Identifying and Studying the Interrelationships amongst Various Challenges in Successful Implementation of IoT to Military and Defence Systems in India

Mukesh Bansal
IAS, Raipur
Chattisgarh, India

Lakshay Aggarwal
Recventure Education
Services Private Limited
Delhi, India

Arnav Jain
Techture Structures
Private Limited
Indore, India

Remica Aggarwal
Recventure Education
Services Private Limited
Delhi, India

ABSTRACT

Internet of Things (IoT) is undeniably transforming the way that organizations communicate and organize everyday businesses and industrial procedures. Its adoption has proven well suited for sectors that manage a large number of assets and coordinate complex and distributed processes. As far as Military and Defence is concerned , an IoT-enabled, seamless supply chain can help the Department of Defense (DoD) achieve end-to-end asset visibility to ensure the right supplies are delivered to the right location at the right time. This will ensure decision-makers have timely and accurate information on the location, condition, and status of critical supplies, ranging from equipment, weapons and spare parts to food, fuel, and medical supplies. However despite these benefactors , successful implementation of IoT is still a challenge in most of the developing countries including India particularly in military and defence sector .The objective of the paper is therefore to first identify various barriers or challenges to successful implementation of IoT in military and defence and thereafter to study the interrelationship amongst them using ISM methodology.

Keywords

Internet of Things (IoT); ISM Methodology ; Military & Defence

1. INTRODUCTION

Internet of Things (IoT) represents the convergence of several interdisciplinary domains such as networking, embedded hardware, radio spectrum, mobile computing, communication technologies, software architectures, sensing technologies, energy efficiency, information management and data analytics [1-5] . IoT services have been mainly classified into identity related services , information aggregation services , collaborative aware services and ubiquitous services . The four basic drivers for IoT implementation includes the declining costs and miniaturization of microelectronics such as transducers (sensors and actuators), processing units (e.g., microcontrollers, microprocessors etc.) The second factor is the fast pace and expansion of wireless connectivity. The third is the expansion of data storage and the processing capacity of computational systems. Finally, the fourth one is the advent of innovative software applications and analytics, including advancements in machine-learning techniques for big data processing. However despite these benefactors , successful implementation of IoT is still a challenge in most of the developing countries including India particularly in military and defence sector . Hence, authors felt the need to study the interrelationship or interactions amongst the various challenges and barriers for the successful implementation of Internet of Things to military and defence systems in developing countries such as India .

The objective of the paper is to identify various barriers to successful implementation of IoT in military and defence and then study their inter-relationship using ISM methodology. The paper is organized as follows. Section 2 deals with literature review. Section 3 explains the ISM methodology and thereafter it has been explained through case example in section 4. Finally managerial implications and directions for future research have been discussed in section 5.

2. LITERATURE REVIEW

2.1 Review of Literature on IoT and Military & Defence

The Internet of Things (IoT) is a distributed system for creating value out of data. It enables heterogeneous physical objects to share information and coordinate decisions. The impact of IoT in the commercial sector results in significant improvements in efficiency, productivity, profitability, decision-making and effectiveness. IoT is transforming how products and services are developed and distributed, and how infrastructures are managed and maintained. It is also redefining the interaction between people and machines. From energy monitoring on a factory [6] to tracking supply chains, IoT optimizes the performance of the equipment and enhances the safety of workers. Until today, it has allowed for more effective monitoring and coordination of manufacturing, supply chains, transportation systems, healthcare, infrastructure, security, operations, and industrial automation, among other sectors and processes. IoT is estimated to reach 50 billion connected devices by 2020 and the potential economic impact will be from $3.9 trillion to $11.1 trillion per year by 2025 [7]. Overall, IoT would allow for the automation of everything around us.

Regarding Machine-to-Machine (M2M) communications, traffic volume is expected to increase at an annual growth rate of 25 percent up to 2021. In total, in such a year there will be around 28 billion connected devices with more than 13.2 billion using M2M communications [8]. Currently, the industrial and business sector is leading the adoption of IoT. Businesses will spend $3 billion in the IoT ecosystem and deploy 11.2 billion devices by 2020, while customers will invest up to $900 million [9]. On the other hand, the public sector is estimated to increase significantly its adoption and spend up to $2.1 billion and install 7.7 billion devices, being the second-largest adopter of IoT ecosystems, particularly in areas like smart cities [10].

Defense and Public Safety (PS) organizations play a critical societal role ensuring national security and responding to emergency events and catastrophic disasters. Instead of PS, some authors use the term Public Protection Disaster Relief (PPDR) [11] radio communications. (DR) radio communication which is the communications used by agencies and organizations dealing with a serious disruption in the functioning of society, posing a significant, widespread threat to human life, health, property or the environment, whether caused by accident, nature or human activity, and whether they happen suddenly or as a result of complex, long-term processes.

Typically, first responders include police officers, firefighters, border guards, coastal guards, emergency medical personnel, non-governmental organizations (NGOs) and other organizations among the first on the scene of a critical situation**.** For example, [12] propose a fault detection method that is based on a network partitioned into clusters for the military domain. Yushi, Fei and Hui [13] introduce a layer architecture and review some application modes. They also include the example of a weapon control application. References [10,14,15,16] contain short surveys for leveraging the IoT for a more efficient military.

2.2 Literature review on barriers in Military & Defence

Communication capabilities need to be provided in very challenging environments where critical infrastructures are often degraded or destroyed. Furthermore, catastrophes, natural disasters or other emergencies are usually unplanned events, causing panic conditions in the civilian population and affecting existing resources. In large-scale natural disasters, many different PS organizations (military organizations, volunteer groups, non-government organizations and other local and national organizations) may be involved. At the same time, commercial communication infrastructure and resources must also be functional in order to alert and communicate with the civilian population. In addition, specific security requirements including communication and information protection can also exacerbate the lack of interoperability. The authors of [17,18,19] focus on security challenges, while TCG drafts a guideline for securing IoT networks [20].

3. INTERPRETIVE STRUCTURAL MODELLING METHODOLOGY

Suggested by Warfield [21], ISM works with the following steps: It starts with identifying the relevant elements and pair-wise establishing the contextual relationship amongst them. Thereafter, a structural self-interaction matrix (SSIM) may be developed between two variables i.e. *i and j* establishing a "Lead to" relationship between criteria. Four symbols *viz.* V, A , X & O are used for establishing the relationships. It further lead to developing initial reachability matrix and then a final reachability matrix after removing transitivity. Afterwards, the reachability set and antecedent set for each criterion and for each element can be obtained from the final reachability matrix . After that a level partition matrix can be obtained based on establishing the precedence relationships and arranging the elements in a topological order . A Mic-Mac analysis is performed categorizing the variables in to autonomous, dependent, driver and linkage category. Finally, a diagraph can be obtained.

4. CASE EXAMPLE

In this section, ISM model is developed for studying the interrelationships amongst various barriers which serve as impediments in successful implementation of IoT in military & defence.

Some 18 barriers *viz.* complex technology and regulatory landscape (CTRL) ; structural and cultural difference (SCD) between private sector and military ; sheer volume of data handling(SVDH) ; problem in storing and quickly retrieving large volume of data (PSRD); diversity of data (DoD); security risk and breaches (SRB) ; hacking (Ha) ; challenges of crisis management (CCM); catastrophes and natural disasters (CND) ; problem with mobility capabilities (PMC); privacy issues and profile access (PIPA) ; prone to data disruption (PDD) ; improper reliability (IR) ; improper availability (IA); improper interoperable capabilities (IIC) ; complexity and high cost of defence (CHC); numerous cost overruns (CO) and schedule overruns (SO) have been identified through literature survey over search engines such as google scholar exploring published articles available in Research gate , academia.edu etc.

Fig 1: SSIM matrix for pair wise relationship amongst barriers

S. No.	Barriers	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
		CTRL	SCD	SVDH	PSRD	DoD	SRB	Ha	CCM	CND	PMC	PIPA	PDD	IR	IA	IIC	CHC	CO	SO
1	CTRL		A	A	V	X	A	A	V	O	V	X	A	A	V	V	V	V	V
2	SCD			V	V	V	V	V	V	O	V	V	V	A	V	V	V	V	V
3	SVDH				V	X	V	V	V	A	V	V	V	A	V	V	V	V	V
4	PSRD					A	V	V	V	A	V	V	V	A	V	V	V	V	V
5	DoD						V	V	V	A	V	V	V	A	V	V	V	V	V
6	SRB							V	V	O	V	V	V	A	V	V	V	V	V

7	Ha								V	A	V	V	V	A	V	V	V	V	V
8	CCM									A	V	A	V	A	V	V	V	V	V
9	CND										V	O	V	A	V	V	V	V	V
10	MC											V	V	A	V	V	V	V	V
11	PIPA												V	A	V	V	V	V	V
12	PDD													A	V	V	V	V	V
13	IR														V	V	V	V	V
14	IA															V	V	V	V
15	IIC																V	V	V
16	CHC																	V	V
17	CO																		V
18	SO																		

Fig 2: Initial reachability matrix

S. No.	Barriers	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
		CTRL	SCD	SVDH	PSRD	DoD	SRB	Ha	CCM	CND	PMC	PIPA	PDD	IR	IA	IIC	CHC	CO	SO
1	CTRL	1	0	0	1	1	0	0	1	0	1	1	0	0	1	1	1	1	1
2	SCD	1	1	1	1	1	1	1	1	0	1	1	1	0	1	1	1	1	1
3	SVDH	1	0	1	1	1	1	1	1	0	1	1	1	0	1	1	1	1	1
4	PSRD	0	0	0	1	0	1	1	1	0	1	1	1	0	1	1	1	1	1
5	DoD	1	0	1	1	1	1	1	1	0	1	1	1	0	1	1	1	1	1
6	SRB	1	0	0	0	0	1	1	1	0	1	1	1	0	1	1	1	1	1
7	Ha	1	0	0	0	0	0	1	1	0	1	1	1	0	14	1	1	1	1
8	CCM	0	0	0	0	0	0	0	1	0	1	0	1	0	1	1	1	1	1
9	CND	0	0	1	1	1	0	1	1	1	1	0	1	0	1	1	1	1	1
10	PMC	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1	1	1
11	PIPA	1	0	0	0	0	0	0	1	0	0	1	1	0	1	1	1	1	1
12	PDD	1	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	1	1
13	IR	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
14	IA	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1
15	IIC	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1
16	CHC	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1
17	CO	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
18	SO	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Fig 3 : Final reachability matrix

S. No.	Barriers	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	
		CTRL	SCD	SVDH	PSRD	DoD	SRB	Ha	CCM	CND	PMC	PIPA	PDD	IR	IA	IIC	CHC	CO	SO	D.P
1	CTRL	1	0	0	1	1	1	0	1	0	1	1	1	0	1	1	1	1	1	13
2	SCD	1	1	1	1	1	1	1	1	0	1	1	1	0	1	1	1	1	1	16
3	SVDH	1	0	1	1	1	1	1	1	0	1	1	1	0	1	1	1	1	1	14
4	PSRD	1	0	0	1	0	1	1	1	0	1	1	1	0	1	1	1	1	1	13
5	DoD	1	0	1	1	1	1	1	1	0	1	1	1	0	1	1	1	1	1	15
6	SRB	1	0	0	0	0	1	1	1	0	1	1	1	0	1	1	1	1	1	12
7	Ha	1	0	0	1	1	0	1	1	0	1	1	1	0	1	1	1	1	1	13
8	CCM	1	0	0	0	0	0	0	1	0	1	1	1	0	1	1	1	1	1	10
9	CND	1	0	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	16
10	PMC	1	0	0	0	0	0	0	1	0	1	1	1	0	1	1	1	1	1	10
11	PIPA	1	0	0	0	0	0	0	1	0	1	1	1	0	1	1	1	1	1	10
12	PDD	1	0	0	1	1	0	0	1	0	1	1	1	0	1	1	1	1	1	12
13	IR	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	18
14	IA	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	5
15	IIC	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	4
16	CHC	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	3
17	CO	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	2
18	SO	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
	De.P	13	2	5	9	8	8	8	13	2	13	13	13	1	14	15	16	17	18	

D.P : Driving power;   De.P : dependence power

4.1 Level Partition

From the final reachability matrix, reachability and final antecedent set for each factor are found. The element for which the reachability and intersection sets are same are the top-level element in the ISM hierarchy. After the identification of top level element, it is separated out from the other elements and the process continues for next level of elements. Reachability set, antecedent set, intersection set along with different level for elements have been shown below in table 4 to table 10.

Table 4.3.1: Iteration I

S. No.	Reachability set	Antecedent set	Intersection set	Level
1.	**18**	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18	18	
2.	17,18	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17	17	
3.	16,17,18	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16	16	I
4.	15,16,17,18	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15	15	
5.	14,15,16,17,18	1,2,3,4,5,6,7,8,9,10,11,12,13,14	14	
6.	1,8,10,11,12,14,15,16,17,18	1,2,3,4,5,6,7,8,9,10,11,12,13	1,8,10,11,12	
7.	1,4,8,10,11,12,14,15,16,17,18	1,2,3,4,5,7,9,12,13	1,4,12	
8.	1,4,6,7,8,10,11,12,14,15,16,17,18	1,2,3,4,5,7,9,13	1,4,7	
9.	1,4,5,6,7,8,10,11,12,14,15,16,17,18	1,2,5,7,9,13	1,5,7	
10.	1,3,4,5,6,7,8,10,1	2,5,9,13	5	

	1,12,14,15,16,17,18			
11.	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18	2,13	2,13	

Table 4.3.2: Iteration II

S. No.	**Reachability set**	**Antecedent set**	**Intersection set**	**Level**
2.	**17**	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17	17	**II**
3.	16,17	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16	16	
4.	15,16,17	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15	15	
5.	14,15,16,17	1,2,3,4,5,6,7,8,9,10,11,12,13,14	14	
6.	1,8,10,11,12,14,15,16,17	1,2,3,4,5,6,7,8,9,10,11,12,13	1,8,10,11,12	
7.	1,4,8,10,11,12,14,15,16,17	1,2,3,4,5,7,9,12,13	1,4,12	
8.	1,4,6,7,8,10,11,12,14,15,16,17	1,2,3,4,5,7,9,13	1,4,7	
9.	1,4,5,6,7,8,10,11,12,14,15,16,17	1,2,3,5,7,9,13	1,5,7	
10.	1,3,4,5,6,7,8,10,11,12,14,15,16,17	2,3,5,9,13	5	
11.	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16, 17	2,3,13	2,3,13	

Table 4.3.3: Iteration III

S. No.	**Reachability set**	**Antecedent set**	**Intersection set**	**Level**
3.	**16**	1,2,3,4,5,6,7,8,9,10,11,12,13, 14, 15,16	**16**	**III**
4.	15,16	1,2,3,4,5,6,7,8,9,10,11,12,13, 14, 15	15	
5.	14,15,16	1,2,3,4,5,6,7,8,9,10,11,12,13, 14	14	
6.	1,8,10,11,12, 14,15,16	1,2,3,4,5,6,7,8,9,10,11,12,13	1,8,10,11,12	
7.	1,4,8,10,11,12,14,15,16	1,2,3,4,5,7,9,12,13	1,4,12	
8.	1,4,6,7,8,10,11,12,14,15, 16	1,2,3,4,5,7,9,13	1,4,7	
9.	1,4,5,6,7,8,10,11,12,14, 15,16	1,2,3,5,7,9, 13	1,5,7	
10.	1,3,4,5,6,7,8,10,11,12,14,15,16	2,3,5,9,13	5,3	
11.	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16	2,3,13	2,3,13	

Table 4.3.4: Iteration IV

S. No.	**Reachability set**	**Antecedent set**	**Intersection set**	**Level**
4.	**15**	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15	**15**	**IV**
5.	14,15	1,2,3,4,5,6,7,8,9,10,11,12,13,14	14	
6.	1,8,10,11,12,14,15	1,2,3,4,5,6,7,8,9,10,11,12,13	1,8,10,11,12	
7.	1,4,8,10,11,12,14,15	1,2,3,4,5,7,9,12,13	1,4,12	
8.	1,4,6,7,8,10,11,12,14,15	1,2,3,4,5,7,9,13	1,4,7	
9.	1,4,5,6,7,8,10,11,12,14,15	1,2,3,5,7,9,13	1,3,5,7	
10.	1,3,4,5,6,7,8,10,11,12,14,15	2,3,5,9,13	5,3	
11.	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15	2,3,13	2,13	

Table 4.3.5: Iteration V

S. No.	**Reachability set**	**Antecedent set**	**Intersection set**	**Level**
5.	**14**	1,2,3,4,5,6,7,8,9,10,11,12,13,14	**14**	
6.	1,8,10,11,12,14	1,2,3,4,5,6,7,8,9,10,11,12,13	1,8,10,11,12	
7.	1,4,8,10,11,1	1,2,3,4,5,7,9,	1,4,12	

	2,14	12,13		V
8.	1,4,6,7,8,10, 11,12,14	1,2,3,4,5,7,9,1 3	1,4,7	
9.	1,4,5,6,7,8, 10,11,12,14	1,2,3,5,7,9,13	1,3,5,7	
10.	1,3,4,5,6,7,8, 10,11,12,14	2,3,5,9,13	5,3	
11.	1,2,3,4,5,6,7, 8,9,10,11, 12,13,14	2,3,13	2,3,13	

Table 4.3.6: Iteration VI

S. No.	Reachability set	Antecedent set	Intersection set	Level
6.	**1,8,10,11,12**	1,2,3,4,5,6,7,8, 9,10,11,12,13	1,8,10,11,1 2	VI
7.	1,4,8,10,11,1 2	1,2,3,4,5,7,9, 12,13	1,4,12	
8.	1,4,6,7,8,10, 11,12	1,2,3,4,5,7,9, 13	1,4,7	
9.	1,4,5,6,7,8, 10,11,12	1,2,5,7,9,13	1,5,7	
10.	1,3,4,5,6,7,8, 10,11,12	2,3,5,9,13	5,3	
11.	1,2,3,4,5,6,7, 8,9,10,11, 12,13	2,3,13	2,3,13	

Table 4.3.7: Iteration VII

S. No.	Reachability set	Antecedent set	Intersection set	Level
7.	**4**	2,3,4,5,7,9, 12,13	4	VII
8.	4,6,7	1,2,3,4,5,7,9,1 3	1,4,7	
9.	4,5,6,7	1,2,5,7,9,13	1,5,7	
10.	3,4,5,6,7	2,3,5,9,13	5,3	
11.	2,3,4,5,6,7, 13	2,3,13	2,3,13	

Table 4.3.8: Iteration VIII

S. No.	Reachability set	Antecedent set	Intersection set	Level
8.	**6,7**	1,2,3,4,5,7,9,1 3	1,7	VIII
9.	5,6,7	1,2,3,5,7,9,13	1,3,5,7	
10.	3,5,6,7	2,3,5,9,13	5,3	
11.	1,2,3,5,6,7, 8,9,13	2,3,13	2,3,13	

Table 4.3.9: Iteration IX

S. No.	Reachability set	Antecedent set	Intersection set	Level
9.	**5**	1,2,5,9,13	1,5,7	IX
10.	3,5	2,3,5,9,13	3,5	
11.	2,3,5,9,13	2,3.9,13	2,3,9,13	

Table 4.3.10: Iteration X

S. No.	Reachability set	Antecedent set	Intersection set	Iteration
10.	**3**	2,3,9,13	3	X
11.	2,3,9,13	2,3,9,13	2,3,9,13	

Table 4.3.11 : Iteration XI

S. No.	Reachability set	Antecedent set	Intersection set	Iteration
11.	2,9,13	2,9,13	2,9,13	XI

4.2 Classification of factors

The critical success factors described earlier are classified in to four clusters *viz.* autonomous factor, dependent factors, linkage factors and independent / Driving factors are mentioned below.

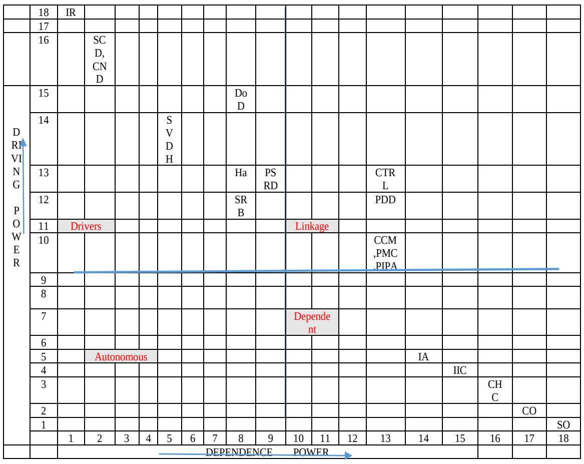

Fig. 4.Driving Power and Dependence Diagram

5. LITERARY OBSERVATIONS AND RECOMMENDATIONS

- Commercial IoT still faces many challenges, such as standardization, scalability, interoperability, and security.
- Researchers working on defence have to cope with additional issues posed by tactical environments, and the nature of operations and networks.
- Beyond the earliest military IoT innovations, complex battlefields will require additional research advances to address the specific demands.

- Moreover, battlefield domains that closely integrate human cognitive processes will require new or extensions of current theories of information that scale into deterministic situations.
- As in any industry, there is no one-size-fits-all solution to the IoT for defense. The military and first responders should establish a testbed for identifying and experimenting with technologies that could remodel the way missions are accomplished, and which would serve as a link between war fighters in the field and IoT developers.

6. CONCLUSIONS

Present research work highlights the interrelationships amongst the various barriers to successful implementation of IoT in Military & Defence with the help of ISM methodology.

7. ACKNOWLEDGMENTS

Our thanks to the anonymous reviewers whose comments have helped us in improving the manuscript . Author Remica Aggarwal extend her warm regards towards Prof. S.P Singh from DMS , IIT Delhi for disseminating the knowledge about ISM methodology which has helped her in preparing this manuscript.

8. REFERENCES

[1] D. Zheng , W.A. Carter, Leveraging the IoT for a more Efficient and Effective Military. Rowman & Littlefield; Lanham, MD, USA: 2015. Technical Report.

[2] A. Al-Fuqaha , M. Guizani , M. Mohammadi , M. Aledhari , M. Ayyash. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Commun. Surv. Tutor. 2015;17:2347–2376. doi: 10.1109/COMST.2015.2444095.

[3] D. Miorandi , S. Sicari , F.D. Pellegrini ,I. Chlamtac , Internet of things: Vision, applications and research challenges. Ad Hoc Netw. 2012;10:1497–1516. doi: 10.1016/j.adhoc.2012.02.016.

[4] L.Atzori , A. Iera, G. Morabito, The internet of things: A survey. Comput. Netw. 2010;54:2787–2805. doi: 10.1016/j.comnet.2010.05.010.

[5] Akyildiz , I.F. , Jornet, J.M. 2010. The Internet of nano-things. IEEE Wirel. Commun., 17, 58–63. doi: 10.1109/MWC.2010.5675779.

[6] Lee ,H.,Yoo , S., Kim ,Y.W. 2016. An energy management framework for smart factory based on context-awareness; Proceedings of the 18th International Conference on Advanced Communication Technology (ICACT); Pyeongchang, Korea. 685–688.

[7] Manyika ,J.,Chui, M., Bisson,P., Woetzel ,J., Dobbs , R., Bughin , J. and Aharon, D. 2015. The Internet of Things: Mapping the Value beyond the Hype. McKinsey Global Institute; Washington, DC, USA. Technical Report.

[8] Ericsson . Ericsson Mobility Report on the Pulse of the Networked Society. Ericsson; Stockholm, Sweden: Nov, 2015. Technical Report.

[9] Business Insider (BI) Intelligence . The Internet of Things: Examining How the IoT Will Affect the World. Business Insider; New York, NY, USA: 2015. Technical Report.

[10] Zanella ,A. , Bui , N., Castellani ,A., Vangelista ,L., Zorzi ,M. Internet of things for smart cities. IEEE Internet Things J. 2014;1:22–32. doi: 10.1109/JIOT.2014.2306328.

[11] Al-Fuqaha , A., Guizani, M., Mohammadi ,M., Aledhari , M., Ayyash , M. 2015. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Commun. Surv. Tutor, 17, 2347–2376. doi: 10.1109/COMST.2015.2444095.

[12] Chudzikiewicz , J., Furtak , J., Zielinski , Z. 2015. Fault-tolerant techniques for the Internet of Military Things; Proceedings of the IEEE 2nd World Forum on Internet of Things (WF-IoT); Milan, Italy. 496–501.

[13] Yushi , L., Fei , J.,Hui , Y. 2012. Study on application modes of military Internet of Things (MIOT); Proceedings of the IEEE International Conference on Computer Science and Automation Engineering (CSAE); Zhangjiajie, China. 630–634.

[14] Zheng , D., Carter , W.A. 2015. The Internet of Things for Defense. Wind River Systems; Alameda, CA, USA. . Technical Report.

[15] Mariani , J. Williams, B. Loubert, B. 2015. Continuing the March: The Past, Present, and Future of the IoT in the Military. Deloitte University Press; Deloitte, UK. Technical report.

[16] Suri , N., Tortonesi , M., Michaelis ,J., Budulas, P. , Benincasa , G. Russell , S., Stefanelli, C., Winkler , R. 2016. Analyzing the applicability of internet of things to the battlefield environment; Proceedings of the International Conference on Military Communications and Information Systems (ICMCIS), Brussels, Belgium.

[17] Wrona, K. 2015. Securing the Internet of Things a military perspective; Proceedings of the IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy. 502–507.

[18] Eom, J. 2015. Security threats recognition and countermeasures on smart battlefield environment based on IoT. Int. J. Secur. Appl., 9, 347–356. doi: 10.14257/ijsia.2015.9.7.32.

[19] Alqassem I. , Svetinovic , D. 2014. A taxonomy of security and privacy requirements for the Internet of Things (IoT); Proceedings of the IEEE International Conference on Industrial Engineering and Engineering Management; Bandar Sunway, Malaysia. 1244–1248.

[20] Trusted Computing Group, Guidance for Securing IoT Using TCG Technology, Version 1.0, Revision 21. http://www.trustedcomputinggroup.org/wp-content/uploads/TCG_Guidance_for_Securing_IoT_1_0r21.pdf.

[21] Warfield, J.N. 1974. Developing interconnection matrices in structural modelling. IEEE Transactions on System, Man, and Cybernetics, SMC-4 (1), 81-87.