Advances in Internet of Things, **2012, 2, 1-7**
http://dx.doi.org/10.4236/ait.2012.21001 Published Online January 2012 (http://www.SciRP.org/journal/ait)

Cyber-Physical-Social Based Security Architecture for Future Internet of Things

Huansheng Ning, Hong Liu
School of Electronic and Information Engineering, Beihang University, Beijing, China
Email: ninghuansheng@buaa.edu.cn, liuhongler@ee.buaa.edu.cn

Received December 7, 2011; revised December 28, 2011; accepted January 15, 2012

ABSTRACT

As the Internet of Things (IoT) is emerging as an attractive paradigm, a typical IoT architecture that U2IoT (Unit IoT and Ubiquitous IoT) model has been presented for the future IoT. Based on the U2IoT model, this paper proposes a cyber-physical-social based security architecture (IPM) to deal with Information, Physical, and Management security perspectives, and presents how the architectural abstractions support U2IoT model. In particular, 1) an information security model is established to describe the mapping relations among U2IoT, security layer, and security requirement, in which social layer and additional intelligence and compatibility properties are infused into IPM; 2) physical security referring to the external context and inherent infrastructure are inspired by artificial immune algorithms; 3) recommended security strategies are suggested for social management control. The proposed IPM combining the cyber world, physical world and human social provides constructive proposal towards the future IoT security and privacy protection.

Keywords: Internet of Things; Physical; Social; Cyber, Security; Architecture

1. Introduction

The Internet of Things (IoT) becomes an attractive research topic, in which the real entity in physical world becomes virtual entity in cyber world, and both physical and digital entities are enhanced with sensing, processing, and self-adapting capabilities to perform interaction through special addressing scheme [1]. Along with the combination of Internet and modern sensor technologies such as Radio Frequency Identification (RFID), Near Field Communication (NFC), and Wireless Sensor and Actuator Networks (WSAN), IoT itself is suffering from more rigorous security challenges. Several issues in terms of system architecture, standard, and human involvement are subsequently raised. The following security problems seem to be intense speculations, such as how to design appropriate security framework for things' intelligent applications? What is advanced security technology applied into mass data processing? How to maintain a balance between things' high security requirements and supporting infrastructures' hardware limitation? And how human society securely participates in both cyber and physical worlds with interconnection?

Such significant obstacles influence the development of the future IoT, along with the exposure of mass data which causes various potential vulnerabilities from robust adversaries. Besides, resource restrictions including heterogeneous networks and sensor nodes, communication channels/interfaces, bandwidth, storage, and energy, may also induce unique model design. Towards the general IoT, studies on its architecture model, standard, communication protocol, and network management have been researched [2-5]. Towards the particular IoT security, there are several open issues such as cryptographic algorithms, authentication protocols, access control, trust/privacy, and governance frameworks [6]. Several researches mainly focus on specific communication techniques (e.g., WLAN, RFID) [7,8], detailed cryptographic mechanisms (e.g., key management) [9], and practical applications (e.g., supply chain management, multimedia traffic) [10,11]. Meanwhile, the security frameworks in traditional networks can also provide merits for IoT security protection. However, security issue towards the future IoT is not a simple technically tough problem, but a multidimensional topic which combines the information security, network security, infrastructure security, and management security. Most existent schemes provide solutions for special communication techniques or applications, which may lack universality for the complicated system. Thus, we will establish an integrated security architecture to promote universal security consideration for the future IoT.

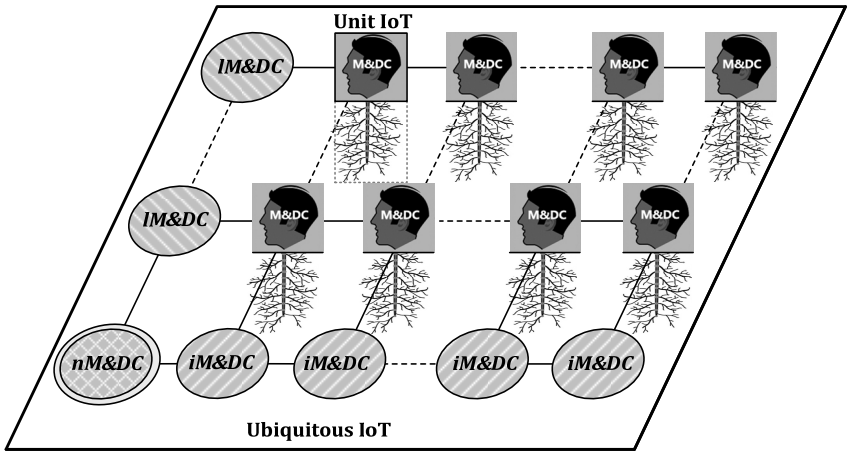
In the paper, we focus on a typical future IoT architecture (short for U2IoT) which comprises two subsystems that Unit IoT and Ubiquitous IoT [12]. In the U2IoT model, conceptions of mankind neural system and social organization framework are introduced for the future IoT. Thereafter, we propose a systematic security architecture

(named IPM) by integrating the awareness and interactivity of cyber world, physical world, and human social into the U2IoT model. Meanwhile, the proposed IPM is presented with embedded interactions among information, physical, and management. Specifically, 1) information security model with the considerations for basic and advanced security requirements that are mapped into the security layer to deal with sensing, networking, application, and social attribution; 2) physical security including external context and inherent infrastructure are inspired by artificial immune, and it ensures that the things should be adaptable to dynamic semantic contexts with innate and adaptive immunities against malicious attacks; 3) management security provides recommended strategies for hierarchical classified scenes with rationality and compatibility. IPM realizes the unison of cyber world, physical world and human social to guarantee security and privacy for U2IoT.

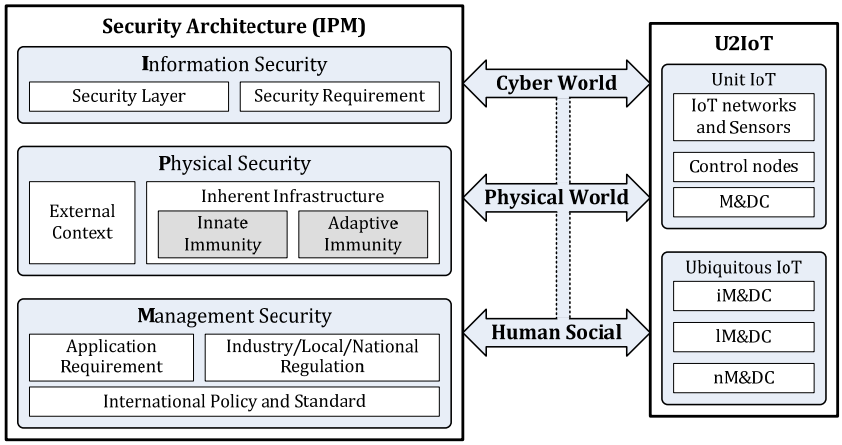
The remainder of the paper is organized as follows. In Section 2, we illustrate the existent U2IoT model, and propose the security architecture (IPM). The main features of IPM referring to information security, physical security, and management security are given in Section 3. Finally, Section 4 draws a conclusion.

2. Proposed Security Architecture for U2IoT

The U2IoT model is shown in **Figure 1(a)**, which is essentially a heterogeneous system including Unit IoT and Ubiquitous IoT. Thereinto, Unit IoT resembling human neural network, refers to the basic cell providing solutions for special applications. Ubiquitous IoT includes the industrial IoT, local IoT, national IoT, and global IoT which is integration of multiple Unit IoTs with ubiquitous features, and it is similar to the social organization framework. Concretely, Unit IoT comprises IoT networks and sensors, distributed control nodes, and management and centralized data center (M&DC), and Ubiquitous IoT respectively includes iM&DC, lM&DC, and nM&DC, for the industry, local, and national IoTs. **Figure 1(b)** illustrates the proposed security architecture (IPM) that addresses U2IoT security in three perspectives.



(a)



(b)

Figure 1. U2IoT model and its security architecture (IPM). (a) The U2IoT (Unit IoT and Ubiquitous IoT) model; (b) The proposed security architecture (IPM) based on U2IoT.

- **I:** Information security includes two perspectives (*i.e.*, security layer and security requirement). Awareness of information data is captured, interpreted, and represented by things' capability, along with aggregation algorithms, protocols, and functions are included for intelligent information interactions.
- **P:** Physical security relates to environmental monitoring, motion detection, localization, tracking, perimeter control, and consumption supervision. The concept of artificial immunity is applied to detect passive and active defenses for maintaining homeostasis.
- **M:** Management security provides the recommended application requirement, industry/local/national regulation, and international policy and standard to guide activities and events in the human social.

In IPM, human social activities occurring in physical world are identified and mapped into the unique cyber world, which realizes harmonious unification of human, network and things. Such triple relationships of entity in U2IoT, makes entity identification and service discovery are effectively performed in current cyber-physical world, and are easily to extend to human social and its social networks. The security aspects underline main characteristics of U2IoT entities, as shown in **Table 1**.

Table 1. The main characteristics of U2IoT entities.

Characteristics	Descriptions
Cyber, Physical, Social Co-existence	Any entity exists in the physical world, along with its existence in the cyber world in the virtual form via specific communication and network technologies; and the entity also has its social identity and attribution which not isolated from cyber and physical attribution.
Connectivity, and Interactivity	Any entity can interoperate and collaborate with other heterogeneous entities within its access domain, and the entities are interrelated and interact on each other.
Space-time Consistency	Any entity can dynamically interact with other entities at any time, any place, and in any mode; the entity can freely enter/leave the networks without influencing the ongoing communications; and synchronization is needed during heterogeneous network accessing.
Multi-identity Status	Any entity has multi-identity statuses that include a unique core identity, and other temporary identities according to its underlying applications.

3. Proposed Security Architecture: IPM

3.1. Information Security

Information security protects both raw data and contextualized information, and an information security model that comprises U2IoT, security layer, and security requirement is established in **Figure 2**.

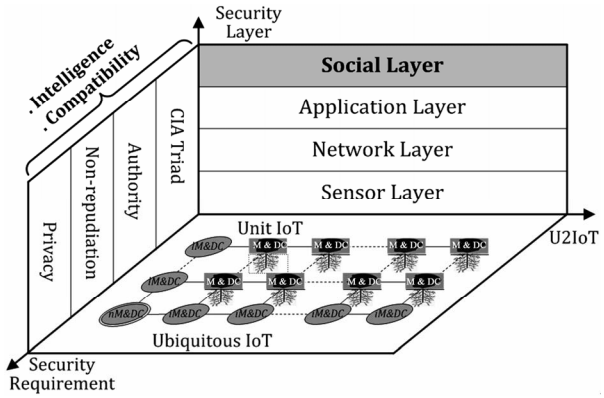


Figure 2. Security layer and security requirement.

1) *Considering Social Factor for Security Layer*: U2IoT is generally divided into four layers as follows.

- **Sensor layer:** it comprises generalized sensors and gateways to perform entity identification and service discovery. The function of sensor layer is to perceive the entities, to extract information, and to realize semantic resource discovery. The sensor techniques are applied to realize effective integration and interaction adaptation of the collected uncertain information.
- **Network layer:** it includes network interfaces, communication channels, network management, information maintenance, and intelligent processing. The centralized, distributed, and hybrid network topologies are involved to assist monitoring and maintaining the real-time network configuration. The network layer ensures reliable information transmission by adopting data coding, extraction, fusion, restructuring, mining, and aggregation algorithms. The main function is to transfer and process the information obtained by sensor layer, and to realize data exchange among large-scale heterogeneous networks.
- **Application layer:** it exports functionalities for specific applications, and provides embedded interfaces for infrastructures to perform testing, monitoring, or auditing applications. The standard protocols and service composition technologies are applied to realize the integration between heterogeneous distributed networks and its applications, such as logistics monitoring, smart grid scheduling, intelligent search, and cloud computing. Such applications should adapt in dynamic environments.

Particularly, an additional social layer on the top of the architecture considers the social attribution in U2IoT. The social layer is mainly devoted to communicate among objects and other supporting networks to perform correlation between the cyber individual and the corresponding profile in social networks. Correlative social attributions are granted to each entity, and hierarchical management and data centers operate overall security considerations. In social layer, diverse interfaces are accessed by a real entity which acts on its corresponding cyber entity to control its behaviors. Meanwhile, other social composi-

tions are also considered, such as ownership control management, social relationship modeling, and entity behavior formalization.

In the perspective of information security, the sensor and network layers specify multiple networks and sensor nodes, which are used to capture data streams, to detect activities and events with identification algorithms, and to realize specific application functions. Core of data acquiring is sensor technology (e.g., RFID, WSN, femtocell) and Global Sensor Network (GSN) middleware, whose security is challenged by constrained resources. Note that distributed control nodes provide the capabilities to survive under formidable conditions, and by information security controls such as error detection and correction, random access control, and fault tolerance are recommended.

2) *Adding Intelligence and Compatibility for Security Requirement*: Elements of security requirements include CIA Triad, authority, non-repudiation, and privacy. Additional requirements that intelligence and compatibility are added into advanced security considerations, which provide reliable security and privacy protection. **Table 2** presents the comparison of security requirements among the traditional network, general IoT, and U2IoT.

Intelligence represents that an entity should own abstract capabilities including self-learning, self-adapting, and self-reasoning to adapt itself to dynamic semantic environments. In non-deterministic channels and open interfaces, virtual intelligent entities should be autonomously interconnected in U2IoT. The embedded intelligence makes the entity have strong efficacies to adapt dynamic information that is the mapping of environment interactions, social connections, and human behaviors.

Table 2. Comparision of security requirements.

Requirement	Traditional network [13]	General IoT [14,15]	Additional Requirements in U2IoT
CIA Triad	a) Data Confidentiality: Protect data from unauthorized disclosure; b) Data Integrity: Ensure correctness or accuracy of data; c) Data Availability: Ensure that there is no denial of authorized access to network elements, information flows, services and applications.	Bottom-up cryptographic algorithms should be recommended for heterogeneous network infrastructure: - Key management infrastructures; - Block/Stream ciphers algorithms; - Digital signatures; - Hash function; - Pseudo-random number generators.	a) Ubiquitous forward, backward, and ongoing security: Ensure ubiquitous unlinkability among the prior, later, and the current interrogations, which cannot be correlated. b) Dynamic session freshness: Ensure session freshness check into the integrity check mechanism. c) Self/Non-self identification: Ensure only authorized self entity can access the network resources and services, and eliminate any non-self entity.
Authority	a) Authentication: Ensure that only legal entities can access network resources to exclude any illegal entity from the networks; b) Authorization: Realize different access control among legal entities.	Advanced authentication and authorization mechanisms: a) Assignment of users contributions to a single contributor; b) Upgrading users trust status without revealing identities to service provider.	a) Intelligent access control: Use heterogeneous authentication and identification for semantic access control on legal information interoperation; b) Compatible certificate authority: Authenticate entity and grant authority to access system resources; c) Hierarchical authentication: Establish hierarchical mutual authentication: individual/group authentication, and source/terminal authentication.
Non-repudiation	a) Providing available proofs to prevent any entity from denying having performed a particular behavior related to the exchanged messages; b) Ensuring the availability of evidence that can be presented by a trusted third party, and proving that an entity's behavior has occurred before.		Social attribution: Assign social attribution to an entity's cyber behaviors, which are applied for compatible social computing and behavior supervision.
Privacy	Any sensitive information is protected, that may be derived from the observation of network activities.	Dynamic Consent Tool: Permit certain services or applications to access as little or as much of that the data as desired.	a) Transparency: Let user know which entity contains its related data, when and where the entity has used the data, and how the entity realizes the specific function. b) Traceability: Let the entity know the network and service information that it has even connected.

Compatibility requires that an entity has appropriate interconnection and interoperability to adjust to heterogeneous data formats, interfaces, channels, and networks in U2IoT model. The supplemental requirements address advanced criterions for information interaction. Meanwhile, compatibility can be promoted to scalability, expansibility and modularity among heterogeneous entities and the multi-context environments.

The both requirements operate together to promote the security and privacy preservation: 1) ensure diverse entities own artificial intelligence and autonomous security control against the strong attackers; 2) ensure heterogeneous entities, networks and applications establishing reliable interconnection without compromising any communication data and individual privacy.

3.2. Physical Security

Physical security is denoted in external context and inherent infrastructure, in which human-like security immune safeguard is achieved.

1) *External Context*: Simple context and complex context are specified in [16], in which the former determines the basic identity, location, and entity status by a single parameter; the latter refers to geographical structures, traceability information, and real world conditions. Above both contexts are refined to support creating, debugging and integrating applications of Ubiquitous IoT, and provide interface interconnection and restriction for Unit IoTs. In U2IoT model, the borders of each entity's external context merge even vanish, and the obscure contexts spanning from an individual, an object, or an environment to social relationships, should support the hierarchical IoT subsystem. Particularly, intrusion detection algorithm is significant to acquire context information for monitoring sensors behavior, discover control node breaches, and other potential vulnerabilities.

2) *Inherent Infrastructure*: Artificial immune security system as computational intelligence is applied to analyze inherent infrastructure, which belongs sensorial system inspired by principles and processes of the natural immune system. Typical algorithms (e.g., clonal selection, negative selection, and immune network) exploit the immune system's features of detection, learning and memory to constitute innate immunity and adaptive immunity. Physical security issues such as intrusion detection, adaptive disposition, context-driven feedback, and error recovery can be addressed as follows.

- **Innate immunity:** It provides basic barriers against foreign invasions in real-time environment, and it is triggered upon sensors identifying abnormal or malevolent attacks by the intelligent pattern recognition mechanisms. Co-stimulation signals are transmitted to distributed control nodes via Unit IoT networks, and then rejection reactions are performed by management centers. During defense operations, activation thresholds are defined to ensure the detection optimization, and fuzzy diagnosis can also applied for imperfect detection. Note that the innate immune defense is non-specific, meaning that U2IoT model responds to the various attacks in a general scheme. Such system cannot afford long-lasting immunity against a certain attack. The innate immune system is dominant to confront the dynamic contexts and continuously refreshing threats.
- **Adaptive immunity:** It refers to acquired resistance, where an attack is marked as a specific signature. Selective response requires recognizing non-self element during attack prototype presentation. If U2IoT has been infected by the same or similar invasion, specific memory module would be aroused to eliminate damaging effects by generating improved response to return the system into secure state. Adaptive immunity executes fuzzy diagnosis to variations of the same former attack, and optimal stimulation such as subsidiary vaccination is available by updating M&DCs' profile databases.

According to both innate and adaptive immunities [17], three main features should be achieved in U2IoT model.

***Multithreaded and Hybrid Configuration*:** The U2IoT model may apply multithreaded security algorithms for the massively parallel network architecture that comprises a diverse set of components. The components are organized in hybrid mode, in which both centralized and distributed configurations are included. Towards Unit IoT, the allocation of the sensing and query processing is performed by the central M&DC. Towards Ubiquitous IoT, the industry IoTs and local IoTs are relatively independent, which commonly construct national IoT. In U2IoT model, such multithreaded and hybrid configuration are throughout all the networks, sensor and control nodes, and management and data centers.

***Multilayered and Autonomous Organization*:** There is no single security mechanism that offers complete immunity. Therefore, multilayered protection should independently operate for all-round safeguards. During the layered organization, U2IoT model autonomously makes its decisions by detecting potential attacks and proposing feasible solutions based on artificial immune algorithms.

***Heterogeneity*:** U2IoT model should be accessible by a large number of heterogeneous communication technologies with different networks, channels, interfaces, and hardware/software capabilities. Such heterogeneity of entities adds complexity to its security situations, which makes that a certain attack may simultaneously act on multiple entities in different IoTs, but the attack cannot act on all the involved IoTs. The immune protection ensures that the

entire heterogeneous components cannot be corrupted due to the same attacker.

3.3. Management Security

Towards the future IoT, it is scarcely possible to establish a uniform security protocol as Internet, just like different nations and/or regions cannot adopt an identical safety precaution. Hence, distinctive management mechanisms are significant for both security and interconnection requirements. Due to the limitations of technological approaches, appropriate management should couple with the implementation of information security and physical security. Security strategies working on human behaviors should be considered to ensure that virtual cyber data is adapted to the real physical contexts.

Application requirement for distributed sensor and control nodes provides generic/specific protection. IPM is of benefit to practical application security, such as historical query, project management, risk assessment, software design, and system certification. For a specific scenario, customized requirements are assigned to describe the authorized/-unauthorized usage in a particular organization or individual. Additionally, application requirement should also be consistent with privacy prevention which realizes that the sensitive data is exchanged, stored, and shared without revealing any user privacy.

Industry/Local/National regulation mainly serves for iM&DC/lM&DC/nM&DC to provide rules and guidance for U2IoT. It takes legal or disciplinary actions to resist the offensive individuals or institutions which do not comply with the regulations. Thereinto, industry regulation describes approaches to achieve high-level security objective for a special industrial authority organization, such as agriculture, energy, and military. For instance, in the chemical hazards medical management, the regulations require certain parameters (e.g., temperature, vibrations, and relative proximity), caution the users for violation thresholds, and guarantee system security by warning abnormal implement and configuration. Thereinto, local regulation should coincide with local customs and practices to adopt humanistic perspectives for designing, implementing, and maintaining the local IoTs. National regulation governs guidelines to realize nation-to-nation compatibility, and formal memorandum of agreements needs to be shared across national boundaries. Additionally, customized roles and responsibilities can be codified among different nations.

International policy considers the global IoT consociation during connectivity and consistency of nM&DC and global IoT. Moreover, international standards should be addressed by governments to promote security confidence and ensure interoperability. It indicates that a general international governance framework with reasonable enforcement policies will provide permanent mechanism towards security protection.

4. Conclusion

In this paper, a security architecture IPM is proposed for U2IoT model. The main purpose is to establish an integrated security architecture with considerations on cyber-physical-social world. The proposed IPM comprises three essential security perspectives (*i.e*., information, physical, and management), in which three-dimensional information security model introduces social layer, and intelligence and compatibility for security consideration; artificial immunity is applied to describe physical security; and a series of social strategies are recommended to achieve management security.

5. Acknowledgements

This work is jointly funded by National Natural Science Foundation of China (NSFC) and Civil Aviation Administration of China (CAAC) (61079019), and is also supported by the Fundamental Research Funds for the Central Universities (YWF-11-02-264).

REFERENCES

[1] H. Ning, "RFID Major Projects and State Internet of Things (Second Edition)," China Machine Press, Beijing, 2010.

[2] J. Ma, J. Wen, R. Huang and B. Huang, "Cyber-Individual Meets Brain Informatics," *IEEE Intelligent Systems*, Vol. 26, No. 5, 2011, pp. 30-37. doi:10.1109/MIS.2011.55

[3] L. Atzori, A. Iera and G. Morabito, "The Internet of Things: A Survey," *Computer Networks*, Vol. 54, No. 15, 2010, pp. 2787-2805. doi:10.1016/j.comnet.2010.05.010

[4] D. Bandyopadhyay and J. Sen, "Internet of Things: Applications and Challenges in Technology and Standardization," *Wireless Personal Communications*, Vol. 58, No. 1, 2011, pp. 49-69. doi:10.1007/s11277-011-0288-5

[5] H. Ning, N. Ning, S. Qu, Y. Zhang and H. Yang, "Layered Structure and Management in Internet of Things," *Proceedings of Future Generation Communication and Networking* (*FGCN* 2007), Jeju, 6-8 December 2007, pp. 386-389.

[6] R. Roman, P. Najera and J. Lopez, "Securing the Internet of Things," *Computer*, Vol. 44, No. 9, 2011, pp. 51-58. doi:10.1109/MC.2011.291

[7] R. Kaur, "Advances in Intrusion Detection System for WLAN," *Advances in Internet of Things*, Vol. 1, No. 3, 2011, pp. 51-54. doi:10.4236/ait.2011.13007

[8] G. P. Hancke, K. Markantonakis and K. E. Mayes, "Security Challenges for User-Oriented RFID Applications within the 'Internet of Things'," *Journal of Internet Technology*, Vol. 11, No. 3, 2010, pp. 307-313.

[9] R. Roman, C. Alcaraz, J. Lopez and N. Sklavos, "Key Management Systems for Sensor Networks in the Context of the Internet of Things," *Computers & Electrical Engineering*, Vol. 37, No. 2, 2011, pp. 147-159. doi:10.1016/j.compeleceng.2011.01.009

[10] L. D. Xu, "Information Architecture for Supply Chain Quality Management," *International Journal of Production Research*, Vol. 49, No. 1, 2011, pp. 183-198. doi:10.1080/00207543.2010.508944

[11] L. Zhou and H. C. Chao, "Multimedia Traffic Security Architecture for the Internet of Things," *IEEE Network*, Vol. 25, No. 3, 2011, pp. 35-40. doi:10.1109/MNET.2011.5772059

[12] H. Ning and Z. Wang, "Future Internet of Things Architecture: Like Mankind Neural System or Social Organization Framework?" *IEEE Communications Letters*, Vol. 15, No. 4, 2011, pp. 461-463. doi:10.1109/LCOMM.2011.022411.110120

[13] Draft ITU-T Recommendation X.805 (Formerly X.css), Security Architecture for Systems Providing End-to-End communications, 2003.

[14] D. Havlik, S. Schade, Z. A. Sabeur , P. Mazzetti, K. Watson, A. J. Berre and J. L. Mon, "From Sensor to Observation Web with Environmental Enablers in the Future Internet," *Sensors*, Vol. 11, No. 4, 2011, pp. 3874-3907. doi:10.3390/s110403874

[15] L. Atzori, A. Iera and G. Morabito, "The Internet of Things: A Survey," *Computer Networks*, Vol. 54, No. 15, 2010, pp. 2787-2805. doi:10.1016/j.comnet.2010.05.010

[16] N. Koshizuka and K. Sakamura, "Ubiquitous ID: Standards for Ubiquitous Computing and the Internet of Things," *IEEE Pervasive Computing*, Vol. 9, No. 4, 2010, pp. 98-101. doi:10.1109/MPRV.2010.87

[17] P. K. Harmer, P. D. Williams, G. H. Gunsch, G. B. Lamont, "An Artificial Immune System Architecture for Computer Security Applications," *IEEE Transactions on Evolutionary Computation*, Vol. 6, No. 3, 2002, pp. 252-280. doi:10.1109/TEVC.2002.1011540

