Semantic Edge Computing and IoT Architecture for Military Health Services in Battlefield

Dhananjay Singh
Dept. of Electronics Eng.
Hankuk Univ. of Foreign Studies (HUFS), Korea
dan.usn@ieee.org

Gaurav Tripathi
Central Defense Lab.
Baharat Electr. Ltd., (BEL)
Ghaziabad, India

Antonio M. Alberti
ICT Lab, National Inst. of Tele.- INATEL
Brazil
alberti@inatel.br

Antonio Jara
Ins.of Info. System, HES-SO, Sierre
Switzerland
jara@ieee.org

***Abstract* —In this paper, we are visualizing a military health service (MHS) platform which is based on hierarchical IoT architecture. We propose a semantic Edge based network model which plays a significant role for communicating tactical and non-tactical piece of information over the network. Further, the exchange of information and subsequent data analysis on the MHS makes the system intelligent and smart. In any standard battlefield scenario, there is a command and control center that correlates the events happening in real time. We have made this command and control center as semantic edge component. This center is entrusted with making vital decisions on the tactical arena of the battlefield. The main aim of the proposed architecture is to provide secured zone to monitor soldiers health and their weapons conditions, respectively. We have also introduced the semantic edge computing mechanism to deal with the large amount of health data in terms of processing, storing and sharing information.**

Keywords- Internet of Things (IoT); Cloud Computing; Edge Computing; Battlefield; Military healthcare

I. INTRODUCTION

The defense of any nation is very vital for its survival. Apart from financial independence of the state, the borders of the nation must be guarded by latest technological assistance. Physically, the military personnel have to be in good health in all kinds of turbulent terrains. In any standard battlefield scenario, there is a command and control center that regulates the battlefield and takes tactical decisions of shuffling the reinforcements and chalk out their respective battlefield plans for an outright victory over their respective opponent [1]. We are talking about a software/hardware system and its implementation, where IoT services are used and are clubbed with semantic cloud-based solutions [2]. Generally, the sensors are supposed to provide lots of information about its respective environment and object concentration [3]. We are getting a step ahead with the latest use of Edge computing, which is the latest entrant in the storage and computing domain. Edge computing provides storage and services at the edge of the networks [4]. In this case, if there is a need of offline data analysis, the data from Edge can be transported to cloud for data mining purposes. Thus, a novel IT paradigm shift is occurring in ways where Edge and IoT are merged together to make the current as well as the future internet technologies even more exciting. An efficient IoT protocol needs to be developed between homogeneous devices (humans to humans, machine to machine, etc.) as well as cross protocol communication among heterogeneous devices (human beings to vehicles, kitchenware to shoes, vehicles to mobile phones, etc.). Ultimately, they communicate to the Edge nodes [4]. These nodes can then process the information and further communicate the data to the cloud for data mining process.

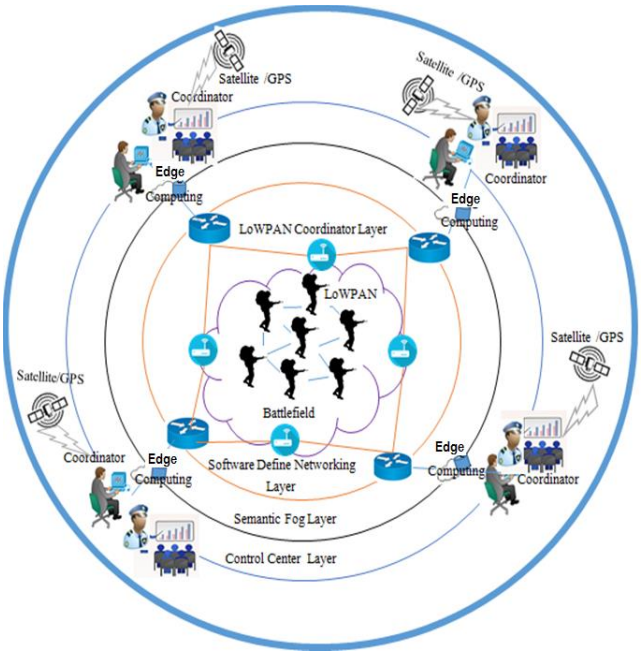

Fig.1. Overview of IoT architecture for military services.

In the Fig. 1, we have represented the hierarchical IoT architecture for military personnel health monitoring systems, which can collect the vital health parameters of every military personnel in the battlefield as well as their weapon status along with their geographical location. This data can be sent to semantic Edge computing over software defined networking (SDN) for analysis by their respective commanding officer and control center. The hierarchical IoT architecture has several tiers

with specific role for identification of soldier's to overall process refinement [6], making efforts for tactical advantage easy. We are visualizing sensors-tagged soldiers, which will become the sensor reports to the layered system. The hierarchical model employs sensors and smart embedded devices to monitor the soldier's health parameter and weapons conditions. This platform can make the battlefield systems aware of the overall health of their military personnel. This health sensing can be taken in to amount by the commanding officer for taking overall tactical decision in case of war [7]. All the above discussions are pointing out to the fact that we are actually moving towards the power to the edge concepts. These concepts talk about the technological advances which will eliminate the bandwidth constraints, and will aptly provide a platform for tactical information sharing and processing with minimal losses and latency [15].

The rest of this paper is organized as follows: Section II provides an insight to the motivation and their challenges of battlefield scenario. Section III gives general requirements impetus of military health services (MHS) based on semantic Edge for the IoT architecture. Section IV discusses the basic functionality of hierarchical IoT architecture for military and their related terminologies based on Edge computing. Section V brings out a discussion of semantic Edge computing for MHS. Section VI presents final remarks of proposed scenario and their challenges of security and privacy in Edge computing enabled IoT systems. Finally, we have concluded our work in and its future aspects in the Section VII.

II. Requirements of Military Healthcare Services

A. *Edge Computing*

Edge computing is popularly known to enable computing directly at the edge of the network, which can deliver new applications and services for billions of connected devices. Edge devices are usually set-top-boxes, access points, road side units, cellular base stations, etc [9]. However Edge computing can be termed as the extension of cloud computing, which occurs at the edge of the networks where a huge number of ubiquitous, homogeneous, heterogeneous and decentralized devices communicate among themselves to perform storage and information processing. Edge computing has the property of supporting mobility at the edge of the networks which is the basis of providing services in the military healthcare system. Interaction between Edge nodes is lot more low latency affair as compared to the application-cloud pair or Edge-cloud pair [10].

B. *Semantic Computing*

In the world of IoT, the smart and intelligent IoT applications must devise ways for machine-interpreted data for decision making. Also, they must adapt themselves to various situations and concepts. Different ontologies for specific domains are required for a better understanding. Semantic technologies can increase the level of reasoning of IoT elements and increase interoperability among a variety of applications and systems [16].

C. *Semantic Data Representation*

Uniform semantic web representations can be applied in the domain of IoT. The author of [17] has studied in detail about the different data formats for semantics for IoT.

D. *Ontologies*

Ontologies are used for organizing information. They can also be used for representing the knowledge formally. Ontologies enable sharing, merging and reusing of represented knowledge. W3C Semantic Web standard web ontology language (OWL)[18] is a knowledge representation language for sharing and providing knowledge in the form a machine can understand using their own parsers. There have been special efforts by Open Geospatial Consortium (OGC) sensor web enablement (SWE) Domain Working Group [19] and semantic sensor networks (SSN) Incubator Group [20] to facilitate interoperability of sensor networks by standardization and providing high level ontologies for appropriate service integration. There have been a classic survey on the utilization of semantic technologies in IoT in [21], which clearly brings out the fact that the semantic interpretation becomes important for interoperability of IoT systems.

E. *Semantic Edge Computing*

Semantic Edge means some meaningful understanding of the machines to machine communication and cross understanding of machine to humans communication. In the domain of military information exchange, it applies logical rules to decipher sensible information for proper execution of military services. This can be done at the Edge computing level itself. In the military healthcare services, the platform does not requires all the bulky data, periodically. The system should be event based and information collection should be based on querying.

F. *Body Area Network (BAN)*

The IEEE 802.15 working groups have been presented a standard communication protocol aptly suitable for low power devices and suitable operations on, in or around the human body (but not limited to humans) to facilitate a variety of applications including medical, consumer electronics, personal entertainment, and other. This BAN technology is used for bio-medical sensors, sports field, wireless audio transmission, and for personal devices. Each of the above mentioned applications have their unique set of requirements about bandwidth, latency, power usage and distance. The main role of device is to provide pervasive nature, it allow connectivity with existing IP-based networks [11].

G. *Software Defined Networks (SDN)*

SDN is an emerging approach for programmable networks and it is dynamic, manageable, cost-effective, and adaptable. In the SDN format, hardware is decoupled from software by providing network services [12]. Generally, hardware is supposed to increase the network bandwidth. To overcome these hardware limitations there is lot of work going on the software level, to increase the network bandwidth. The SDN is easily programmable, agile, and managed efficiently.

H. *Battlefield Monitoring System*

The battlefield consists of various objects ranging from military soldiers, military weapons, military communication equipment, and military sophisticated weapons from both sides of the fighting armies. In any battlefield, information is the power of military soldiers. Also, the capability to exchange information between military soldiers and control center is highly relevant. The battlefield objects and their information are highly secured due to software defined networking (SDN) based hierarchical IoT architecture [8].

I. *Hierarchical IoT Architecture*

It has to focus on specific functions in each layer to design a network topology in discrete layering forms. However, a typical hierarchical topology is a core layer of high-end routers and switches that are optimized for availability and performance. A distribution layer of routers and switches implement policies, i.e. an access layer that connects users via lower-end switches and wireless access points. For example, in a battlefield top tier (tier 0) can carry traffic across the enterprise (battlefield) backbone; medium-tier (tier 1 to n-1) can connect a specific zone; and End tier (last) can connect military soldiers weapons and their wearable devices [6].

III. HIERARCHICAL IOT ARCHITECTURE FOR MILITARY

The goal of the hierarchical military health service (MHS) is to facilitate understanding and communication among acquisition military managers, military theoreticians, war games designers, evaluation, and users of data fusion techniques to permit cost-effective system design, development, and operation. Fig. 2 shows the hierarchical MHS model where each layer has a specific role for identification of objects to overall process refinement of the platform. When we are talking about virtual sensors like all sensors-tagged soldiers, they will actually be the sensor reports to the layered system. The MHS system has utilized hierarchical model by using sensors as well as smart embedded device for sensing the events, soldiers health condition, and weapons for a better situational awareness. At the top layers these systems must combine sources data with varying temporal, spatial, spectral and radiometric characteristics.

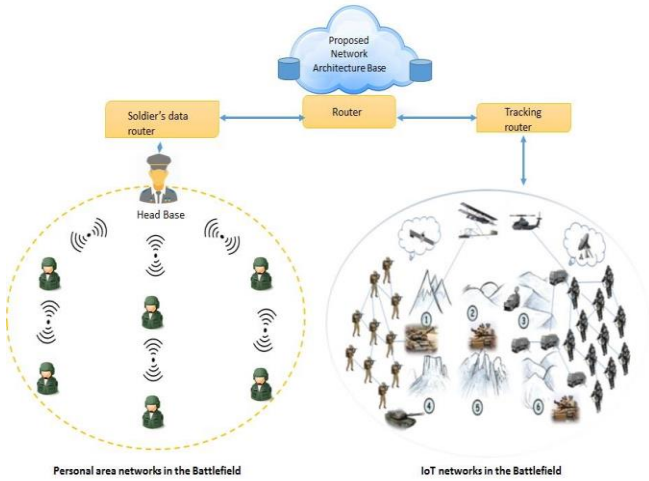

Fig. 2. An overview of hierarchical IoT architecture.

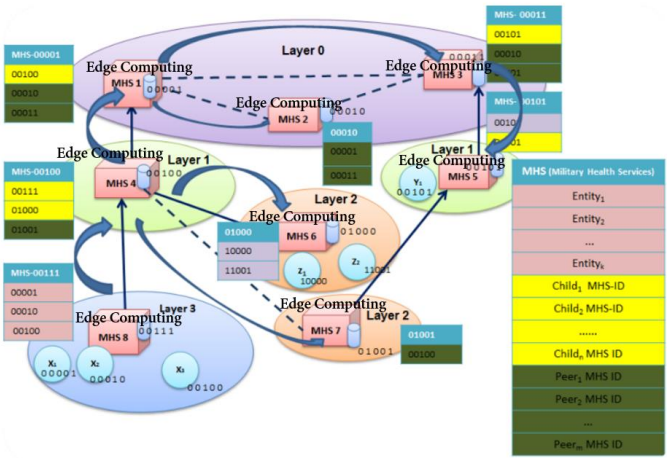

Fig.3. Hierarchical MHS layered structure based on edge computing.

Fig. 3 shows the overview of hierarchical MHS layered structure. In this structure, each layer has its set of MHS management station. There are two kind of relationship between MHS: parent-child and peer relations. Layer0 is the Top-Level-Layer where all MHS are fully peered and have parent relation. Layer1 and Layer2 are Intermediate Layers. They have both parent child relation and peer relation. Layer3 and Layer2 are leaf Layers and connected to entities. Therefore, a leaf layer cannot become a parent of another MHS. Each MHS has to store parent node entities and child node entities information and location as well as they can share their database with peer's node too. In general, if we denote layer (MHS) to be a layer of given MHS, then it should satisfy the relation Layer (MHS) = MAX (Layer (parents))+1, where parents mean parents MHS of a given MHS. This implies that whenever a new MHS is added, its parent should be in an one level upper Layer.

Algorithm-: Pseudocode for adding the entities from lower MHS layer to upper MHS layer into ***hierarchical IoT architecture***

T[i] ← i^{th} layer
W[i] ← i^{th} MHS server
T[i].W[j] ← j^{th} MHS server belonging to i^{th} layer
max_parent ← maximum no. of parent of any MHS
max_child ← maximum no. of child of any MHS
init(i,j) ← do the initialization of both *i* and *j*
add_child (i,j) ← make child of *i* also of *j*
while $i <$ max_parent, $j <$ max_child
do initialization (tier, IWSS)
input *a, b*
if $a < b$
add_child (T[b].W[i], T[a].W[j])
end if
end while

In a battlefield MHS scenario, to detect an isolated soldiers at a specific location and classifying it as at a risk level (or safe levels) and even identifying it specifically in a specific age bracket, it is all covered under an object assessment from lower Layer3. The unique tag number found and location would further indicate soldier's safety parameters levels, if not the exact level, and possibly the soldier disposition of a movement to contact. The impact assessment modules (at the surveillance

control room) use this information and then indicate that the route and risk levels detected by IoT based sensors are raising and emit an alert or an alarm. Thus, nearest patrolling unit would be directed to reach the spot, immediately. However, there are the following feasible mechanisms to identify entities in the system.

A. *MHS Information aggregation*

In the battlefield scenario, each soldier's carries unique features having sensing and actuating devices. Where the bio-medical sensors devices detect soldier's health condition and their weapons status in the physical/measurable quantity. The hierarchical IoT architecture will use raw data during this communication between soldier's devices to semantic Edge or control center. Then, the semantic Edge network will responsible to process the data into a meaningful information. The most common approach is by using a hierarchy of MHS data aggregation devices.

B. *MHS actuation*

Soldiers can have one or more actuators, which will work as results of sensor information. Therefore, any change in the sensor information can trigger the corresponding changes in the actuator systems. However, MHS system can sense and change the density of soldier and their weapons status in the battlefield. Sensors and actuator can change the aggregate definition with the respect of soldier's security density or the inferences dependent upon the soldier's security density. Thus, actuation devices can release alarms, alerts or danger situations to the control center.

C. *Control Center*

The control center can query the status of the soldier's health and their weapons condition from a MHS station. Depending on the number of soldier's aggregated into MHS, it will forward soldier's status to the control center in their area of Interest.

IV. SEMANTIC EDGE COMPUTING

The future of the embedded technologies and their services is dependent upon the foundation of IoT and their software, hardware, middleware, and so on. The growth interest in IoT and cloud, Edge computing technologies and their services is driving connectivity to any and every device. However, there have already been instances in the past where huge numbers of homogeneous and heterogeneous devices decentralized to communicate among themselves and with the network to perform storage and computation tasks. An examples is sieve, process and forward (SPF) proposal, which is an IoT middleware developed in the research efforts of [27][28]. Another latest approach shows the middleware interacting with programmable IoT gateways (PIGs), located along the edge between IoT networks and tactical edge networks [29], although it also claims that it is computationally expensive. Due to edge location, edge computing has a performance advantage and is able to support various near real time experiences with low latency issues. This edge location provides benefits in the context of ubiquitous network surrounding the Edge devices and information about the client side. Edge computing can assist in the tracking of the client and peer side devices [15].

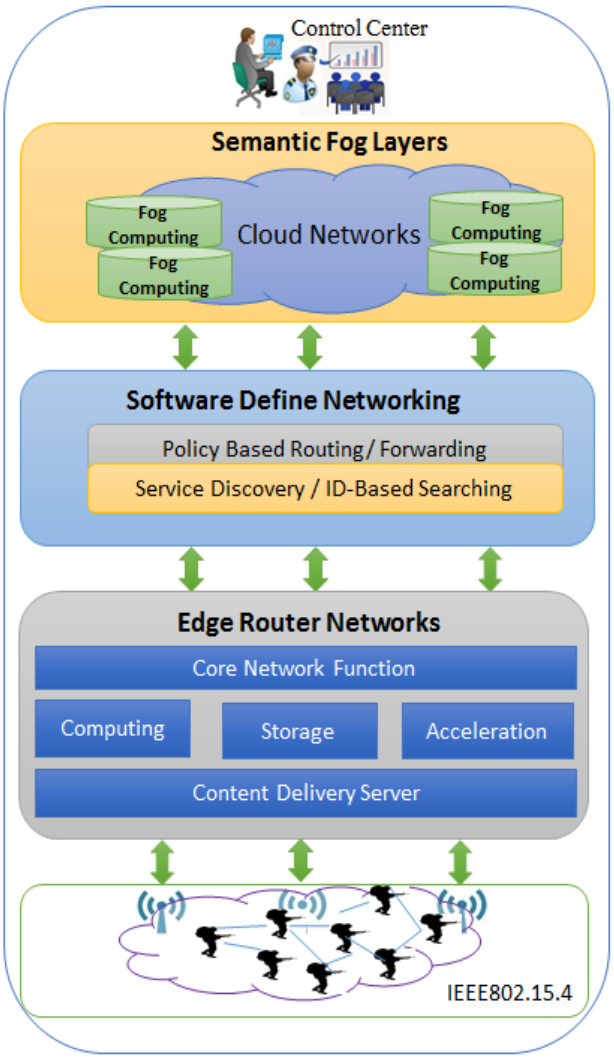

Fig. 4. Semantic Edge based hierarchical IoT architecture.

The support of mobility at the edge of the networks can be helpful in MHS system, where each soldier is a potential client. Interaction between Edge devices is lot more low latency affair as compared to the application-cloud pair or Edge-cloud pair. We have represented the semantic Edge based hierarchical IoT architecture framework to support military health service (MHS) systems in the Fig. 4. The approach can established a network based on IEEE and IETF standardization to monitor the vital health parameters of every military personnel in the battlefield as well as their artillery status along with their geographical location. These raw data can be sent to semantic Edge over SDN, which will be analysed for their respective commanding officer and control center. One of the difficult issues in the battlefield scenario is that the soldiers are not aware about their health parameters as well as their friendly targets. They are aware of the battlefield tactics of enemy but their health awareness about the evolving MHS must also be increased to a level where they can make proper tactical decisions with minimum causalities. In the hierarchical IoT environment we are introducing the information integration of dge computing that can make the computations and storage activities in the near MHS real-time systems. Table

1 sheds light on the attributes of semantic Edge computing in IoT technologies.

V. Final Discussion of Semantic Edge computing

We have discussed health and weapons status management system in the battlefield aware of the deployed soldiers. The hierarchical IoT communication architecture has capability to support two way communication between control center (commander) and soldiers. Thus, commander can monitor soldier's health (parameters like body temperature, heart beat sensor, blood circulation, sugar levels, ECG levels etc.) and weapons status and then take tactical decisions that are relevant for the army.

TABLE 1. RELATIONSHIP BETWEEN IOT AND EDGE COMPUTING.

Internet of Things	Edge Computing
Pervasive	Edge ubiquitous
Real world	Edge resources
Computationally weak	Computationally strong with respect to IoT computations
Limited storage	Larger storage with respect to the IoT storage
Edge data source	Means to manage Edge data and rest forward to cloud

TABLE 2: SECURITY CHALLENGES OF IOT AND EDGE COMPUTING

Semantic Edge and IoT	Description
IoT is expanding	Use of smart embedded system and sensor based devices has increased.
Edge is essentially vendor dependent	Vendor dependencies can cause make unwanted dependencies.
Unwanted Edge nodes remote access.	In the name of remote monitoring, Edge based IoT devices run the risk of corruption of their data.
Edge Data access	The data in the tactical battlefield operations can become vulnerable for attacks and theft.

There are vital soldier's healthcare signs that need to be monitored in the battlefield. Several communication protocols are also possible solutions, but we have considered software define networking (SDN) to establish communication between control center and soldier's. Therefore, we propose a hierarchical IoT architecture for battlefield where MHS system with semantic Edge computing is aimed for processing of real-time responses to the soldiers on the ground. The rules of health and weapons status and their respective responses have been fed in to the Edge devices.

A. Identification and Sensing

The basic thing in any IoT services is the sensing of data and the respective environment. This sensed data is important for real-time responses and over the time as well as it is used for data mining process in order to decipher relevant patterns. Thus, identification through sensors is very important. It is here that we deployed body area networks (BAN). This is the aim of IEEE 802.15.4/LoWPAN (Low-Rate and low power Wireless Personal Area Networks) protocol for communication in the Internet domain. However, IEEE 802.15.4 / LoWPAN has its own sets of limitations like overhead and latencies, to name a few. LoWPAN specifies how the physical and the MAC layer can help the health parameters to communicate between soldiers and commander [11]. The use of Low–Power, Wide-Area Networks (LPWAN) is projected to support a major portion of the billions of devices forecasted for the Internet of Things (IoT) [22]. It offers greater battery lifetime and it is designed for sensors and applications that need to send small amounts of data over long distances a few times per hour from varying environments. Reference [22] also discusses about LoRaWAN, which is defined as a communication protocol and system architecture for the network, while the LoRa physical layer enables the long-range communication link. The protocol and network architecture have the most influence in determining the battery lifetime of a node, the network capacity, the quality of service, the security, and the variety of applications served by the network. LoRaWAN can be a good option for communication in the IoT based MHS applications.

B. Link with FIWARE IoT platforms

As the IoT becomes prevalent there is a need for link up with latest IoT platforms. One such platform is FIWARE [23]. We can use FIWARE IoT stack handles and known IoT protocol standards (MQTT, LWM2M/CoAP, etc) and exposes the same data REST API to developers. It can provide us with our own connector to our proprietary protocols. It is an open source and thus can be freely integrated. One such success stories using FIWARE is presented in [24], which takes the challenges in the e-health sector. Thus, linking with IoT platforms is challenging and beneficial too.

C. Link with Other IoT Platforms

IoTivity is an open source software framework enabling seamless device-to-device connectivity to address the emerging needs of the Internet of Things [25]. There is Google Cloud Platform [26] which can be researched into adapting MHS model deployment.

D. BAN Gateway (semantic Edge)

There are many wireless communication protocols that are used for the IoT services, such as: Wi-Fi, Bluetooth, IEEE 802.15.4, Z-wave, and LTE-advanced. However, the soldier BAN devices in the MHS should maintain a low power usage for a long lasting and efficient device output. Therefore, a special standard of IEEE 802.15.4 specifies usage of physical layer and a medium access control (MAC) for low power wireless networks for scalable solutions. In the MHS system, the IEEE 802.15.4/LoWPAN devices are responsible to transfer soldier's bio-medical date and weapons status to the semantic Edge. It is routed through a suitable gateway to the reach of the Edge devices. The bio-medical sensor information is relayed to a gateway device on the body and then to MHS semantic Edge base station for analysis. Again, we emphasize that LoRaWAN can be a good option for relaying information.

E. Edge Computation and Data analysis

The IoT based battlefield world is supposed to be having many soldiers in the tactical area. Our main focus is to communicate soldier's health condition to the Edge devices to have the health awareness at both ends. Once the Edge based system adheres to the increasing scalability to the new systems, it can become tremendously successful. Thereafter only the integration, development and deployment of Edge based solutions

have to be done. It is the scalability that is the need of the hour. From the Edge based systems, there can be whole lot of information which can be transmitted to the respective cloud for further and intensive data mining processes.

F. Security in Semantic Edge

Security layer in the Edge based IoT stacks can be a major breakthrough in customizing the security solutions. The IoT devices generally communicate with a server in bidirectional manner. The communication happens on the port on which the IoT device is waiting indefinitely for any communication. This opening of such port provides an opportunity for malware attacks, theft of data and so on. Then, with the increase in the Edge based IoT devices, the publishing/subscribing model must support the scalability of the IoT devices [13]. However, Table 2 shows vulnerability of Edge based IoT devices. Therefore, security is the most critical of any Edge based IoT applications. Any corruption with these kinds of data can lead to disaster and even loss of lives. The time is near when our dependencies on Edge based IoT system will exceed many times. Without palpable security any Edge based IoT solutions would be simply could collapse.

Finally, we can see the paper has discussed about MHS which allows seamless communication between soldier's and commander (control station) in battlefield operations, providing health situational awareness of the soldiers. In this paper, we have analysed that the future of IoT and Edge computing is bright in every aspect be it technological and financial. The merging of IoT based Edge computing promises not only great technological success, but also a great investment and return of money. Thus the future business model for economic reforms will hugely be based on Edge computing based IoT services.

ACKNOWLEDGMENT

This works is supported by Hankuk University of Foreign Studies research fund 2016 and the support of Institute of Information Systems funding. The authors would like to thank also projects SAFESENS ENIAC Joint Undertaking with the Grant Agreement no: 621272, and the EU Horizon 2020 projects ENTROPY with the Grant Agreement no: 649849, INPUT with the Grant Agreement no: 644672.

REFERENCES

[1] Hyun Seok Yoon, Dong Hwi Lee, Gangtaek Lee, Kuinam J. Kim, "A Study on the Information Superiority of Network Centric Warfare for Future Battlefield", International Conference on Information Science and Security, Seoul, 10-12 Jan. 2008, pp 224-231.

[2] Singh, D., Tripathi, G., and Jara, A. J., "A survey of Internet-of-Things: Future vision, architecture, challenges and services," in Proc. of the IEEE World Forum on Internet of Things (WF-IoT), pp. 287-292, IEEE, 2014.

[3] Zhu, J., et al.: Improving web sites performance using edge servers in Fog computing architecture. In: SOSE. IEEE (2013).

[4] Dinh, H.T., Lee, C., Niyato, D., Wang, P.: A survey of mobile cloud computing: architecture, applications, and approaches. WCMC (2013).

[5] Vaquero, L.M., Rodero-Merino, L.: Finding your way in the Fog: Towards a comprehensive definition of fog computing. ACM SIGCOMM CCR 44 (2014).

[6] D. Singh, "Developing an Architecture: Scalability, Mobility, Control, and Isolation on Future Internet Services", Second International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 1873-1877

[7] Gaurav Tripathi, Dhananjay Singh, "Scale Free Network Management Mechanism for an Intelligent Battlefield System", International Journal of Advancements in Computing Technology, Vol. 6, No. 4, pp. 34 ~ 43, 2014.

[8] Bonomi, F., Milito, R., Zhu, J., Addepalli, S.: Fog computing and its role in the internet of things. In: workshop on Mobile cloud computing. ACM (2012).

[9] M. A. Chaqfeh and N. Mohamed, "Challenges in middleware solutions for the Internet of Things," in Proc. Int. Conf. CTS, 2012, pp. 21–26.

[10] D. Singh, "Secure 6lowpan Computing Stack for Global Healthcare Monitoring Services", Journal of Theoretical and Applied Information Technology, Vol. 76, No.2, pp. 143 ~ 151, 2015.

[11] Nunes, Bruno AA, et al. "A survey of software-defined networking: Past, present, and future of programmable networks." Communications Surveys & Tutorials, IEEE 16.3 (2014): 1617-1634.

[12] D. Singh, G. Tripathi, A. Jara, " Secure Layers Based Architecture for Internet of Things Services ", IEEE World Forum on Internet of Things (WF-IoT), Milan, Italy, Dec. 14-16, 2015

[13] Antonio M. Alberti and Dhananjay Singh, "Internet of Things: Perspectives, Challenges and Opportunities", International Workshop on Telecommunications (IWT 2013), INATEL, Santa Rita do Sapucai, May 6-9, 2013 pp. 1-6.

[14] Zhang, Q., Cheng, L., Boutaba, R., "Cloud computing: state-of-the-art and research challenges", Journal of internet services and applications (1) (2010).

[15] http://www.dodccrp.org/files/Alberts_Power.pdf

[16] O. Vermesan, P. Friess, P. Guillemin, H. Sundmaeker, and M. Eisenhauer, "Internet of things strategic research and innovation agenda," Internet of Things: From Research and Innovation to Market Deployment, pp. 7–141, 2014.

[17] X. Su, J. Riekki, J. K. Nurminen, J. Nieminen, and M. Koskimies, "Adding semantics to internet of things," Concurrency and Computation: Practice and Experience, 2014, doi: 10.1002/cpe.3203.

[18] http://www.w3.org/TR/owl2-primer/

[19] http://www.opengeospatial.org/projects/groups/sensorwebdwg

[20] http://www.w3.org/2005/Incubator/ssn/wiki/SSN

[21] P. Barnaghi, W. Wang, C. Henson, and K. Taylor, "Semantics for the internet of things: Early progress and back to the future," International Journal on Semantic Web & Information Systems, vol. 8, no. 1, pp. 1–21, Jan. 2012.

[22] https://www.lora-alliance.org/portals/0/documents/whitepapers/LoRaWAN101.pdf

[23] https://catalogue.fiware.org/iot_about

[24] https://www.fiware.org/success_stories/alzhup

[25] https://www.iotivity.org/

[26] https://cloud.google.com/docs/overview/

[27] M. Tortonesi, J. Michaelis, N. Suri, and M.A. Baker, "Software-defined and Value-based Information Processing and Dissemination in IoT Applications," in Proceedings of the 14th IEEE/IFIP Network Operations and Management Symposium (NOMS 2016) - Short Papers Track, Istanbul, Turkey, 25-29 Apr. 2016.

[28] M. Tortonesi, J. Michaelis, A. Morelli, N. Suri, and M.A. Baker, "SPF: An SDN-based Middleware Solution to Mitigate the IoT Information Explosion," in Proceedings of the Twenty-First IEEE Symposium on Computers and Communications (ISCC 2016), Messina, Italy, 27-30 Jun. 2016.

[29] Michaelis, James R., et al. "Applying Semantics-Aware Services for Military IoT Infrastructures." (2016).