Formal Approach to Internet of Things in the Context of the Web 7.0 Project

Radomir A. Mihajlović
Data Science & Software Arcitecture
NYITS & Persida-Bio Co Inc
Brooklyn, NY, USA
billmic@gmail.com

Lyudmila Zharova
FON
University of Belgrade
Belgrade, Serbia
lzharova077@gmail.com

***Abstract*— Since the introduction of the Internet of Things (IoT) by the International Telecommunication Union (ITU), relevant technology has been a subject of intensive Research and Development (R&D). Various definitions of IoT have been introduced by different R&D groups and authors, as well as by the involved standardization organizations. Upon the review of the vast body of IoT-related literature we have witnessed on numerous occasions arbitrary IoT relevant terminology. Our conclusion was that a more rigorous approach to this fascinating area of R&D is necessary. This paper is primarily focused on IoT semantics consolidation, IoT security, and new horizons of the application of the Zero Trust Architecture (ZTA) to secure and private IoT systems design. The attribute of privacy, being frequently mixed up with security, has been addressed in the context of the Web 7.0 project. In this paper we consider IoT as an extension of the Internet, i.e., as Internet 2.0, and IoT privacy as an extension of the ZTA set of design goals or principles.**

Keywords*— *Internet of Things, Access Control, Zero Trust, Homomorphic Encryption. Blockchain, Web 7.0.

I. INTRODUCTION

Our general view of “a thing” or “a plant” is as follows: "a thing" refers to unidentified physical (material, existing, or real) object, a logical (imagined, conceptual) object appearing as an idea, or virtual (computing) software simulated object, when the specific name of the given object is abstracted or ignored. In unusual situations, a thing may refer to an event or an action. In summary, a thing may be:

- Real,
- Logical, or
- Virtual.

Virtual thing appears to general-user (human, machine or software) as a real object, while in fact it does not exist [1]. If users of a thing can benefit while using it, the fact that virtual thing does not exist is ignored. It is important to observe that virtuality assumes two attributes:

- Existence (Not existent), and
- Appearance (Yes, functionally available to users).

Real things (with virtuality attributes Existence=YES and Availability=YES) are primary subjects in the IoT R&D reports and technical publications. Logical and Virtual things are rarely of interest in the literature on the topic of IoT.

Common understanding is that IoT refers to the assembly of things that have built in computation and communication capability. Adding these capabilities transforms “a thing” into “a Thing.” If each of the Things is networked and can be accessed over the Internet, the assembly of Things can be categorized as Internet of Things or IoT. Taking this point of view, we consider an IoT, in its most general form, as an extension of the Internet. Traditional view of the Internet assumes Internet to be a global network of computing devices such as workstations, and servers. With an arbitrary things as Things, possibly added to the Internet, we have obtain new Internet, which we refer to as Internet 2.0.

At this point we may distinguish two definitions of IoT. In the wide-sense, IoT is an extension of the Internet interconnecting legacy-computer and things redesigned as Things. In the narrow-sense, IoT is a network of Things appearing as nodes in the edge of some given systems, where all IoT nodes can be accessed via Internet.

We must clearly distinguish between a Thing and network of Things, i.e., Internet of Things. In conclusion IoT is a network and a Thing is a node in the IoT network.

In what follows we deal with the IoT security problems and some state of the art approaches that extend concept of security, leading to the “security++” with privacy.

II. MACHINE TO MACHINE VS IOT PROTOCOLS

Machine (M) local network implementing M2M lines and links not exposed to Internet, unable to provide remote access to individual nodes via Internet (TCP/IP driven network) does not qualify to be considered as an IoT network.

Supervisory Control and Data Acquisition (SCADA) systems contain M2M local networks without all individual network nodes being available, directly or indirectly, for remote access across Internet. M2M and SCADA nodes resemble IoT nodes, however without some additional redesign, IPv.4 or IPv6 protocols cannot be used.

III. IOT TECHNOLOGY STACK

In the broad sense, IoT stack term is hardware and software model of the abstract IoT system. In the narrow sense, IoT stack describes a single node or a pair of linked IoT nodes.

Fig. 1. An example of a commonly used rough model of the IoT technology stack [2].

Ad-hoc and superficial references to the IoT stack, frequently appear in the relevant papers, ignoring and bypassing essential meaning and purpose of the term "stack." An example of the improvised IoT technology stack is shown on Fig. 1.

When designing IoT systems architecture, the purpose of the IoT stack is to highlight modular design with stacked layers acting as independent modules. Stack layers or modules can be designed and later upgraded independently of each other. The independent stacked layers represent fundamental elements of the Open System Interconnection (OSI) architecture. To maintain the design and layer to layer modifications independence, the stack inter-layer interface must be maintained unchanged. This is the only major constraint imposed on the layers of the OSI architecture. Apparently various R&D texts keep presenting ad-hoc improvised versions of the IoT stack that do not conform with the fundamental OSI architecture design principles.

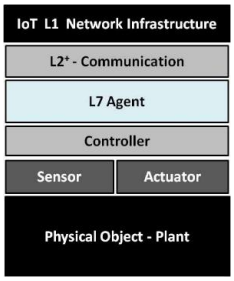

Fig. 2. An IoT single network node stack [3], (A thing is labeled here as controlled plant).

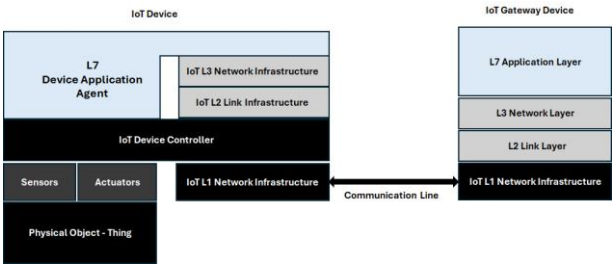

Fig. 3. Trivial local network IoT-stack model.

In this paper we present formal IoT stack model. One version of the formal model described in [3] is shown in Fig. 2. The other version of the formal IoT stack, shown in Fig. 3 is modelled as a trivial IoT network (The simplest possible local network) made up of two linked nodes.

Both IoT stack models clearly distinguish original thig hardware and augmented electronics (Thing) hardware that includes:

- Thing sensors,
- Thing control/computation hardware,
- Thing actuation hardware, and
- Thing communication (L1) hardware.

The IoT stack hardware layer-set encompasses the physical components of the IoT device, that include bare physical Thing, sensors, actuators, signal transmitter and receiver or transceiver, communication lines (wired or wireless), micro-controller, (processor, memory and I/O ports). Power source (e.g., a battery) is not a part of the IoT stack. ISO-OSI layers L1, L2 and L3 of the model are designed to maximize communication Quality of Service (QoS), and energy efficiency while minimizing the cost.

Our IoT stack models shown in figures Fig. 2 and Fig. 3 conform with the OSI architecture design recommendations using module stacking.

IV. IoT Zero Trust Access Control

By common dictionary definitions trust may be viewed as a questionable or unquestionable belief in certain truth of something. Questionable trust may be quantified by the associated probability of the truth validity, while unquestionable trust remains directly related to the so-called absolute trust. Questionable trust with probability of value zero may be considered as Zero Trust (ZT). In this paper, the truth related to IoT security is that any user of any resource in the IoT system is not an attacker. All users are considered as ZT or totally not trusted users.

The ZT Access Control (AC) framework is based on the ultimate micro segmentation and super fine granularity of any resource rights-to-use control. ZTAC requires trust establishment for any user (Human, software or hardware object), whether user is inside or outside of the resource-object main domain, (Such as a network perimeter).

The micro segmentation principle applies to network portions available for remote access, systems and application software and data resources, as well to time slices of possible resource use, and frequency bands of communication lines.

Super-fine granularity of resources approach originates from the Role Based Access Control (RBAC) model of AC systems design [1]. One may view RBAC as the AC system without micro-segmentation of individual roles.

Common implementation of the ZT Architecture (ZTA) assumes two-way authentication and authorization of both user and resource. Two-way authentication should not be mixed up with the multi-level authentication such as Multi Factor Authentication (MFA) that relies on multiple channels enabling (e.g., production and side channel) parallel AC sessions.

ZTA model proposes that any production session initiation protocol assumes that all users, (acting as session primaries), or computing resources (acting as session secondaries), by default, are not permitted to initiate session. All session primaries are subjected to the AC sub-session. In addition, with ZTA systems, session-secondary is subjected to the AC sub-session authentication and authorization too. In other words, the common definition of the ZTA proposes two-way authentication that may also be multi-level.

V. IoT in the Web 7.0 Framework

Developments of the homomorphic and functional cryptography [4,5] with blockchain based architectures [6, 7, 8], have introduced new secure systems design options. We distinguish "project Web 7.0" as one example of a new approach to secure distributed software architectures based on the mentioned developments, [9]. Project Web 7.0 recommends using Decentralized IDentifiers (DIDs) [10] with the derived DIDComm protocol [11], and concept of Verifiable sender-receiver Credentials (VC) [12]. These new design tools are welcome in the situation where addition of the massive IoT networks have imposed excessive loads on the centralized network access control.

Homomorphic cryptography and the concepts of DID and DIDComm have facilitated privacy of all data provided to untrusted application-specific remote processing servers. Namely, untrusted servers can process encrypted data using encrypted functions without ever decrypting any of the two, originally provided data (e.g., encrypted database) or function (e.g., encrypted query). Hiding data is the fundamental principle of what is known as privacy. The new set of tools allow small computing capacity IoT network nodes to have private encrypted data sent and processed by the untrusted remote servers, (e.g., High-Performance Computing HPC servers). Untrusted servers are not capable of decrypting provided data. Safe employment of untrusted remote HPC services is essential for the application of AI algorithms to IoT systems. In addition, using such services adds another seemingly paradoxical dimension to the ZTA based systems, where zero trusted computing resources are provided with private data and private functions without any access control.

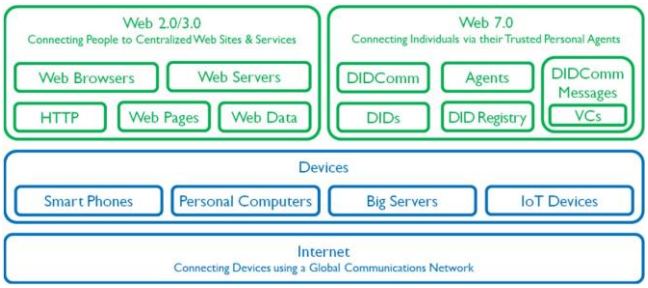

Fig. 4. Web 2.0/3.0 and Web 7.0 ad-hoc arcihtecture models comparison.

With the massive addition of complex IoT networks centralized authentication management became almost impossible problem to deal with. To facilitate implementation of complex ZTAC protocols decentralization of the Access Control System (ACS) components was necessary. ACS decentralization development efforts have produced the Decentralized Digital IDentity (DDID) concept and Self-Sovereign Identity (SSI) management algorithms. These developments are used to strengthens the ZTA based systems security.

Further developments of the above concepts and algorithms have inspired Michael Herman [9] to initiate Web 7.0 project. The name of the project indicates that several future versions of the Web infrastructure were bypassed. Fig. 4 illustrate ad-hoc layered stack diagram of the secure ZTA based application according to [9]. We have to stress that WWW, the Web or W3, represents standardized type of a distributed application layer, that "runs on the Internet."

Fig. 5 presents Web stack based on the well-established Web 2.0/3.0 standards supported by the HTTP/HTTPS application communication protocol layer. Most of the currently used distributed applications running on the Internet are in compliance with the standard Web stack.

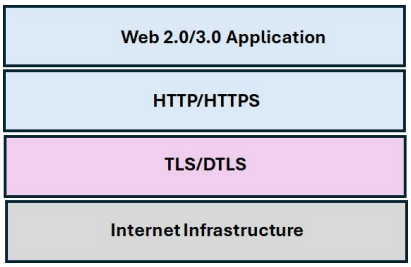

Fig. 5. Web 2.0/3.0 stack with application session security capability.

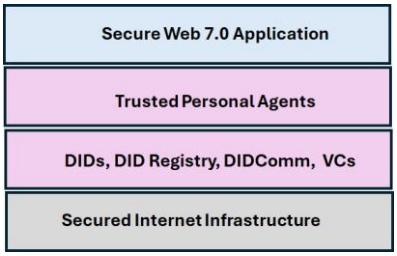

Fig. 6. Web 7.0 stack with application security and privacy capability.

We use project Web 7.0 as an illustration of the modernized distributed ZT security solution. The upward migration trend of the security relevant software into the application layer is apparent. This migration is the result of the evolutionary IoT driven growth of the Internet, and the rising complexity of distributed applications. Project Web 7.0 suggests that future Web standards will incorporate a standardized ZT layer providing a secure platform on which distributed applications may be developed. The Trusted Personal Agents layer shown in Fig. 6 constitutes an example of a trusted platform.

VI. Concluding Remarks

Work on this paper has been inspired by the experience during the round table discussion at Cisco NYC headquarters, in June of 2022. During the meeting the authors of this paper were surprised with Cisco senior network experts diverse understanding of what is IoT and how does it compare with the M2M or SCADA systems.

Our definitions of IoT relevant technology components and models are presented in this paper. We insist on formal avoidance of the arbitrary ad-hoc and technically imprecise terminology. Assumptions that many IoT technology definitions are "self-evident" are not truly justified. Extreme generality such as ITU IoT definition stating that "IoT is a global infrastructure for the information society that provides advanced services through the connection between physical and virtual objects," may be counterproductive.

In conclusion, we consider IoT as an extension of the Internet, proposing a term "Internet 2.0." In addition, we propose an extended scope of the systems security, that we refer to as "Security++." Security++ covers security, privacy and verification of credentials, while supporting secure activity audit trail. Core traditional technologies such as

symmetric and asymmetric cryptography with digital signature and digital certificate followed up by the advancements in the fields of the homomorphic cryptography and block chain technology, led to the paradigm shifting approach to the overall systems security.

REFERENCES

[1] R. Mihajlovic, A. Mihajlovic, “Operating Systems Security,” Soft Electronics, NYC, NY, USA, 2015, ISBN

[2] "The 5 Layers of the IoT Technology Stack," Emnify.com

[3] L. Zharova, “Development of safe IoT networks based on Zero Trust architecture,” Access to Doctoral Studies. FON, University of Belgrade, Belgrade, Serbia, 2018.

[4] Craig Gentry, "A Fully Homomorphic Encryption Scheme," PhD Dissertation, Stanford U, September 2009

[5] Craig Gentry, "Computing Arbitrary Functions of Encrypted Data," Communications of ACM, Posted Mar 1, 2010, https://cacm.acm.org/research/computing-arbitrary-functions-of-encrypted-data/

[6] Shanshan Zhao, Shancang Li, Fuzhong Li, Wuping Zhang, Muddesar Iqbal, "Blockchain-Enabled User Authentication in Zero Trust Internet of Things," Third EAI International Conference, SPNCE 2020, Lyngby, Denmark, August 6-7, 2020.

[7] Shoubai Nie, Jingjing Ren, Rui Wu, Pengchong Han, Zhaoyang Han, and Wei Wan, “Zero-Trust Access Control Mechanism Based on Blockchain and Inner-Product Encryption in the Internet of Things in a 6G Environment,” Academic Editor: Raffaele Bruno, Sensors 2025, 25, 550, https://doi.org/10.3390/s25020550

[8] Mohammed A. Aleisa, “Blockchain-Enabled Zero Trust Architecture for Privacy-Preserving Cybersecurity in IoT Environments,” IEEE Access, Vol13, PP(99):1-1, January 2025. https://ieeexplore.ieee.org/document/10839415.

[9] Michael Herman, "WEB 7.0 Trust Spanning Layer Framework Featuring Raw Credential Sender-Receiver Model and Verifiable Credential Sender-Receiver Model," Trusted Digital Web Hyperonomy Digital Identity Lab Parallel Space Corp, Bindloss, Alberta, Canada.

[10] W3C Editor, "Decentralized Identifiers (DIDs) v1.1; Core architecture, data model, and representations," Draft 31 May 2025. https://w3c.github.io/did/

[11] Sam Curren, atal, "DIDComm Messaging v2.x Editor’s Draft,” Distributed Identity Foundation (DIF), https://identity.foundation/, https://identity.foundation/didcomm-messaging/spec/

[12] Ivan Herman, atal, "Verifiable Credentials Data Model v2.0," Standard Documentation, W3C Recommendation 15 May 2025, https://www.w3.org/TR/vc-data-model-2.0/