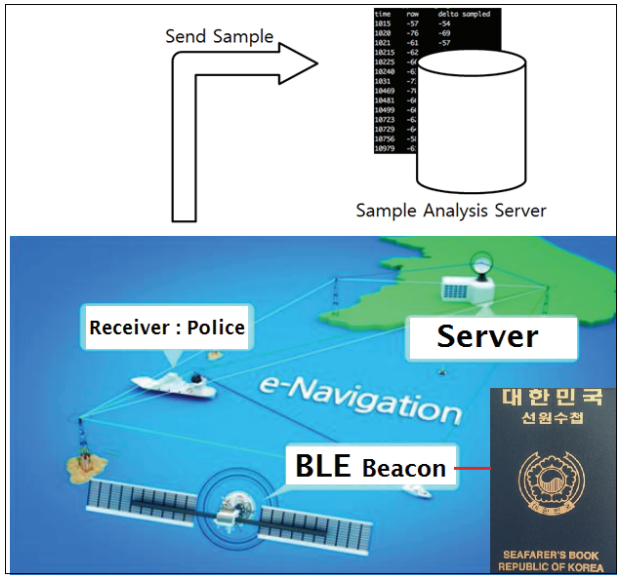

Fig. 5. A whole system design of a seafarer's book system.

The position of a beacon can be determined by using RSSI and a unique identifier for the distance calculations to perform triangulation. In this way, the location of the target certificate onboard. Also, it is possible to find the location of a certificate from outside the ship by applying BLE 5 technology, which will be quite useful for the Coast Guard or other maritime authorities to confirm the number of crew onboard. The Bluetooth function currently embedded in most smartphones can assume the role of distance measuring equipment to avoid additional cost.

The CR2045 battery usually lasts about 1.8 to 28.7 months when used for BLE equipment because of the equipment's low-energy efficiency. The BLE chipset and the expected battery life in different settings are shown in Fig. 6 and there is no wiring required to install the beacons. The battery recharging system described in this study can be useful to those certificates with the validities over 5 years.

Chipset	Advertising Interval	Est. Battery Life CR2032	Est. Battery Life CR2045	Est. Battery Life CR2477
Gimbal	100ms	n/a	n/a	n/a
Gimbal	645ms	1 month	2.5 months	4.1 months
Gimbal	900ms	n/a	n/a	n/a
Nordic Semiconductors	100ms	1.2 months	3.1 months	5.1 months
Nordic Semiconductors	645ms	7.0 months	18.19 month	29.3 months
Nordic Semiconductors	900ms	11.1 months	28.7 months	46.29 months
Bluegiga	100ms	0.9 months	2.4 months	3.8 months
Bluegiga	645ms	5.9 months	15.4 months	24.8 months
Bluegiga	900ms	9.3 months	23.9 months	38.5 months
Texas Instruments	100ms	0.7 months	1.8 months	2.9 months
Texas Instruments	645ms	4.1 months	10.6 months	17.1 months
Texas Instruments	900ms	5.6 months	14.4 months	23.1 months

Aislelabs

Fig. 6. BLE chipsets and their battery lives depending on settings.

The Data Rate vs. Data Range of each available technology in the preceding study [3] is arranged in Fig. 7. Both Bluetooth 5 and 4.2 are suitable for such a system because of their excellent data ranges regardless of humidity issues.

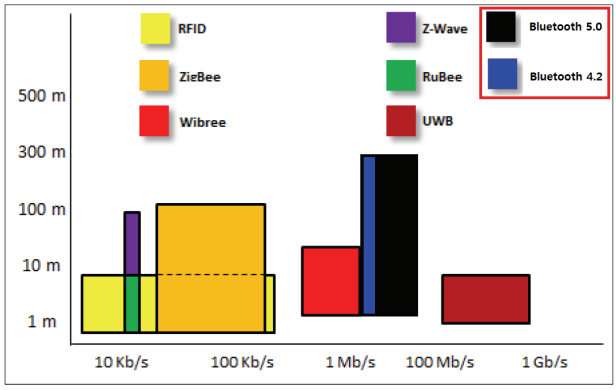

Fig. 7. Comparing data rate versus data range.

Bluetooth 5 technology was introduced by the Bluetooth Special Interest Group (Bluetooth SIG) in June 2016. Its transmission distance and data transfer rate have been greatly improved. For example, the transmission distance has increased four times whereas the data transfer rate has increased two times than that of Bluetooth 4.1, which was introduced in December 2013. Bluetooth 5 specifically targets drone, wearable, smart bulb, home automation, and IoT equipment markets but it can be widely used for positioning systems. Bluetooth SIG predicted that equipment embedded with Bluetooth 5 would appear in early 2017 and such a prediction was fairly accurate.

4. Implementation of Digitalization of Seafarer's Book Authentication for Authentication and e-Navigation

Fig. 8 shows the entire service diagram for the digitalization of a seaman's certificate. A crew member registers the contents of his/her seafarer's book in advance and then the maritime police will be able to request the contents and receive them.

The intermediate stage between the maritime police and the server is processed with the BLE beacon links where Bluetooth 4.2 has been used. The data flow chart is shown in Fig. 9.

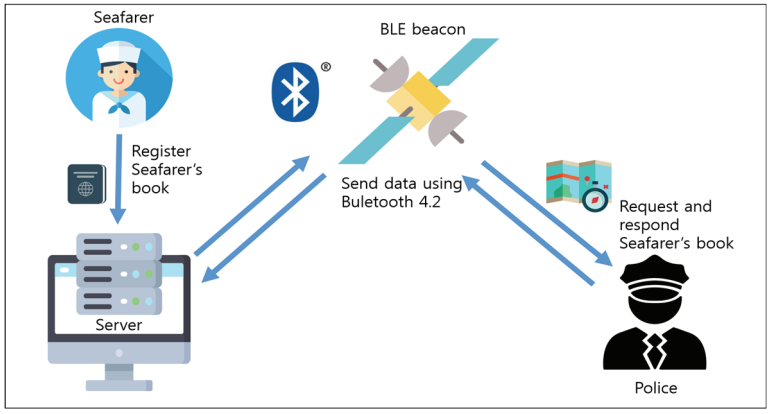

Fig. 8. The entire service diagram for the digitalization of a seafarer's book.

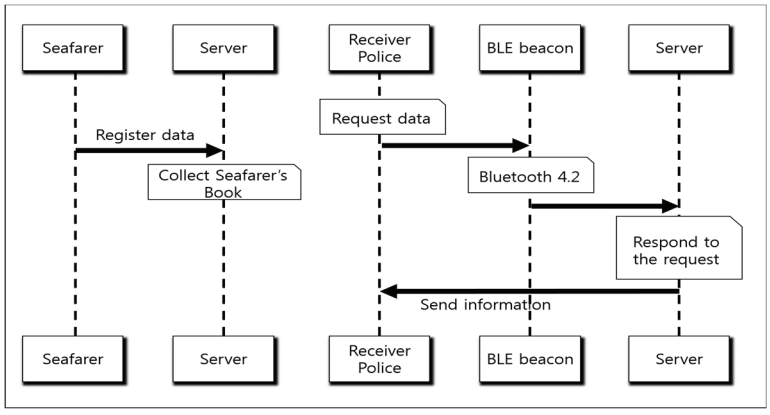

Fig. 9. The data flow chart for the digitalization of a seafarer's book.

Fig. 10 shows a brief system drawing for the digitalization of a seafarer's book Authentication for Authentication and e-Navigation. As described, the ship sensors transmit the information to the server. First, each sensor is represented in a rectangular box. The main sensors are indicated as icons to let the reader see the overall configuration at a glance (in the UX-like form, for example). From the left, Navigation Route, Map, Anchor, Switchboard, and seafarer's book are itemized. The sensor values will be transmitted to the server with Bluetooth 4.2.

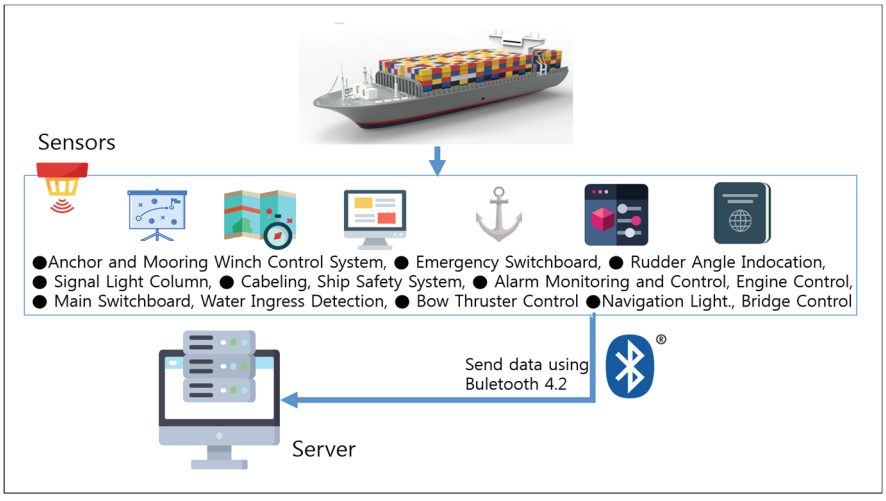

Fig. 10. A system drawing for the digitalization of seafarer's book for e-Navigation.

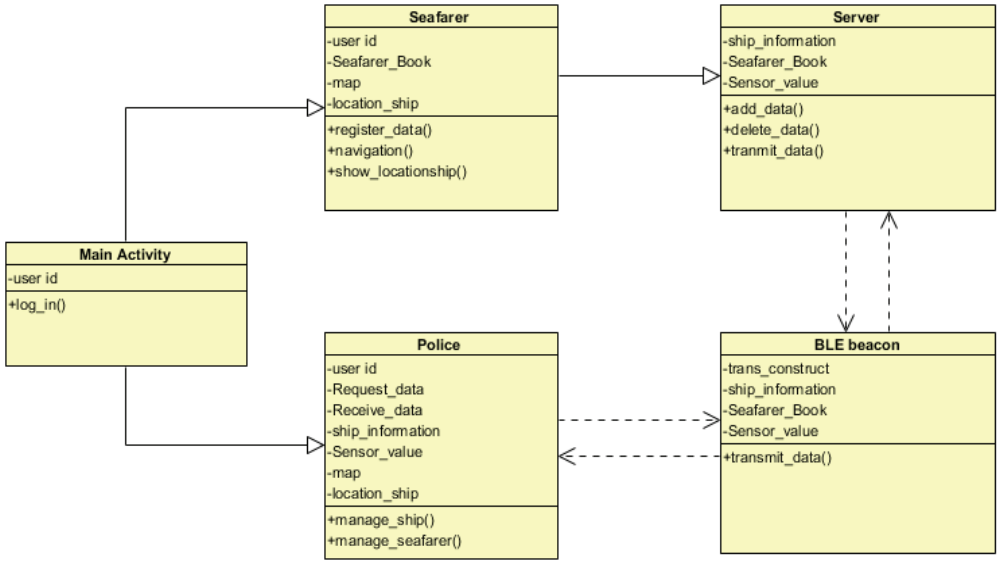

Fig. 11. The UML of the Android application for digitalization of a seafarer's book.

Fig. 11 is the UML of the Android application used to digitalize a seafarer's book. The main activity starts first and one needs to log in here. The log-in part is separated into different roles depending on if the crew or the maritime police are using it. The variables at the upper left include ID, seaman's certificate,

map, and the position of navigating ship. The primary function of the UML is to register information on the server and let the user see the current position and information of the navigating ship. Once ServerClass registers the information on the server, the server stores them subsequently. The information of the ship or the seafarer's book and the sensor values collected from the ship can be added or deleted. The values can also be delivered by using BLE beacons.

Next, the primary objective of the login by the maritime police is to use the management function. The variables, in this case, include user ID, requesting data, receiving data, ship's information, sensor values, map, and the current position of the ship. The management function can be used in this class against the ship or the crew. This class also performs the task of passing through BLE beacon(s) to fetch the server data to support the management function. Meanwhile, the BLE beacons are positioned in the intermediate stage between the ServerClass and the MaritimepoliceClass to perform the function of delivering values.

Fig. 12 shows the UI of the application for digitalization of a seafarer's book. The menu includes Home, Map, Register, Load, Sensor, and Setting but the main functions are map and register. Observing more closely, the user has logged-in with an administrator account. That is, an ID of the Maritime Police has been used to check the information of the ship. The first screen shows the navigating ship. Looking closely at the ship in the middle, there are the Mark and Select buttons. The design was implemented in a way that the screen will move to the second screen once one of the ships on the map has been selected.

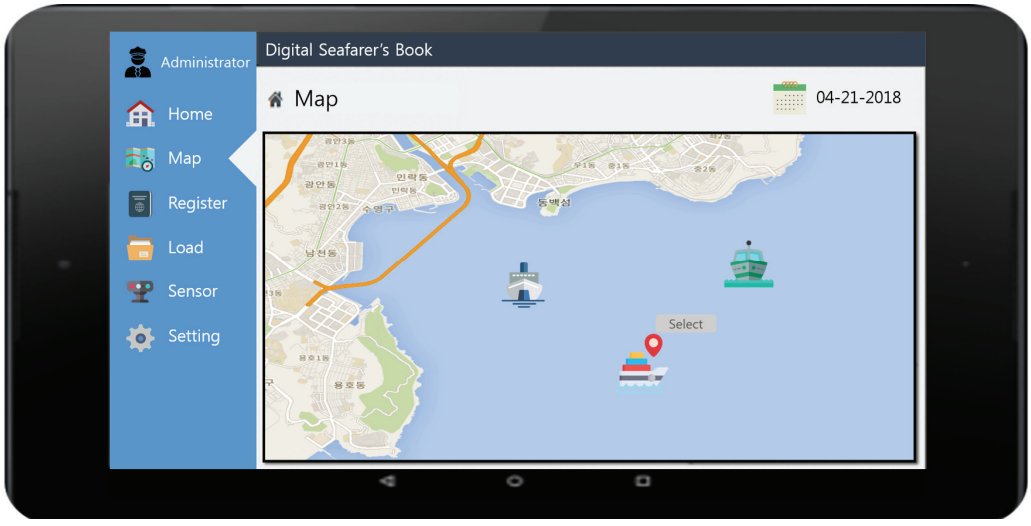

Fig. 12. The UI of the application for digitalization of seafarer's book for e-Navigation.

Fig. 13 shows the UI of information verification for digitalization of a seafarer's book. The information window appears when the select button has been clicked. The information scanned or digitalized in advance can be checked with the application. The seafarer's book contains information such as the holder's health information, his/her qualifications, the contract date, etc. The icon of a currently selected ship appears in the above box together with its information window. As such, one can find out about the ship's information as well as the crews' qualifications and the expiry dates of their licenses. This can also be a useful system when identifying some malicious captains.

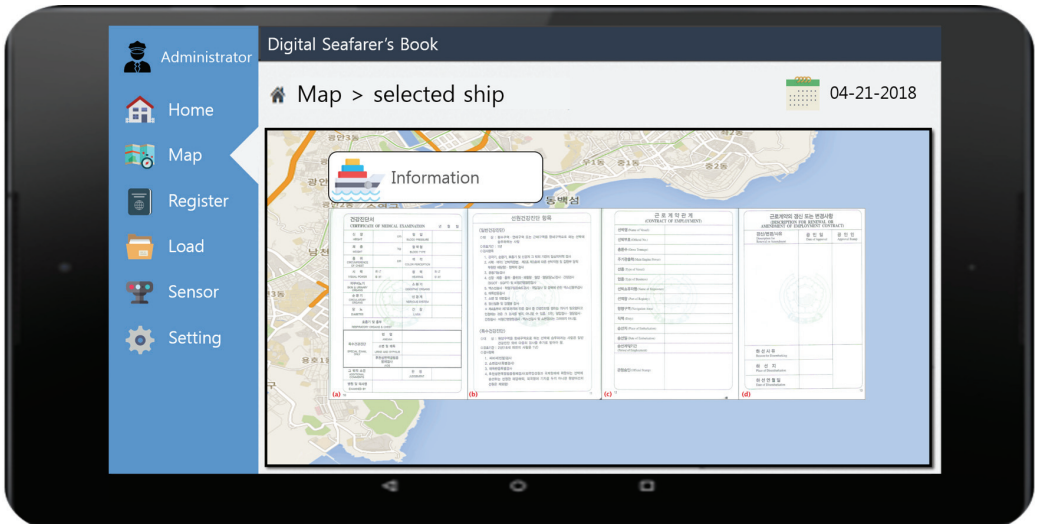

Fig. 13. The UI of information verification for digitalization of a seafarer's book.

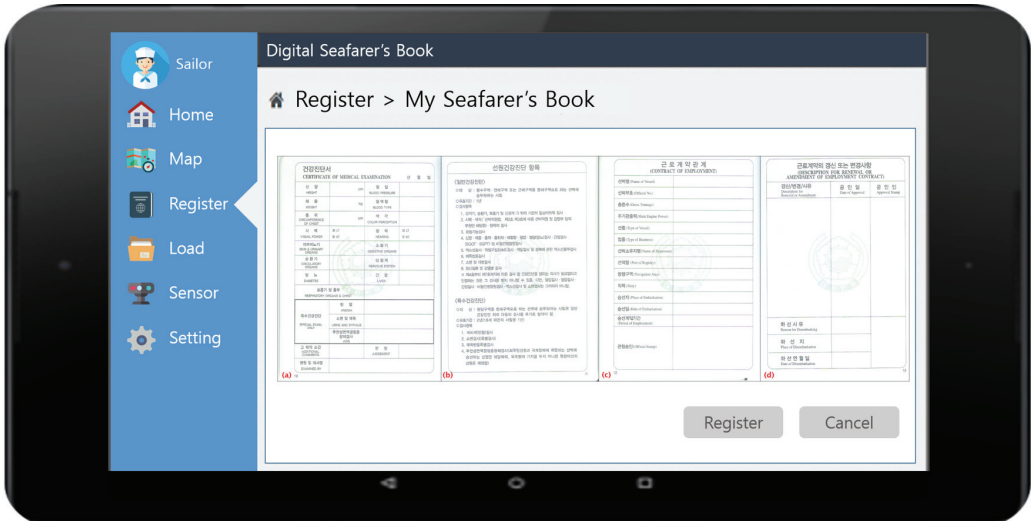

Fig. 14. The UI of a seafarer's book registration for digitalization.

Typically, the seaman's certificates are recorded by the captains, medical institutions, and authorization authorities and kept in the onboard safe or cabinet. Due to the possibility of contamination by mold, the certificates are usually made of a cloth resistant to salinity. The simultaneous inspection of the ships by the ROK's Maritime Police is lengthy and expensive. Thus, this study proposes a system which allows them to conveniently manage the ships in their territories.

Fig. 14 shows the UI of a seafarer's book registration system for digitalization. If one wishes to see the information on the seaman's certificate, the digitalized certificate must be registered first. The upper left of the picture shows that the crew or the captain's ID is currently logged in. In the menu Register, there are spaces in which the information on the certificate should be entered. Once the Register button has been pushed, the registration will be complete.

5. Conclusion and Future Work

This study focused on the digitalization method for seaman's certificate to prepare for the imminent era of total e-Navigation. During the research, it was found that the Bluetooth 4.2 and BLE technologies were the most effective means of communication while attempting to find some robust sensors which would work well and adaptable to the certificates regardless of surrounding on-board conditions. Further studies have been performed in relation to the possibility of embedding the functions of e-Navigation system terminal to the certificate itself but the problems of excessive processing and memory overheads have to be solved to design a more effective and efficient protocol.

This manuscript is the product of a system design and implementation carried out for the ROK's Maritime Police where many author's alumni (Fishery Dept., Currently Department of Marine Industry and Maritime Police of Jeju National University at Ara) are still working. The interviews with them were quite helpful. It is not easy to distinguish the identities of the crews without a license or certificate, unless stowing away on a ship were possible. The number of unfortunate deaths in the maritime police is continuing due to attacks by criminals or those who have committed something illegal. Thus, the inspections or crackdown operations will become more efficient and effective if the number of crew members or workers can be determined quickly and remotely. Also, the necessity of additional forces can be judged swiftly.

The author plans to disclose the system as open source technology after registering for the patent and continuously updating the system. This is in a hope to assist the maritime police when they exercise legal governmental power and to reduce the number of fatalities.

As a future work, it may be possible to implement a congestion control mechanism. The protection of the transmitted data was not taken into consideration in our protocol so that the discussion concerning protection methodology can also be one of the future studies.

Acknowledgement

This research was supported by the Research Grant of Pukyong National University in 2017.

References

[1] S. Park and J. H Huh, "Effect of cooperation on manufacturing IT project development and test bed for successful industry 4.0 Project: Safety Management for Security," *Processes*, vol. 6, no. 7, article no. 88, 2018.

[2] W. Khan, H. Ullah, A. Ahmad, K. Sultan, A. J. Alzahrani, S. D. Khan, M. Alhumaid, and S. Abdulaziz, "CrashSafe: a formal model for proving crash-safety of Android applications," *Human-centric Computing and Information Sciences*, vol. 8, article no. 21, 2018. https://doi.org/10.1186/s13673-018-0144-7.

[3] M. Zareei, A. Zarei, R. Budiarto, and M. A. Omar, "A comparative study of short range wireless sensor network on high density networks," in *Proceedings of the 17th Asia Pacific Conference on Communications*, Kota Kinabalu, Malaysia, 2011, pp. 247-252.

[4] A. Ault, X. Zhong, and E. J. Coyle, "K-nearest-neighbor analysis of received signal strength distance estimation across environments," in *Proceedings of the 1st Workshop on Wireless Network Measurements*, Trentino, Italy, 2005, pp. 1-6.

[5] J. Jung, D. Kang, and C. Bae, "Distance estimation of smart device using Bluetooth," in *Proceedings of the 8th International Conference on Systems and Networks Communications*, Venice, Italy, 2013, pp. 13-18.

[6] Q. Dong and W. Dargie, "Evaluation of the reliability of RSSI for indoor localization," in *Proceedings of 2012 International Conference on Wireless Communications in Underground and Confined Areas*, Clermont Ferrand, France, 2012, pp. 1-6.

[7] M. Botta and M. Simek, "Adaptive distance estimation based on RSSI in 802.15. 4 network," *Radioengineering*, vol. 22, no. 4, pp. 1162-1168, 2013.

[8] J. Kang, D. Kim, and Y. Kim, "RSS self-calibration protocol for WSN localization," in *Proceedings of 2007 2nd International Symposium on Wireless Pervasive Computing*, San Juan, Puerto Rico, 2007.

[9] P. Kumareson, R. Rajasekar, and P. Prakasam, "Accurate location identification using Bluetooth in Android smart phone," *The International Daily Journal*, vol. 30, no. 120, pp. 81-86, 2015.

[10] T. Saito, "Smart card for passport, electronic passport, and method, system, and apparatus for authenticating person holding smart card or electronic passport," U.S. Patent 8918900, 2014.

[11] O. Brunet, J. F. Salvo, and I. Peytavin, "Method of producing a contactless microelectronic device, such as for an electronic passport," U.S. Patent 7992790, 2011.

[12] P. K. Sharma, J. H. Ryu, K. Y. Park, J. H. Park, and J. H. Park, "Li-Fi based on security cloud framework for future IT environment," *Human-centric Computing and Information Sciences*, vol. 8, article no. 23, 2018. https://doi.org/10.1186/s13673-018-0146-5.

[13] T. Kasper, D. Oswald, and C. Paar, "Side-channel analysis of cryptographic RFIDs with analog demodulation," in *RFID Security and Privacy*. Heidelberg: Springer, 2011, pp. 61-77.

[14] Y. Liu, T. Kasper, K. Lemke-Rust, and C. Paar, "E-passport: cracking basic access control keys," in *On the Move to Meaningful Internet Systems* 2007: CoopIS, DOA, ODBASE, GADA, and IS. Heidelberg: Springer, 2007, pp. 1531-1547.

[15] S. Vaudenay, "E-passport threats," *IEEE Security & Privacy*, vol. 5, no. 6, pp. 61-64, 2007.

[16] R. Peeters, J. Hermans, and B. Mennink, "Speedup for European epassport authentication," in *Proceedings of 2014 International Conference of the Biometrics Special Interest Group (BIOSIG)*, Darmstadt, Germany, 2014, pp. 1-6.

[17] J. H. Huh, "PLC-based design of monitoring system for ICT-integrated vertical fish farm," *Human-centric Computing and Information Sciences*, vol. 7, article no. 20, 2017. https://doi.org/10.1186/s13673-017-0101-x.

[18] J. Zhu, K. Zeng, K. H. Kim, and P. Mohapatra, "Improving crowd-sourced Wi-Fi localization systems using Bluetooth beacons," in *Proceedings of 2012 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, Seoul, Korea, 2012, pp. 290-298.

[19] W. M. Kang, S. Y. Moon, and J. H. Park, "An enhanced security framework for home appliances in smart home," *Human-centric Computing and Information Sciences*, vol. 7, article no. 6, 2017. https://doi.org/10.1186/s13673-017-0087-4.

[20] J. Lee, J. Jung, P. Park, S. Chung, and H. Cha, "Design of a human-centric de-identification framework for utilizing various clinical research data," *Human-centric Computing and Information Sciences*, vol. 8, article no. 19, 2018. https://doi.org/10.1186/s13673-018-0142-9.

[21] F. Hamad, J. Zraqou, A. Maaita, and A. A. Taleb, "A secure authentication system for epassport detection and verification," in *Proceedings of 2015 European Intelligence and Security Informatics Conference*, Manchester, UK, 2015, pp. 173-176.

[22] G. M. Ezovski and S. E. Watkins, "The electronic passport and the future of government-issued RFID-based identification," in *2007 IEEE International Conference on RFID*, Grapevine, TX, 2007, pp. 15-22.

[23] Y. J. Chang, Y. Y. Chu, C. N. Chen, and T. Y. Wang, "Mobile computing for indoor wayfinding based on Bluetooth sensors for individuals with cognitive impairments," in *Proceedings of 2008 3rd International Symposium on Wireless Pervasive Computing*, Santorini, Greece, 2008, pp. 623-627.

[24] V. Pasupathinathan, J. Pieprzyk, and H. Wang, "Formal security analysis of Australian e-passport implementation," in *Proceedings of the 6th Australasian Conference on Information Security-(AISC)*, Wollongong, Australia, 2008, pp. 75-82.

[25] S. Kim and K. I. Hwang, "Design of real-time CAN framework based on plug and play functionality," *Journal of Information Processing Systems*, vol. 13, no. 2, pp. 348-359, 2017.

[26] M. S. S. Danish, A. Yona, and T. Senjyu, "Insights overview of Afghanistan electronic national identification documents: eGovernment, eID card, and ePassport schemes," in *Proceedings of 2014 IEEE International Conference on Internet of Things (iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom)*, Taipei, Taiwan, 2014, pp. 251-255.

[27] C. H. Li, X. F. Zhang, H. Jin, and W. Xiang, "E-passport EAC scheme based on identity-based cryptography," *Information Processing Letters*, vol. 111, no. 1, pp. 26-30, 2010.

[28] Government of Pakistan, *The Gazette of Pakistan (Extraordinary)*. Islamabad, Pakistan: Government of Pakistan, 2001, pp. 1290-1298.

[29] About Seamen Book [Online]. Available: http://shippingoffice.gov.pk/ssb.html.

[30] J. H. Huh, "A study on digitalization of Seafarer's Book Republic of Korea for e-Navigation: focusing on wireless network," in *Advances in Computer Science and Ubiquitous Computing*. Singapore: Springer, 2016, pp. 1046-1052.

Jun-Ho Huh https://orcid.org/0000-0001-6735-6456

He was born in Kyoto, Japan. He was finished the Cooperative Marine Science and Engineering Program, Texas A&M University at Galveston, USA in 2006, received B.S. in Science degree from Department of Major of Applied Marine Sciences (Currently Faculty of Marine Biomedical Sciences) and B.S. in Engineering degree (Double Major) from Department of Major of Computer Engineering from Jeju National University at Ara, Jeju, Korea in 2007. And he has a completion of the Secondary School (Middle and High schools) Teacher Training Curriculum in accordance with Republic of Korea Secondary Education Act (Aug. 2007), and received M.A. in Education degree from Department of Major of Computer Science Education, Graduate School of Education, Pukyoug National University, Busan, Korea in 2012. Also he has a completion of the Secondary School (Middle and High schools) Teacher Training Curriculum in accordance with Republic of Korea Secondary Education Act (Aug. 2012) and received the Ph.D. in Engineering degree from Department of Major of Computer Engineering, Graduate School, Pukyoug National University, Busan, Korea in 2016. He received the Best Paper Award from Korea Multimedia Society nine times (Nov. 2014, May. 2015, Nov. 2015, May, 2016. Oct, 2016, May, 2017; three times, Oct, 2017). And he received Undergraduate Student Paper Bronze Medal (corresponding author) Awarded, Korea Information Processing Society (Apr. 28, 2017). Also, he received Best Paper Award of the 10th 2016 International Interdisciplinary Workshop Series from HSST (Aug. 2016). Also, he received Best Paper Award of the 16th International Conference on Control, Automation and Systems (Oct. 2016), ICROS with IEEE Xplore. He has been serving as chairs in some conferences and workshops; MUE 2017, BIC 2017, CUTE 2017, WITC 2018, MUE 2018, PDCAT 2018, BIC 2018, CUTE 2018, CSA 2018, WITC 2019. He is Technical Committee at IFAC (International Federation of Automatic Control), CC 1 (Systems and Signals), TC 1.5. (Networked Systems) (2017-2020). And, Technical Committee at IFAC, CC 3 (Computers, Cognition and Communication), TC 3.2 (Computational Intelligence in Control) (2017-2020). Technical Committee at IFAC, CC 7 (Transportation and Vehicle Systems), TC 7.2. (Marine Systems) (2017-

2020). Currently he is Associate Editor at Human-centric Computing and Information Sciences (HCIS), Springer Berlin Heidelberg (SCIE/SCOPUS indexed). Also, he is Associate Editor at Journal of Information Processing Systems (JIPS), Korea Information Processing Society (SCOPUS/ESCI indexed) and a Research Professor of Dankook University, Yongin, Korea (Jul. 2016–Sep. 2016). Currently he is Assistant Professor of Department of Software, Catholic University of Pusan, Korea (Dec. 2016–now). His research interests are green IT, smart grid, network security, IoT, system architecture.

Kyungryong Seo https://orcid.org/0000-0002-3891-7821

He received B.S. degree in Engineering from Pusan National University, Busan, Korea in 1983, M.S. degree in Electrical Engineering from Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea in 1990, and Ph.D. degree in Electrical Engineering from KAIST, Daejeon, Korea in 1995. Currently, he is a Full Professor (Tenure) of Computer Engineering Departments, Pukyong National University at Daeyeon, Busan, Korea. His research interests are high speed computer network, network security, high availability computing.