International Journal of Security and Its Applications
Vol. 10, No. 2 (2016), pp.141-150
http://dx.doi.org/10.14257/ijsia.2016.10.2.13

Security Enhancement Scheme supporting range queries on encrypted DB for Secure e-Navigation Era

Donghyeok Lee and Namje Park†

Department of Computer Education, Teachers College, Jeju National University
{bonfard, namjepark}@jejunu.ac.kr

Abstract

The Maritime Cloud is the term used to describe the concept of an infrastructure that support authorized, seamless information transfer, as requested by the IMO e-navigation strategy, and as derived from testbeds focused on e-navigation. In this paper, we proposed Bucket ID Transformation that is a new encryption mechanism and the scheme can range search without order-preserving. Bucket ID Transformation is performed by recursive HMAC as many as a value of Bucket ID.

Keywords*: Cloud, E-navigation, IMO, Secure Maritime, e-Nav.*

1. Introduction

The IMO e-navigation strategy has requested a communication infrastructure providing authorized seamless information transfer between stakeholders. The Maritime Cloud is the term used to describe the concept of an infrastructure that support authorized, seamless information transfer, as requested by the IMO e-navigation strategy, and as derived from testbeds focused on e-navigation. The Maritime Cloud concept is similar to the maritime infrastructure framework, adding those elements, that are necessary to support the e-navigation domain. A limited testbed version of the Maritime Cloud concept exists, which has so far demonstrated interoperable information exchange between systems developed by different e-navigation testbed projects in Northern Europe and Korea. Based on the experience of several e-navigation test bed projects in Europe (EfficienSea, MonaLisa, and ACCSEAS) as well as projects in Korea and Japan, the concept of the Maritime Cloud has been developed into an open source functional prototype.

When traditional encryption algorithm apply to the database, efficiency decline problem was occured because order of encoded data is not equal to order of plaintext. To overcome this limit, Haciquimus proposed bucket based index[6] that can bring performance improvement for queries over encrypted data. besides, Order-Preserving Encryption scheme that is possible range queries over encrypted data without decryption was proposed by Sun[8], Agrawal[1], *Et*cs. But, Encrypted data by Order-Preserving Encryption Scheme was exposed order of plaintext, As a result, the scheme cannot secure against inference attack. Especially, the scheme cannot used for rank scale. On the other hand, Damiani proposed hash-based indexing method that can prevent frequency-based inference attack. This scheme encourage use of collided hash function for protecting inference attack. But, the method has problem in search of range data using reference by index. Moreover, overhead problem was exist because the method must bring other tuple that have equal hash column when search only one tuple.

* This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (2013R1A1A4A0 1013587)
† Corresponding author : Namje Park (namjepark@jejunu.ac.kr)

ISSN: 1738-9976 IJSIA

In same paper, Damiani proposed auxiliary b+-tree method. The method can range search over encrypted data and can prevent frequency-based inference attack because each tuple has different encrypted data by whole-tuple-encryption. But, the method has problem that can't search by one-time range query transaction. That is, this method needs d+n times of queries for range search. (d: tuples in range, n : nodes of tree) Finally, the method couldn't solve overhead problem. Use of order-preserving function is desirable for efficiency. On the other side, obviously, order-preserving function cannot prevent the inference attack. Therefore, it needed stabilize trade-off to solve the problem.

In this paper, we proposed Bucket ID Transformation that is a new encryption mechanism and the scheme can range search without order-preserving. Bucket ID Transformation is performed by recursive HMAC as many as a value of Bucket ID. The proposed method, whose order is not exposed, has a more enhanced security than Sun and Agrawal and is also more efficient compared to Damiani's method as it can recover the original value by transmitting queries times (q: bucket size, d: number of transmitted queries of damiani, n: number of nodes) to the database.

2. Related Works

2.1. Based Index [6]

Hacigumus *et al*.[6] proposed the technique that queries encrypted data. This is based on the definition of the number of buckets in the attribute area. Let's assume that ri is the plaintext relation with schema Ri(Ai1, Ai2, . . . , Ain) and rki is the corresponding encrypted relation in Rki(Counter, Etuple). When a plaintext attribute Aij exists in RI where a domain is Dij, the bucket-based indexing technique can divide Dij without overlapping it. This is called "bucket". A bucket has a continual value.

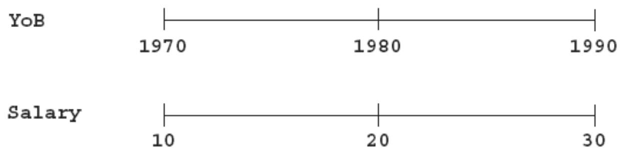

Figure 1. Bucketization Example

This procedure called "bucketing". The buckets are always created with same size. Each bucket is connected with a unique value and this value is a domain for connection between Ij and Aij. If a plaintext tuple t is given in ri, the value of attribute Aij for t should belong to a bucket. This is very important in keeping data confidentiality.

2.2. B+Tree[2][3]

An untrusted DMBS can find encrypted data only and any B+-Tree defined on the index doesn't reflect the order of plaint text. This, in effect, makes the range search impossible. To overcome this problem, we can entrust a trusted front-end with the decision on B+-Tree information. This paper proposes encrypting the whole B+-Tree node. The original B+-Tree is represented as two attributes (Node ID and encrypted value) in an untrusted DBMS.

2.3. Anti-Tamper Database : Open Form Encryption[8], Order-Preserving Encryption For Numeric Data (OPES)[1]

If this is expressed in a formula; E(n) = $\sum_{i=1}^{n}(Z_i + P_i)$. For numeric data, it may be a serious problem, if the attacker can get a value close to plaintext p corresponding to encrypted text c, though he doesn't know p exactly. In other words, in ordinary Order-Preserving Mechanism, if the distribution is known, the plaintext can be inferred. Since this paper considers the ciphertext only attack only, the proposed mechanism is secure from estimation exposure. However, when using this method, the order is exposed due to the nature of Order-Preserving. The p value can be inferred by designating a certain location. The fact that order is kept means consequently that the order is known and this means that some of information is exposed. Therefore this paper proposes an encryption mechanism that allows range query without keeping the order.

3. The Proposed Mechanism

3.1. Notations

Notations that are used in this section is as following :
m : Plaintext, r : residue of plaintext, I_B : Bucket ID, S_B : Size of Bucket, T(x) : Transform execution result of x, IT(x) : Inverse Transform execution result of x, $T(I_B)^K$: Encrypted Bucket ID, $T(r)^{IB||K}$: Encrypted residue (Ciphertext), K : Key of Keyed-HMAC

3.2 Overview of Our Scheme

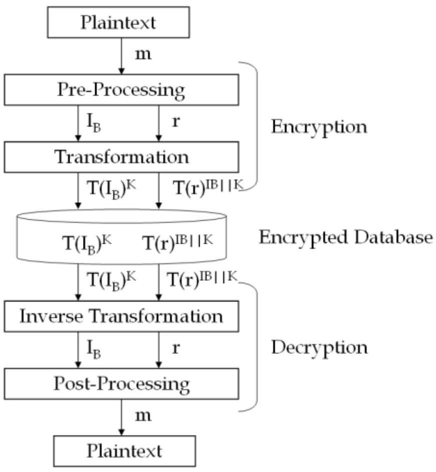

Figure 2. Illustrating Our Scheme

In our mechanism, encryption and decryption procedure are constructed each two stage.

(1) Encryption process
- Pre-Processing: Pre-process stage for plaintext m, extract m in two integer and calculate bucket threshold in this stage.
- Transformation : Integer IB, r is transform into hashed value that can not recognize by attacker.

(2) Decryption process
- Inverse Transformation: Calculate set of IB, r from each set of T(IB)K and T(r)IB||K.
- Post-Processing : Calculate plaintext m based on IB, r.
- According to these each two stage, authorized database manager can encrypt plaintext and decrypt ciphertext securely.

3.3 Encryption Process

(1) Pre-Processing
1) Scaling of Plaintext
m_s = m * There are 4 scales; nominal scale, ordinal scale, interval scale and ratio scale. The nominal scale is a scale that we cannot define the order and the scope of this paper is confined to ordinal scale, interval scale and ratio scale. This process executes integarization as follows. If it is ordinal scale and the ordinal value is rank, m_s equals rank. If it is interval or ratio scale, m_s equals m for the column that treats integers while m_s equals m * for the column that allows decimals.

2) Modulo Arithmetic
All intergers has quotient IB and residue r by dividing arbitrary given SB. Computational procedure is as following :

Calculate residue value r by next expression.

$$r \equiv m_s \bmod S_B$$

IB is calculated by next expression.

$$I_B = \frac{m_s - r}{S_B}$$

Relation of IB and r about ms, is as following :

$$0 \leq r \leq SB$$

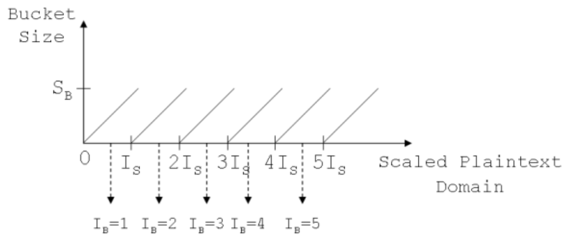

Figure 3. Encryption Process

Accroding to incresement of ms, increse IB too. and r value is not over then the value of SB because r is created by modulo arithmetic. We consider IB as bucket ID that has bucket size SB because the plaintext ms was segmentd equally within SB size.

(2) Transformation
1) Decision of Bucket Threshold
In this stage, We consider processing of decision of bucket threshold. The reason that calculating of bucket threshold is to be quantity of each bucket are approximate uniform. By threshold of bucket quantity, the number of point of each bucket is not over than threshold value. As a result, Bucket-based Frequency inference attack is very hard.

Suppose The number of bucket on domain is m and full amount of point is l, Bucket threshold is defined as following:

$$\text{Bucket Threshold} = \frac{\sum_{i=1}^{m} p_i}{m}$$

By bucket threshold value, bucket size is not over than threshold value. This characteristic makes hard the inference attack. As shown Figure.1, Bucket 3 is splitted because excess of threshold value. Splitted buckets have each other hash values. If does not consider the bucket threshold in stage of pre-processing, the attacker can inference bucket 3 from collected bucket frequency very easily. Through dividing the bucket by threshold, the attacker can't perform frequency based inference attack.

1) Transformation Process

In transformation stage, transformed value T(IB) and T(r) is calculated from recursive HMAC of the number of times of IB and r. That is, Integer IB or r is equal to the number of times of performing of recursive hashing. Numeric seed s is given beforehand value. Here, K is a symmetric key and must keep secret.

2) Key Generation by Contiguation

In the process of transformation of r, set the key K is IB||K. That means, If two of r are located within same bucket, transformation key are identical. But, location of each r are different buckets, the key of each r are different too. It can represent T(IB)K and T(r)IB||K. The reason of diffent key assignment in each other bucket is protection of inferencing for SB. That is, If every r have equal key, T(r) may repeat by SB cycle. This characteristic can occur the problem that exposure of SB. In case of an attacker try known-plaintext attack, the attacker can inference range of r that has identical bucket id. This problem can be solved by different key assignment for each bucket.

As a result, encrypted data is {T(IB)K,T(r)IB||K}. Database manager can insert these encrypted data in the databse securely. For example, Suppose transformed IB values of attribute of Bob, James and Alice is named IBB,IBJ and IBA, The attributes are insert as following :

Name	Salary
Bob	4835
James	3527
Alice	7723

Name	$T(x)^K$	$T(x)^{IB\|\|K}$
Bob	YwaVIQ+XW7Q3w4LK+E9Rms=	Iai6yp4lQ3nMyjhiyAyz1jhjru4=
James	+Lo7YRIktiicR1nXTzfLD6TnjQo=	FWeAid+ewLO/xncEJSDfcDkoQ=
Alice	gtS0izJW9Xngir5CJ6ZkkehIMi0=	VCpg8E/wPszmO4NWGSblC6Bw=

Figure 4. Encryption Data

Here, Who has K can decrypt original plaintext m. on the other hand, T(IB)K and T(r)IB||K are not preserve order, this characteristic can make robust and reliable protection from inference attack.

3.4 Decryption Process

Input of inverse transformation is a pair of set of T(IB) and T(r). the reason that the input has set of transform values is efficiency of inverse transformation. Input from set is more efficient better than individual processing. Input from set of T(IB)s and T(r)s are need procedure of only two times. Note that K is substitute IB||K when transforming r. According to above procedure, IB and r can be calculated. After this, authorized user can be decrypt original plaintext from scaled plaintext ms.

3.5 Example

Suppose plaintext is 4835 and a key is 624. ms is equal to plaintext 4835 because original plaintext is integer. In stage of modular arithmetic, if suppose that SB is 100, 4835 mod 100 is equal to 35. That is, the value of r is 35. And IB value can calculate by $\frac{4835-35}{100}$ =48. In transformatin stage, T(48)624 and T(35)48||624 are calculated by performing HMAC recursively as IB value 48 and r value 35. Finally, database manager can get encrypted result that are T(IB)K=YwaVI Q+XW7Q3w4LKV7+go+E9Rms= and T(r)IB||K=Iai6yp4lQ3nMyjhiyA yz1j hjru4=. Now, the database contains these encrypted values. Therefore, the attacker cannot inference the original plaintext from encrypted data T(IB)K and T(r)IB||K because the encrypted values are just look like insignificant hashed values.

4. Analysis

Our Scheme Proposed mechanism can prevent frequence and order based inference attack because the mechanism is not preserve order. In addition, our mechanism can perform range query and aggregation queries(MIN,MAX,COUNT) over encrypted data. On the other hand, even if insert or update transactions are much repeat, plaintext decrypting is not needed. In case of range search, number of quries are greatly reduced better than Damiani's method. A comparision table is as following :

Table 1. Comparison Table

	Equality Query	Range Query	Updating	Prevention of Order Exposure
Bucketing[6]	○	△	○	△
B+-Tree[2][3]	○	○	×	○
Hash Based[2][3]	○	×	○	○
OPES[1]	○	○	○	×
Anti-Tamper[8]	○	○	○	×
Our Scheme	○	○	○	○

(○ : Supported, △ : semi-supported, × : not supported)

5. Conclusion

To support the e-navigation strategy for global maritime transport, the Maritime Cloud offers a Maritime Identity concept for all participating stakeholders in a common framework. Information services for e-navigation will be published in a dynamic registry, available for discovery by relevant stakeholders. An opportunity for placing the Maritime Cloud Client Component (or Service Agent) into the ships bridge architecture exists in the ongoing standardization processes. While a window of opportunity for initializing the establishment of the Maritime Cloud exists, a governing structure, business model and operational environment with related evolutionary processes for cooperation amongst many different projects and stakeholders will have to be established for the Maritime Cloud (or maritime infrastructure framework) to ensure long term sustainability.

The security for database needs a separate consideration in addition to traditional cytological security. Especially, since various attacks such as inference attack, query execution attack or known-plaintext attack are possible according to the nature of database, an encryption mechanism suitable for database environment is required. This paper proposes a new encryption mechanism that can carry out range search without exposing the order. This method is more powerful than order-keeping methods of Sun and Agrawal and is expected to secure data more efficiently than Damiani method. As a future desk, we plan to carry out simulated experiments for performance evaluation and compare the results, and design and verify a provably secure encryption mechanism.

Acknowledgments

This paper is extended and improved from accepted paper of ICCIT2007, GST2015 conference. This research was supported by Basic Science Research Program through the

National Research Foundation of Korea(NRF) funded by the Ministry of Education (2013R1A1A4A01013587). Corresponding author: Namje Park (namjepark@jejunu.ac.kr)

References

[1] Dong Hyeok Lee, You Jin Song, Sung Min Lee, Taek Yong Nam, Jong Su Jang, "How to Construct a New Encryption Scheme Supporting Range Queries on Encrypted Database1", Proceedings of the 2007 International Conference on Convergence Information Technology **(2007)**, pp. 1402-1407.

[2] Agrawal, R. *et al*., Order preserving encryption for numeric data. In Weikum, G., K¨onig, A., and Deßloch, S., Eds., Proc. of the ACM SIGMOD 2004, Paris, France. ACM (2004) pp. 563.

[3] E. Damiani, S. D. C. di Vimercati, S. Jajodia, S. Paraboschi, and P. Samarati. Balancing confidentiality and efficiency in untrusted relational dbmss. In Proc. of the 10th ACM Conf. on Computer and Communications Security (CCS), October 2003.

[4] Damiani, E. *et al*., Implementation of a storage mechanism for untrusted DBMSs. In Proc. of the Second International IEEE Security in Storage Workshop, Washington DC, USA. IEEE Computer Society (2003).

[5] J. Domingo i Ferror. A new privacy homomorphism and applications. Information Processing Letters, 60(5):277–282,

[6] D. X. Song, D. Wagner, and A. Perrig. Practical techniques for searches on encrypted data. In IEEE Symp. on Security and Privacy, Oakland, California (2000).

[7] H. Hacigumus, B. R. Iyer, C. Li, and S. Mehrotra. Executing SQL over encrypted data in the database-service-provider model. In Proc. of the ACM SIGMOD Conf. on Management of Data, Madison,Wisconsin (2002).

[8] Iyer, B. *et al*., A framework for efficient storage security in RDBMS. In Bertino, E. *et al*., Eds., Proc. of the International Conference on Extending Database Technology (EDBT 2004), volume 2992 of Lecture Notes in Computer Science, Crete, Greece. Springer (2004)

[9] Sun S. Chung, Gultekin Ozsoyoglu, Anti-Tamper Databases: Processing Aggregate Queries over Encrypted Databases, EECS Department, Case Western Reserve University, Cleveland Ohio, U.S.A., ICDEW'06, IEEE (2006).

[10] Aggarwal, G. *et al*.. Two can keep a secret: a distributed architecture for secure database services. In Proc. of the Second Biennal Conference on Innovative Data S

[11] Jens K. Jensen, Mikael Lind, Kwangil Lee, Jin Hyoung Park, Per Setterberg : How the Maritime Cloud supports e-navigation. E-NAV16-Task 5.1.19 (2015)

[12] Jens K. Jensen, Mikael Lind, Kwangil Lee, Jin Hyoung Park, Per Setterberg : A Maritime Infrastructure Framework. E-NAV16-9.24, Task 5.1.19 (2015)

[13] Jeongho Kim : The weight of the mobile device user authentication protocol study the cloud service communications environment. Soongsil university thesis (2015)

[14] Park N., Cho, S., Kim, B., Lee, B., Won, D., Security Enhancement of User Authentication Scheme using IVEF in Vessel Traffic Service System, Lecture Notes in Electrical Engineering, 203 (2012).

[15] Kim, K., Kim, B., Lee, B., Park, N., Design and Implementation of IVEF Protocol using Wireless Communication on Android Mobile Platform, Communications in Computer and Information Science 339 (2012).

[16] Kang, T., Park, N., Design of J-VTS Middleware based on IVEF Protocol, Lecture Notes in Computer Science,Vol. 7861, (2013), pp.723-729.

[17] Park, N., Kwak, J., Kim, S., Won, D., Kim, H., WIPI Mobile Platform with Secure Service for Mobile RFID Network Environment, In: Shen, H.T., Li, J., Li, M., Ni, J., Wang, W. (eds.) APWeb Workshops 2006. LNCS, Springer Heidelberg, vol. 3842, (2006), pp. 741–748.

[18] Kim, K., Kim, J., Lee, B., Park, N., Performance Enhancement of Wireless IVEF Protocol using XmlPullParser based on Android Mobile Platform, 2013 Korea Information Science Society Fall Conference 2013, (2013), pp. 350-352.

[19] Park, N., Security scheme for managing a large quantity of individual information in RFID environment, In: Zhu, R., Zhang, Y., Liu, B., Liu, C. (eds.) ICICA 2010. CCIS, Springer Heidelberg, vol. 106, (2010), pp. 72–79.

[20] Park, N., Secure UHF/HF Dual-band RFID: Strategic Framework Approaches and Application Solutions, In: ICCCI 2011. LNCS, Springer Heidelberg,Vol.6922, (2011), pp. 488-496.

[21] Lee, J., Design and Implementation of Efficient Mobile E-book Viewer Using Mobile App Framework, Gachon University Graduate School (2012).

[22] Park, N., Implementation of Terminal Middleware Platform for Mobile RFID computing, International Journal of Ad Hoc and Ubiquitous Computing , Vol. 8, No.4, (2011), pp. 205–219.

[23] Park, N., Kim, Y., Harmful Adult Multimedia Contents Filtering Method in Mobile RFID Service Environment, In: Pan, J.-S., Chen, S.-M., Nguyen, N.T. (eds.) ICCCI 2010, LNCS(LNAI), Springer Heidelberg, vol. 6422, (2010), pp. 193–202.

[24] IEC, Maritime navigation and radio communication equipment and systems-Automatic identification systems(AIS)-Part 2: Class A ship borne equipment of the universal automatic identification

system(AIS-Operational and performance requirements, methods of test and required test results, IEC 61993-2 1st Ed., IEC (2001).
[25] Park, N., Song, Y., AONT Encryption Based Application Data Management in Mobile RFID Environment, In: Pan, J.-S., Chen, S.-M., Nguyen, N.T. (eds.) ICCCI 2010, LNCS(LNAI), Springer, Heidelberg, vol. 6422, (2010), pp. 142–152.
[26] Ornulf Jan Rodseth, A Maritime ITS Architecture for e-Navigation and e-Maritime: Supporting Environment Friendly Ship Transport, IEEE ITS Conference 2011 (2011), pp. 1156-1161.
[27] Park, N., Customized Healthcare Infrastructure Using Privacy Weight Level Based on Smart Device, Communications in Computer and Information Science, Springer, vol. 206, (2011), pp. 467–474.
[28] Zeng D, Chawathe S. Hua H, Fei-Yue W., Protecting Transportation Infrastructure, IEEE Intelligent Transportation Systems 2007 (2007), pp 8-11.
[29] Park, N., Secure Data Access Control Scheme Using Type-Based Re-encryption in Cloud Environment. Studies in Computational Intelligence, Springer, vol. 381, (2011), pp. 319–327.
[30] Lee, B., Han, J., Jo, H., Park, N., A Security Architecture of the inter-VTS System for shore side collaboration of e-Navigation, Journal of navigation and port research, vol.36, no.1, (2012), pp.1-7.
[31] Park, N., Song, Y., Secure RFID Application Data Management Using All-Or-Nothing Transform Encryption, In: Pandurangan, G., Anil Kumar, V.S., Ming, G., Liu, Y., Li, Y. (eds.) WASA 2010, LNCS, Springer, Heidelberg, vol. 6221, (2010), pp. 245–252.
[32] Garnier B., Andritsos F., A Port Waterside Security Systemic Analysis, IEEE WSS Conference2010 (2010), pp. 1-6.
[33] Park, N., The Implementation of Open Embedded S/W Platform for Secure Mobile RFID Reader, The Journal of Korea Information and Communications Society, Vol.35, No.5, (2010), pp.785–793.
[34] Lee, B., Han, J., Jo, H., Design of situation awareness and aids to navigation structure of VTS for maritime safety, The Journal of The Korean Institute of Communication Sciences, vol. 35, no. 7, (2010), pp. 1073-1080.
[35] Park, N., Song, Y., Park, K., Secure Distributed Data Management Architecture Using AONT Encryption in Smart Grid Environment, The Journal of the Korea Contents Association, vol.10, no.9, (2010), pp. 57-67.
[36] Seom, G., Seo, S., Embodiment direction of Next e-Navigation, Journal of the Institute of Electronics and Information Engineers, Vol.34, No.11, (2007), pp. 37-45.
[37] Park, N., Implementation of Personalized Advertisement and Information Application Services Using RFID Virtual Tag, Journal of the Korea Society of IT Services, vol.8, no.4, (2009), pp. 151-163.
[38] Arifin B., Ross E., Brodsky Y., Data security in a ship detection and Identification system, IEEE RAST2011 (2011), pp. 634-636.
[39] Park, N., User Privacy Preserving Mobile RFID Personal Information Security Service System, Journal of Korean Institute of Information Technology, vol.8, no.10, (2010), pp. 87-96.
[40] Lee, B., Park, N., Security Architecture of Inter VTS Exchange Format Protocol for Secure u-Navigation, Lecture Notes in Electrical Engineering, Volume 181, (2012), pp. 229-236.
[41] Park, N., UHF/HF Dual-Band Integrated Mobile RFID/NFC Linkage Method for Mobile Device-based Business Application, The Journal of The Korean Institute of Communication Sciences, vol.38, no.10, (2013), pp. 841-851.
[42] Carter B., Green S., Leeman R., Chaulk N., SmartBay:Better Information - Better Decisions, IEEE OCEANS 2008 (2008), pp 1-7.
[43] Park, N., Analysis of Privacy Weakness and Protective Countermeasures in Smart Grid Environment, Journal of Korean Institute of Information Technology, vol.8, no.9, (2010), pp. 189-197.
[44] Frejlichowski D., Lisaj A., Analysis of lossless radar images compression for navigation in marine traffic and remote transmission, IEEE Radar Conference 2008 (2008), pp. 1-4.
[45] Park, S., Park, N., Investigating and Improving the Performance of Mobile VTS Service Platform, 2014 International Conference on Platform Technology and Service (PlatCon-14) (2013) Feb. 11-13; Jeju, Korea.
[46] Park, N., Implementation of Inter-VTS Data Exchange Format Protocol based on Mobile Platform for Next-generation Vessel Traffic Service System, Information, Vol.17, No.10(A), (2014), pp. 4847-4856.
[47] Park, N., Kim, M., Implementation of load management application system using smart grid privacy policy in energy management service environment, Cluster Computing, Vol.17, (2014), pp. 653-664.

Authors

Donghyeok Lee, received the BSc degree in information industry from dongguk university, Korea, and received his M.S. degrees in E.C.T from dongguk university in 2007, respectively. He is a researcher, STS research center at jeju national university since 2015. Prior to joining the researcher at jeju univ., he had worked as a researcher at KT co. ltd. for 7 year. And he had an appointment as the researcher of the information security research division of the Electronics and Telecommunication Research Institute for 1 year. He has many talks related in information security technologies, cloud security.

Namje Park, received the BSc degree in information industry from Dongguk University, Korea in 2000, and received his M.E., and Ph.D. degrees in Information Engineering from Sungkyunkwan University in 2003, and 2008 respectively. He is a Professor of Department of Computer Education in Teachers College at Jeju National University since 2010. He has been serving as a Research Scientist of Arizona State University since 2010. Prior to joining the researcher at ASU, he had worked as a post-doc at University of California, Los Angeles for 1 year. And he had an appointment as the senior engineer of the information security research division of the Electronics and Telecommunication Research Institute for 6 years. He is concerned in the information security technology field for the mobile environments, IoT system, Smart Grid, Mobile XML Security, Web Services Security, Ubiquitous computing including RFID/WSN and a variety of cryptographic technologies. He has many talks related in mobile and information security technologies, computer education.

