Internet of Things and OPC UA

Ravish Kumar
ABB Corporate Research
Bangalore, India
e-mail: ravish.kumar@in.abb.com

Arijit Kumar Bose
ABB Corporate Research
Bangalore, India
e-mail: arijit.bose@in.abb.com

***Abstract*— Internet of Things (IoT) has become very popular due to its envisioned capability. Industry, Health care and Utility sectors are working actively to take advantage of the benefits that the IoT infrastructure can offer. However, it will take a long time until a completely developed IoT infrastructure is in place. Since this requires a large scale technology restructuring, many challenges need to be addressed. Certainly, IoT infrastructure development would happen step by step and it will be slowly accepted by the users, particularly from the industrial sector. In addition, some provision is also required to connect the existing automation system with the IoT infrastructure. In order to facilitate this connection, a bridging technology is required. In this paper, we describe how the industry proven OPC UA technology can be used for connecting the existing automation system with an IoT infrastructure. Furthermore, we also analyze the OPC Unified Architecture (OPC UA) security model from an IoT perspective and highlight the required improvements.**

Keyword-Internet of Things; OPC UA; Security

I. INTRODUCTION

Technology analysts and visionaries have defined Internet of Things (IoT) [5] as a network of physical objects which can be accessed through the Internet. These objects contain embedded technology to interact with the external environment. The objective of IoT is to mix the physical world and the information world. As a result, it will create an environment where one machine can communicate directly with other machines without much manual intervention. IoT has a great potential to influence Industrial application. It will create new ways of organizing processes and information flow across industrial production. By connecting different machines, field devices, production units, transportation information and goods data seamlessly to an IoT infrastructure, a smart production system can be created with more flexibility, resourceful and faster production. Such a smart production system will leverage to incorporate last minute changes in the production cycle and will also possess the ability to respond flexibly to disruptions and failures on behalf of suppliers and other external factors. In addition, the smart system will also induce the capability to respond rapidly to dynamic businesses and engineering processes, thereby facilitating dynamic changes in the production when needed.

For creating an IoT infrastructure, coordination and cooperation between the new generation technologies and existing proven technologies must be considered. Most of the existing industrial automation systems are based on the concept of a Distributed Control System (DCS) [1], which works in isolation and cannot be directly operated from the Internet. Due to this limitation, it has reduced flexibility to handle dynamic business changes in an industrial plant. Therefore, to evolve a DCS architecture to handle dynamic business changes, a new generation of technologies coming traditionally from an Internet world should be considered."

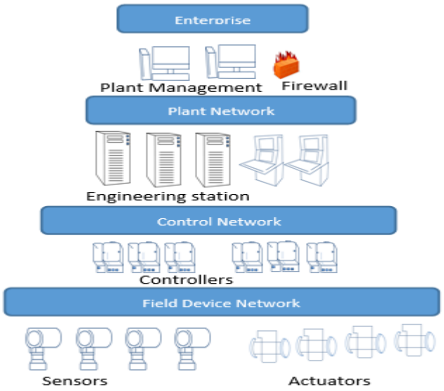

Figure 1. Distributed Control System Architecture.

DCS has different layers for handling various operations. Fig. 1 shows the hierarchy of a typical DCS based industrial automation system. Typically, there are four layers in an automation system. These layers are Enterprise Network layer, Plant Network Layer, Control Network Layer and Field Device Network Layer. All the layers are specialized to perform specific kinds of operations. For example, the Control Network Layer is responsible for the execution of control tasks of the plant process.

Currently, the industrial automation system works in isolation with other entities such as Enterprise Resource Planning (ERP) [2] and Manufacturing Execution System (MES) [3]. ERP is a business management software application, which is used for product planning, inventory and suppliers' management, shipping and payment, etc. MES is a software application, which is used for accessing current conditions of plant processes for resource optimization and decision making. Because they work in isolation, the existing

ISBN: 978-1-61208-404-6

industrial automation systems are not able to handle dynamic processes and to incorporate last minute changes into the process flow. Currently, incorporating any small updates in the production life cycle is expensive because multiple changes and synchronizations need to be done in different places. Connecting the industrial automation system with other entities such as ERP, MES, etc. over the IoT infrastructure produces a whole automation system capable of handling dynamic business and engineering processes.

In this paper, we will investigate the solution for enhancing the existing industrial automation system to leverage benefits from dynamic business and engineering process. This is done by enabling connectivity to an IoT infrastructure by using the industry proven OPC Unified Architecture (OPC) technology [4]. We will also analyze the security framework of OPC UA from an IoT perspective and will be highlighting the required improvements.

The rest of the paper is organized as follows. In Section II, we provide the background and related work of the IoT. In Section III, we provide an overview of the existing OPC UA standard, followed by describing how OPC UA can be used for enhancing the existing industrial automation system to connect with an IoT infrastructure. In Section IV, we provide an overview of the OPC UA security model. In Section V, we analyze the security of OPC UA from an IoT perspective and highlight the required improvements. In Section VI, we provide a conclusion to our work and describe the possible future work.

II. Related Work

IoT is basically a convergence of multiple technologies such as Radio-frequency identification (RFID), sensor technology, Internet, wireless, cloud computing, etc. All of these technologies contribute to enable an IoT infrastructure. The term IoT was first introduced by Kelvis Ashton in the year 1999. His initial idea was to empower computers to gather information on their own, so that computers can see, hear and smell the world by themselves [5]. But, in today’s scenario, it is not just limited to empowering computer to gather information only. Now, it is considered as a communication infrastructure for exchanging information among the things around the globe [6]. Things, in the IoT, refer to a wide variety of devices. The applicability of IoT is not limited to one domain [7][8]. It is suitable for various application sectors like industrial domain, health care, utility, etc. Tan et al. [9] described IoT as future Internet for establishing communication not only between human to human, but expanding to human to machine, and machine to machine. Chen [10] discusses the overview of new paradigm along with different challenges and opportunities. Imtiaz et al. [11] investigated the OPC-UA as a middleware solution for resource-limited devices. To handle an enormous volume of IoT data, Copie et al. [12] highlighted how IoT data can be stored in a cloud database. The Industry 4.0 [13] revolution has been envisioned based on IoT and Cyber Physical System (CPS). Perera et al. [14] examined a variety of popular and innovative IoT solutions in terms of context-ware technology perspective and evaluated them on a framework that they built around well-known context aware computing theories. Singh [15] has presented an efficient hierarchical identification mapping server for identification and location of connected things in the IoT infrastructure for enabling global mobility and scalability. Ungurean et al. [16] discussed an IoT architecture based on the OPC.NET [17] technology. OPC.NET is tightly coupled with Microsoft platform. Because of this platform dependency, freedom of platform independency cannot be achieved in true sense. Furthermore, Ungurean et al. [16] have not discussed the security aspects of OPC.NET from the perspective of an IoT infrastructure.

Keoh et al. [18] provide some salient security enhancements that are required in the emerging IoT protocols like security enhancements for Constrained Application Protocol (CoAP), Datagram Transport Layer Security (DTLS), etc. Sajjad et al. [19] discussed on the security enhancements of IEEE 802.15.4 Media Access Control (MAC) in the context of IoT. However, based on the prior art, we did not find many studies that explain the security enhancements for OPC UA from an IoT perspective.

III. OPC Unified Architecure

OPC UA [4] is an Industry proven standard for exchanging industrial data. It provides a framework for safe and reliable communication among the different industrial devices and applications. This standard is developed with close cooperation with manufacturers, users and research institutes, in order to enable information exchange among heterogeneous systems. It was designed to support a wide range of systems, ranging from sensor device to enterprise server. The services of OPC UA ensure a seamless flow of information among multiple heterogeneous entities of an industrial automation system. OPC UA performs this seamless exchange of information by a typical client-server model, and with a platform agnostic approach. Information is transacted between OPC UA client and server.

OPC UA standard is developed and maintained by the OPC foundation [20]. Its data modelling and object-oriented techniques allow the modelling of any kind of information data. The specifications of the OPC UA standard [4] provide the autonomy for defining industry or standards organization, a specific information model for exchanging information across various kinds of platforms.

IV. Proposed Architecture

Our proposed architecture is presented in Fig. 2. With the help of OPC UA technology, the industrial automation system is enabled to establish connectivity with an IoT infrastructure.

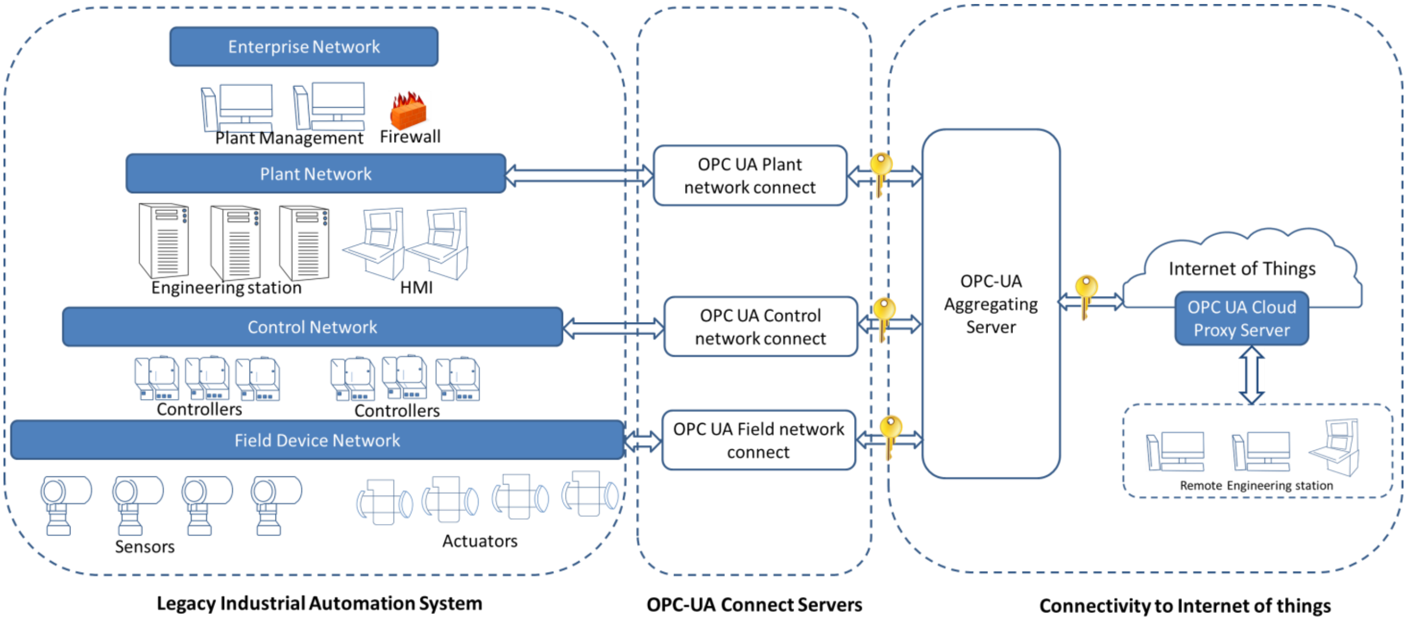
Enterprise Network
Plant Management
Firewall
Plant Network
Engineering station
HMI
Control Network
Controllers
Controllers
Field Device Network
Sensors
Actuators
OPC UA Plant network connect
OPC UA Control network connect
OPC UA Field network connect
OPC-UA Aggregating Server
Internet of Things
OPC UA Cloud Proxy Server
Remote Engineering station
Legacy Industrial Automation System
OPC-UA Connect Servers
Connectivity to Internet of things

Figure 2. Industrial Automation connectivity with an IoT infrastructure.

OPC UA enables, not only pure process data exchange, but also semantic information exchange as well. This architecture is built around three main modules as shown in Fig. 2, i.e. OPC UA Connect server, OPC UA Aggregating server and OPC UA Cloud proxy Server. Three different OPC UA Connect servers, i.e. OPC UA Plant network connect, OPC UA Control network connect and OPC UA Field network connect, are used for modeling the data at the Plant network layer, Control network layer, and Field Device network layer respectively. These three OPC UA Connect servers are leveraged to model the data from the devices located at the factory floor to enterprise applications. The OPC UA aggregating server aggregates the data from the OPC UA Connect servers into one place. It is helpful for any OPC UA client application to access the data from multiple OPC UA servers from a single node. This feature is thus facilitated by the OPC UA aggregating server. OPC UA aggregating server also provides a mechanism for chaining the data from multiple OPC UA servers to a particular OPC UA client application, for limiting functions and data accessibility. OPC UA cloud proxy server provides the proxy connection between OPC UA aggregating server and remotely located different OPC UA client applications such as Enterprise Management System, remote engineering workplace, etc. By divulging the different layers of industrial information data to an IoT infrastructure, an industrial automation system will be capable of exchanging information with other applications such as ERP and MES. Thus, with this architecture, an industrial automation system can be enhanced with a capability for handing dynamic business processes. For example, if a supplier delays the supply of raw materials, with an IoT enabled infrastructure, this information can be conveyed to a production site as quickly as possible. Instead of shutting down the production, the production speed can be slowed down and other maintenance activities can be performed in parallel.

V. OPC UA Security Model Analysis

Security model of OPC UA is a very important aspect for its reliable operation in an industrial automation plant. A security compromised OPC UA server and client application can result into devastating effects on the plant, causing huge financial damages, and could even lead to severe health hazards. The security requirements for OPC UA has been addressed in its standard. This section provides a short overview of the existing security specifications of OPC UA from its reference security standard [21]. OPC UA features the basic security primitives i.e. authentication, authorization, integrity, confidentiality and auditability of data as illustrated below.

A. *Authentication*

In OPC UA, both the server and client application establish a mutual trust between them by validating each other’s identities. This verification and validation of each other’s identity is performed on the basis of X.509 based certificates [22]. Thus, when an OPC UA client application wants to establish a connection with the OPC UA server side application, the server application performs an authentication check of the client application, and vice versa on the basis of X.509 based certificates. Thus, a X.509 certificate acts like an identity of the OPC UA application.

B. *User authentication*

OPC UA server guards the user access control by validating each user’s identity. This can be done with the help of username & password or by a X.509 based certificate based token. OPC UA server checks the authenticity of the

ISBN: 978-1-61208-404-6

users to permit only legitimate users to access the server ontents. When an end user tries to access the OPC UA server from an OPC UA client application through a network, the OPC UA client securely sends the credentials of the user like his username and password to the OPC UA server. The communication traffic between OPC UA server and OPC UA client is made secure by Transport Layer Security (TLS) [23] protocol.

C. User authorization

OPC UA also features authorization controls of users. User can perform only those job functions as per their set privileges.

D. Secure communication

OPC UA client and OPC UA server communicate over a secure channel. The messages that are exchanged between OPC UA server and OPC UA client are digitally signed to provide authentication and integrity. Messages are optionally encrypted to provide confidentiality as per need basis. TLS protocol [23] is used for providing these security features to the exchanged messages.

E. Auditability

Event logging is supported in OPC UA for recording important user and system activities such as user access logs and communication logs on the OPC UA server, when OPC UA clients connects to it.

F. Security policy management

Security policies like cryptographic key sizes, type of crypto algorithms, key expiry time etc. is maintained in Cyber Security Management System (CSMS) [21]. Thus, the security policies of the OPC UA server are managed centrally from this management system. When an OPC UA client tries to connect to a OPC UA server, it performs a discovery mode by sending discovery messages to obtain the security profiles that are supported by the OPC UA server. This helps the OPC UA client to detect, and accordingly use the security policies of the OPC UA server for establishing a secure connection to it.

G. Availability

OPC UA server incorporates protection against message flooding, by limiting the processing of concurrent messages. Security against replay attacks is done by specifying sequence numbers and time stamping for each transacted messages.

VI. OPC UA Security Model Analysis From An IoT Prospective

When using OPC UA in the IoT computing space, the probability of a security attack towards the OPC UA based systems will be larger. This is because the world of Internet is exposed to different types of sophisticated cyber threats. Additionally, the number of cyber security threats will grow, and propagation of new threats can also occur from the Internet domain. Hence, it is important to increase the security level of the OPC UA to defend against the Internet based attacks. In this section, we analyze the existing security workflow and specifications of OPC UA, and propose some ideas for enhancing the security of OPC UA, from an IoT perspective. Following are the security enhancement areas which we propose.

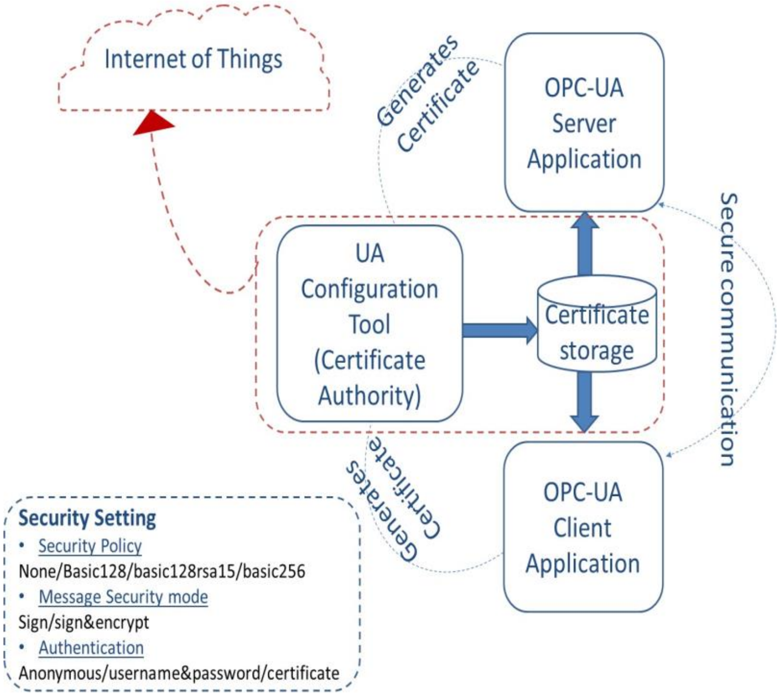

Figure 3. Certificate management of OPC UA.

A. Certificate management in IoT cloud

X.509 based digital certificates are recommended to attest the identity of OPC UA applications, as per its standard prescribed security specifications [21]. During communication, an OPC UA client and server application shall thus perform an authentication check on each other, with the help of their X.509 based digital certificates.

In Fig. 3, we describe the X.509 certificate generation and issuing process for the OPC UA server and client applications. Presently, the existing OPC UA configuration tool has a built in Certification Authority (CA), which generates certificates for the OPC UA applications, and stores them in a certificate storage Database.

During the course of certificate generation process, the administrator of OPC UA configuration tool registers the credentials of each OPC UA application, and subsequently also generates and stores their issued certificates in a certificate storage database. The credentials of OPC UA applications could be the application name, organization that has built the application, etc. Then, each OPC UA server and client application accesses this database to obtain their corresponding issued certificates, and further uses their certificates to securely communicate among each other. In

ISBN: 978-1-61208-404-6

the present state, the CA and certificate database of an OPC UA based system are managed and operated locally within the perimeter of an industrial automation plant.

As we intend to integrate the existing industrial automation system with an IoT infrastructure by using the complementary OPC UA technology, we propose to shift and deploy the CA functionality and certificate storage database of the existing OPC UA based systems into the IoT's cloud computing space. This proposal of shifting is depicted using the red dotted mark, as referred in Fig. 3. The benefit of shifting the OPC UA certificate management functionalities into the IoT cloud is that it will enable to manage the ability to manage the certificates of various OPC UA server and client applications from any geographical location. This will increase the flexibility and scalability of managing the certificates of OPC UA applications.

However, operating the certificate management feature in the IoT cloud space has some business challenges too. Typically, each industrial automation plant tries maintaining and operating its CA in its own corporate network. This is done in order to maintain the certificate related security policies within its perimeter. Therefore, the existing industrial automation plant owners may not be ready and flexible enough to move their CAs into the IoT cloud space.

B. Secure registration of OPC UA applications

We also suggest to consider a secure registration of OPC UA application credentials in the CA, which is managing the certificates of OPC UA applications. As explained before, that in the existing scenario, the OPC UA configuration tool registers the credentials of each OPC UA application, and subsequently generates certificates for the registered applications with its inbuilt CA. Before registration, neither the OPC UA configuration tool nor the administrator of the tool, verifies whether or not the credentials of OPC UA applications are valid. Checking the authenticity of these credentials is crucial for the initial trust establishment of legitimate OPC UA applications with the CA. Before registering each credential of OPC UA applications in the CA, it is important to check their authenticity. If the registered credentials belong to a rogue OPC UA application, the malicious application will manage to legitimately obtain a certificate from the CA. An attacker can further use the rogue application to inject attacks and perform harmful operations on the industrial automation system. The legitimate credentials of OPC UA applications should also be stored and accessed securely. Access to the legitimate credentials of OPC UA applications should be granted only to authorize people. If these credentials reach the hands of an attacker, then the attacker can register a rogue application with the same legitimate credentials in the CA, which is managing the certificates of OPC UA applications.

C. Secure management of time synchronization messages

If a time server from the Internet domain is used for synchronizing the timings of OPC UA devices, it is also important to validate the authenticity of time server and secure the time synchronization messages. A rogue time server can synchronize the OPC UA device with incorrect timings, which could negatively affect certain automation applications. These could have devastating effect on automation applications, whose operations are dependent on accurate timings. Denial of Service (DoS) attack can also be injected in the OPC UA enabled devices by improper expiration of OPC UA application certificates. This can be caused by wrong device timings. If the certificate of a OPC UA server application expires before its lifetime, then OPC UA clients may face issues in connecting to the OPC UA server due to certificate expiry error.

D. Enhance user authentication and authorization

Introducing OPC UA in the IoT space will certainly also increase the number of legitimate users, who can access the OPC UA server and client applications from the Internet. A secure management of such increasing number of user credentials is important for allowing only legitimate user operations on the OPC UA.

E. Secure web services

OPC UA web servers should also adopt security measures against Cross-site Scripting (XSS) and code injection attacks [24]. In such attacks, the attacker tries injecting malicious scripts in a legitimate web server. By injecting such rogue scripts, the legitimate OPC UA web server can malfunction or be directed to execute devastating operations. Such rogue operations include illegitimately changing the configuration parameters of the OPC UA enabled industrial automation device. This can make the device perform unintended and rogue operations inside the automation plant. XSS and code injection based attacks are becoming very popular web attacks in the Internet space [25]. Therefore, OPC UA web server should also consider and implement countermeasures against such sophisticated web attacks.

Proper sanitization of data within the OPC UA web servers is also recommended for securing against such Internet based web attacks. Also, disabling the unnecessary web services of OPC UA is a good security practice to reduce the attacking surface for the Internet attackers.

F. Categorization and securing event loggings

Using OPC UA in the IoT space would create a mixture of OPC UA type events and Internet based events, like the traditional IT related events. For ensuring a well-structured audit log, a clear separation for these two types of event would make the event logs more readily understandable to the operators of the industrial plant. For example, a OPC UA system monitoring engineer would be interested to view the OPC UA event logs instead of IT type events.

Categorization of event logs would enable the OPC UA engineers to quickly view the OPC UA event type data. It is also required to securely transport the event log messages to the OPC UA event logging server. This can be done by digitally signing and optionally encrypting them, when required. This is important especially if the OPC UA event logging and management server is operating in the IoT cloud. It will prevent the attackers from the Internet to produce fake or to modify the legitimate event log messages, which could create a wrong status of the industrial automation system.

VII. Conclusion

IoT is a new technology revamp, which will provide the infrastructure for exchanging the information across different entities. For an industrial automation system, IoT is the one key enabler for facilitating dynamic business and engineering processes. We have analyzed and proposed an architecture which describes how the industry proven OPC UA technology can be used for evolving, and thus enabling an industrial automation system to exchange information with an IoT infrastructure. We have also analyzed the existing security model of OPC UA from an IoT's perspective. Based on our security analysis, we have proposed and thus highlighted the suggested areas where security improvements are required when using OPC UA in the IoT's space. The performance verification and validation of our proposed architecture needs to be thoroughly tested in a real industrial automation system. Our future research work shall focus towards such experimental evaluations of our proposed architecture.

References

[1] Galloway, Hancke B, "Introduction to Industrial Control Networks," Communications Surveys & Tutorials, IEEE , vol.15, no.2, pp.860,880, Second Quarter 2013

[2] http://www.erp.com/component/content/article/324-erp-archive/4407-erp.html [accessed May 2015]

[3] McClellan, Michael (1997). Applying Manufacturing Execution Systems. Boca Raton, Fl: St. Lucie/APICS. ISBN 1574441353.

[4] OPC UA Specification, Part-1 Overview and Concepts. Reterived from https://opcfoundation.org/developer-tools/specifications-unified-architecture/part-1-overview-and-concepts/ [accessed Feb 2015]

[5] Kevin A (22 June 2009). That Internet of Things Thing, in the real world things matter more than idea. Reterived from http://www.rfid-.journal.com/articles/view?4986 [accessed December 2014]

[6] Xu Li,He Wu,Shancang Li, "Internet of Things in Industries: A Survey," Industrial Informatics, IEEE Transactions on , vol.10, no.4, pp.2233,2243, Nov. 2014 doi: 10.1109/TII.2014.2300753

[7] Kim M., Hwang J, "New approach for Convergence of IT + pharmaceutical industry," Information and Communication Technology Convergence, (ICTC), 2010 International Conference on , pp.569,570, 17-19 Nov. 2010

[8] Song Bo, Xing Qian, "On security detecting architechture of food industry based on Internet of Things," Automation and Logistics (ICAL), 2011, IEEE International Conference on , pp.81,85, 15-16 Aug. 2011

[9] Tan L,Wang N, "Future internet: The Internet of Things," Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on , pp.V5-376,V5-380, 20-22 Aug. 2010

[10] Chen Y, "Challenges and opportunities of internet of things," Design Automation Conference (ASP-DAC), 2012 17th Asia and South Pacific, pp.383, 388, Jan. 30 2012-Feb. 2 2012

[11] Imtiaz, J., Jasperneite, J., "Scalability of OPC-UA down to the chip level enables "Internet of Things"," Industrial Informatics (INDIN), 2013 11th IEEE International Conference on , pp.500,505, 29-31 July 2013

[12] Copie A, Fortis T, Munteanu, V.I, "Benchmarking cloud databases for the requirements of the Internet of Things," Information Technology Interfaces (ITI), Proceedings of the ITI 2013 35th International Conference on , pp.77,82, 24-27 June 2013

[13] Recommendations for implementing the strategic initiative INDUSTRIE 4.0, Acatech, April 2013. Reterived from http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Material_fuer_Sonderseiten/Industrie_4.0/Final_report__Industrie_4.0_accessible.pdf

[14] Perera C., Liu C.H., Jayawardena S., Min Chen, "A Survey on Internet of Things From Industrial Market Perspective," *Access, IEEE*, pp.1660,1679, 2014 doi: 0.1109/ACCESS.2015.2389854

[15] Singh D., "Developing an architecture: Scalability, mobility, control, and isolation on future internet services," Advances in Computing, Communications and Informatics (ICACCI), 2013

[16] Ungurean I., Gaitan N., Gaitan V G., "An IoT architecture for things from industrial environment," Communications (COMM), 2014 10th International Conference on , pp.1,4, 29-31 May 2014

[17] http://www.opcconnect.com/dotnet.php [accessed Jan 2015]

[18] Keoh S, "Securing the Internet of Things: A Standardization Perspective", IEEE Internet of Things Journal, Vol. 1, No. 3, June 2014

[19] Sajjad S M, Yousafy M, "Security Analysis of IEEE 802.15.4 MAC in the context of Internet of Things (IoT)", Proceedings of the 2014 Conference on Information Assurance and Cyber Security (CIACS)

[20] https://opcfoundation.org/ [accessed Jan 2015]

[21] OPC UA Security Standard Specifications, OPC UA Specification Part 2: Security Model Release. Reterived from https://opcfoundation.org/developer-tools/specifications-unified-architecture/part-2-security-model [accessed Feb 2015]

[22] RFC 2459, X.509 Certificate.Reterived from https://www.ietf.org/rfc/rfc2459 [accessed Feb 2015]

[23] RFC 5246, Transport Layer Security (TLS) Protocol, Version 1.2. Reterived from https://datatracker.ietf.org/doc/rfc5246 [accessed Feb 2015]

[24] Cross-site Scripting, OWASP guide to XSS attacks. Reterived from https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29 [accessed Feb 2015]

[25] Web Hacking Incident Database (WHID) 2013 statistical records for XSS attacks. Reterived from http://projects.webappsec.org/w/page/13246995/Web-Hacking-Incident-Database#RealTimeStatistics [accessed Mar 2015]