Security & Trusted Devices in the Context of Internet of Things (IoT)

Nicolas Sklavos [I, II], Ioannis D. Zaharakis [II, III], Achilles Kameas [II, IV], Angeliki Kalapodi [I]

[I] SKYTALE Group, Computer Engineering & Informatics Dept., University of Patras, Hellas

[II] Computer Technology Institute & Press – "Diophantus" (CTI), Patras, Hellas

[III] Computer & Informatics Engineering Dept., Technological Educational Institute of Western Greece, Hellas

[IV] School of Science and Technology, Hellenic Open University, Patras, Hellas

Abstract - This work targets to the technologies of the Internet of Things (IoT), regarding to security and trusted devices. It provides to the readers a comprehensive understanding of both security and privacy aspects. Modern systems and networks are quoted, in order to cover any questions arising from the theoretical approach. Hardware integration devices are also presented, for flexible implementations for the presented IoT technologies. Emphasis is given to IoT embedded hardware platforms like Udoo, which fully support IoT implementations. Last but not least, data and information preservation are analyzed, so as not to get lost or misused.

Keywords – Internet of Things (IoT), Security, Privacy, Trusted Devices, Hardware Integrations, Embedded Systems, Udoo

I. INTRODUCTION

Recently, more and more devices get connected to the Internet. Consequently, there will be a huge amount of data and information created by these objects. Accordingly, we concentrate on the exploitation of the opportunities opening up for the creation of applications in the areas of automation, sensing, and so on. Thus, we should have a consolidate and flexible platform to manage the emerging Internet of things (IoT) [1]. This is a representative of information management, that is produced by the devices. It is widely spread in the environment, including the ones that lack human presence. IoT is clustered by the addressing, monitoring, connecting, analyzing the system, and reacting. The number of devices, that produce information and data from the environment and launch it to the Internet, offer a huge variety of applications. IoT finds impeccable implementation in several sectors of our daily life and business, from economic processes to health care systems [1-2].

The information exchange brings together several networks. Up to sixty years of continuous study over the information flow efficient implementation, has highlighted recurring standards and strategies. The uncertainty is the main resultant of the information, hence it is based on spatiotemporal coordinates. Complementary uncertainty arises throughout the information transmission. Consequently, the successful information transmission is statistically considered as random. In human telecommunication networks, the assumptions mentioned above are oversimplified; diversity seems to be a method of successful transmission. Thus, the information should be exchanged more than once. Hence, the information is more likely to be delivered to its destination. Alternately, the successful information may be realized with the transmission standard patterns' and formats' modulation. Resources' use obstructs the information transmission. Complex systems appear to maintain their internal stability. Actually, the resources required for the network stability and successful information transmission are numerous. However, the utility throughout the network appears to be very low.

Wishing to design secure networks, we conclude that the security should be initially unified with the network. Absolut security is almost utopian, since there are several obstacles between security and reliability. Additionally, with the preservation of the system's internal state, security attacks get hidden more effectively. Moreover, with the preservation of the system's internal state, security attacks get hidden more effectively. Thus, the IoT networks enable the unprecedented environment and systems' exploration and influence. The initial design of the Internet disregarded security. As a result, intruders use the information negatively and affect the universal economy, even till recent days. Trust and authentication through encryption and security, play a significant role in the consolidation of modern networks. The factors mentioned above are considered as the main pillars of IoT infrastructures [1].

This work introduces a "state of the art" for the IoT environments and devices. It provides people interested in data security and authentication, with all the necessary aspects for the assurance of the data protection. Former related work has focused on credentials authentication and authorization. Nowadays, the basic subject to be analyzed is the privacy and data integrity between users. The connection of different devices to the Internet results in the production of information and data, available through it. Our goal is to approach the most significant pillars that will protect these data and information. Furthermore, it will let data and information be used by the contracting parties and not by users.

978-1-5386-2146-2/17 $31.00 © 2017 IEEE
DOI 10.1109/DSD.2017.81

Apart from the concepts discussed above, we refer to specific protocols, systems and networks that may assist the deep comprehension of the theoretical analysis. Thus, this paper includes Trust, Privacy, Authentication and Security, followed by their equal examples. Concerning the concepts and protocols analyzed in this paper, the significance of their educational value and utility should not be omitted.

Hardware implementation devices are introduced, for flexible integrations for the presented IoT infrastructures. Emphasis is given to IoT hardware platforms such as Udoo, which provides successfully a fully IoT implementation, hardware platform [3].

In addition, all the above introduced technologies, and presented areas of science, besides industry applications, can be adopted as flexible and efficient educational materials from academia and schools, for the provision of knowledge of IoT, security, privacy etc. In these directions, mobile computing and IoT, can be promoted in science education [2].

II. Trust Management Infrastructures

The following models, described in detail, target to trust management infrastructures. A trust model implements only in small and static networks because of its management constraints and memory requirements. A web-of-trust model requires a peer-to-peer validation but it is not feasible for non-static networks [4]. A hierarchical trust model is managed by one or more trust anchors that organize on-the-fly connection requests between network nodes. This system is considered as appropriate for static networks. The hierarchical trust models are divided into Trust Center Infrastructures (TCI) (system Kerberos) and Public Key Infrastructures (PKI) (X.509, Card Verifiable Certificates (CVC), Figure 1) [5].

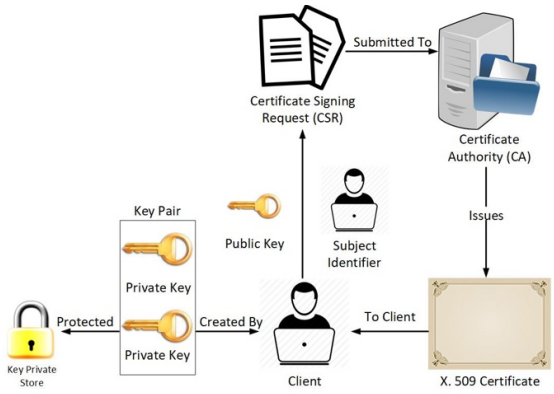

FIG. 1. X.509 Protocol Infrastructure

The identification of both peers is integral part of a digital identity certificate. Uniform Resource Identifiers (URI) are necessary for the identification of the name of a web resource. Nevertheless, the expected number of IoT devices makes the URI inoperable. That is why we use IPv6 address as its unique device identifier. In public key cryptosystems, a pair of keys is provided. That pair of keys is authenticated by both peers. RSA and Elliptic Curve Cryptography (ECC) are the two most famous public key cryptosystems. RSA is based on the difficulty of factoring the product of two large prime numbers. ECC is a quite fresh approach to public key cryptography based on the algebraic structure of elliptic curves over finite fields [6]. ECC appears to be faster than RSA and has established itself as the leading public key cryptosystem of choice for resource-constrained embedded systems. Consequently, an IoT device includes a single universal certificate, whose lifetime is the expected operational life span of the device.

Customized domain-specific Object Identifier (OID) extensions should be defined. This should be done due to the lack of a standardized framework for the encoding of device attributes entailing authorization credentials in a certificate. For Trusted Authentication Protocols, a device may have multiple simultaneous peer-to-peer connections with one or more nodes [7]. In an IP-based environment, the application level protocol is the Transmission Safety Protocol (TLS). In the context of IoT communication, the TLS must be confirmed for a client-authenticated handshake, where both users, exchange and validate the other peer certificate. Several TLS implementations support optional handshake recall functions, that allow the integration of such function ability. In order to facilitate the verification process of a chain of trust, each certification includes the Issued-To and Issued-By fields. The establishment of IoT can only work within its own perimeter. Therefore, the use a two-tier CA hierarchy consisting of a CA root and a set of intermediate CAs is proposed [8]. Embedded systems are usually ineligible in the creation of their own public-private key pairs, as they do lack the entropy to provide fluently random numbers. Device certificates' issue and storage should be controlled and secured.

IoT interfaces should be resistant to exterior cyber- attacks and isolated from the Internet and be self-sufficient. At the initial handshake, device certificates are exchanged by two devices. A PKI should cancel a certificate within the trust chain PKI before it expires [9].

The Certified Catalog Revocation List (CRL) should be downloaded from a warehouse and get processed locally by devices wishing to obtain revocation information.

III. Trust In The Internet of Things

Any trust management system for the IoT should protect its individual devices. A trustworthy firmware usually fails in the process encapsulation via memory virtualization. Consequently, the individual components firmware trustworthiness determination is not enough. Thus, the firmware overall image should be validated. The lack of a secure device firmware updating or patching mechanism is an integral component to maintain security. Otherwise, a vulnerability can compromise a number of systems. An effective patching process should include a network-wide update mechanism. The last one should robust integrity and authenticity checks, minimizes service outages, and allows for a version rollback if needed. Examples of the process mentioned above could be universal serial bus

(USB) dongles, Trusted Platform Modules (TPM) and public key cryptography standards (PKCS).

The system should process as follows: exchange and validate the trust tokens, or create new session tokens. Assurance of the data integrity, optionally in combination with data confidentiality via encryption, for the data trustworthiness is suggested. Data confidentiality via symmetric encryption is often implemented directly in hardware [10-11]; while data integrity is provided via message authentication codes or cryptographic hashes that are attached to the payload data. In this way, a viable mechanism to protect against fabrication is constructed.

IV. Data Privacy And Availability

Threats against data privacy and availability cannot be addressed sufficiently by cryptography-based strategies. Thus, the goal can be achieved with non-cryptography schemes. To prevent the storage nodes overflowing by malicious users practicing attacks, data filtering should be implemented by each storage node for the data sterilization. Their relatively small number leads their constitution to tamper proof hardware, or guarded by humans [12]. Mobile sinks are trustworthy. Nodes can be compromised. When a node is compromised, adversaries can obtain all stored data including secret keys and sensed data. In case of node compromising, the data that are stored will not be available to mobile sinks. Node compromising may cause content privacy breaches, node failure, or even DoS attacks. The level of information uncertainty should be quantified by the definition of privacy [13-17].

Equally, the goal of data availability is the assurance of the production of available data set, with adequate information about the target and acceptable resolution levels, meaning uncertainty. Prior to quantify the information uncertainty, it is important to clarify the relationship between information and messages in sensor networks. Concerning the privacy and availability, the quantity of messages is less important than the content of messages [9]. A typical example of uncertainty is I-states in robotics. As long the weakest point in the system defines its security, the privacy is designated by the definition of the worst state across all possible compounded storage nodes. Similarly, for the network availability definition, the area of the I-state available to the entire network is deemed, compared to the area stored at each storage node. In case of a node failure, the knowledge that may be reconstructed by the left n_{s-1} storage nodes is just the intersection of their I-states. Thus, the worst case across all possible storage node failures is considered as availability:

$$A = \frac{V(\eta * (t))}{\max_{i \in S_1} V(\cap_{j \in S_{1-\{i\}}} \eta_j(t))}$$

Suppose that all the messages are sent only to one storage node, we get A = 0, that is the worst availability, given that the network then has only one failure point. On the contrary, suppose that two (or more) different storage nodes receive each message, A=1, that is the "perfect" availability, as no single failure can end up in data loss. Actually, those are the two heurestics of the energy-efficient protocols failure.

Due to the limited battery capacity to each wireless sensor, one important objective is the minimization of the energy consumed by the messages delivery. Secret-splitting algorithms are the essence of the data dissemination protocols. Like the concept of small pieces of the secret, a rough measurement of the target can be noted by a sensor. A Spatial Privacy Graph (SPG) - based coloring algorithm could offer a sufficient solution to the problem mentioned above.

V. Robust Schemes For Privacy Protection

Due to the development of IoT technologies, more attention is attracted by IoT applications. Two basic applications get analyzed in the personal IoT - the mobile Wireless Body Sensor Network (WBSN) and Participatory Sensing [18-19].

A. Mobile WBSN

Mobile WBSN includes different sensor nodes that get attached to a human body for the monitoring of health or Electro-Encephalo Gram (EEG) physiological sensors. The use of smartphones in eHealth gets interesting more and more. it is useful to use a smartphone as a gateway between WBSN and cloud servers, as long as more smartphones get used and customized applications can be installed on it. Media Access Control (MAC) protocols could protect the communication link privacy among smartphones and cloud servers [20-22].

Nevertheless, superior data encryption for defense against malicious cloud servers is required, as cloud servers are always considered as untrustworthy. So, we should construct a lusty privacy protection (as smartphones may be misused by attackers). Therefore, a lightweight and tough method should be critically designed for the privacy protection [23], (see the following Figure 2).

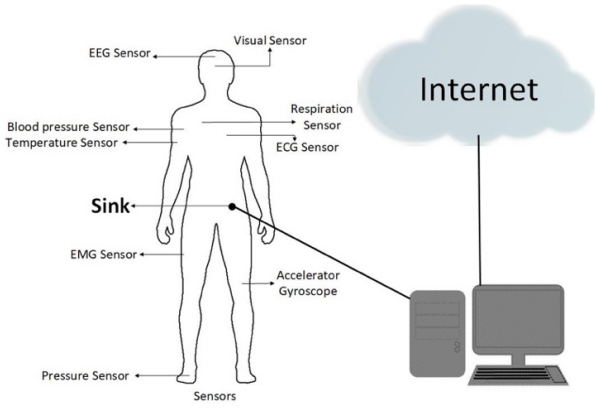

FIG. 2. Protection of Communication Link Privacy

B. Participatory Sensing

The participants (volunteers for information gathering) report their sensory data on their neighbors through smartphones. The stated data are uploaded into central servers, and central servers distribute the data to the users after their processing. The different volunteers may contribute to the

participatory sensing, so as to reach fluent uploaded sensory data and more shared data to be piled [24-27].

Thus, the total defense system should be ensured in order to refrain from the security problems mentioned above. Given that the contributors could be malicious, the security scheme should defend itself against possible interior attackers [24-27].

C. One-Time Mask (OTM) & One-Time Permutation (OTP)

- OTM: Intuitively, a direct method is the follow of an encryption algorithm, for instance the Advanced Encryption Standard (AES). Although, the encryption algorithm invokes a significant computation overhead, the energy consumption per time is proportionate to the number of encryptions [25]. The sensing data uploads' frequency is defined by medical specifications. In this way, the sole factor left for the trade-off is the power consumption reduction of an encryption operation.

  In comparison to AES, XOR-based encryption requires less energy than symmetric encryption methods. Additionally, the source data pieces' number per upload interval is usually low. Thus, the data may rehearse occasionally [28].

- OTP: For all the issues mentioned above, an OTM is considered as safer than a naive XOR scheme and requires less energy in communications. Targeting the larger decrease of the energy consumption, XOR encryption can be replaced with the use of permutation, i.e. the OTP. This is due to the XOR computation elimination, without security being bypassed. As XOR operation is neglected, the computation energy consumption just happens while the one-time permutation generation takes place. OTP's lighter property is justified by its lower cost regarding communication, computation and storage [24].

VI. Entity And Message Authentication

The guarantee that information has not been misused is called authentication. Authentication is verified by the security objective specific to a service. Equally to message authentication, the information from users is preserved by data integrity, whilst the identity of the data originator is ensured by data origin authentication. The identity and the presence of the pretender during the process get both confirmed. The identity verification can be either mutual or unilateral. In the Internet era, the key pairs cannot be verified as the users do not know each other personally. Third parties may assure the CA, that is responsible for vouching the key authenticity.

In terms of authentication, it is classified into two categories:

1. Entity authentication in real time,
2. Message authentication in an elastic time frame.

In the past, authentication was aligned with secrecy. Fixed-password schemes, including time-invariant passwords, are thought as weak authentication, ready to be attacked by eaves dropping and exhaustive search. Several techniques are applied to fixed-password schemes to enhance secrecy. Other than a clear text password, the encrypted password can make it unintelligible or is augmented with a random string to grow the dictionary attack complexity. Nevertheless, as the creation of hash functions and digital signatures proved, authentication does not need secrecy [16]. A hash function forms a one-way function that designs a binary string of arbitrary length to a binary string of fixed length (hash value). The last one enrolls a compact representative of the input string. One-key cryptography with a shared secret key is called symmetric-key encryption; two-key cryptography with a pair of one public key and one private key is called asymmetric-key encryption; unkeyed cryptography with no key is called hash function. The last ones may be used for data integrity to message authentication without maintaining the messages privacy [17]. MAC algorithms aiming to message authentication are keyed hash functions that encrypt hash values with a shared secret key [18]. Moreover, they can be used for digital signatures and identification or entity authentication.

Despite the consideration of identification and entity authentication as synonymous, they can be distinguished as identification only for a stated identity and entity authentication as an identity strengthening. Also, a digital signature is closely related to entity authentication. However, it involves a variable message to be signed for non-renunciation after the fact. Entity authentication uses a fixed message to grant immediate access with no lifetime [28-32].

VII. Authentication Protocols

The parties in entity authentication involve the Claimant (that declares its identity as a message), the Verifier (that is preventing impersonation) and the Trusted third party (mediates between two parties to offer an identity verification service as a trusted authority). The entity authentication objectives include conclusive, transferability and impersonation. The factors of entity authentication are classified, as follows: something known, something possessed and something inherent. These techniques have now been extended beyond authentication of human individuals to device fingerprints. The levels of entity authentication are categorized as weak authentication, strong authentication and Zero-Knowledge (ZK) authentication. The entity authentication properties that are of interest to users are the Reciprocity of identification, the Computational efficiency, the communicational efficiency, the third party and the timeliness of involvement. A CA often runs offline to edit public-key certificates. Its most important components are the nature of trust, the nature of security guarantees and the storage of secrets.

An important implementation is the node eviction in Vehicular Ad Hoc Networks (VANET) [32]. The formation of a VANET constitutes a Vehicular networking features high-speed mobility, short-lived connectivity, and infrastructureless networking.

VANET is an exemplary IoT, with vehicles as things connected to the IoT [33]. Malicious nodes intentionally insert faulty messages to VANET with the potential of massive destruction. Other than faulty nodes, VANET performance is obstructed by malfunctioning Onboard Units (OBU) with fatal aftermaths in safety applications [34]. Moreover, faulty messages inserted to VANET by malicious nodes may cause massive destruction. Errant nodes should get removed anyway

from VANET as fast as possible. Traditionally, a centralized CA revokes an errant node's certificate. Nevertheless, the nature of VANET makes CA-based approaches ineffective. Current node-eviction schemes in VANET allow nodes to decide and act against other errant nodes, both distributed and locally (Figure 3). Local node-eviction schemes can be classified into five categories: Reputation, Vote, Suicide, Abstinence and Police. The performance of node-eviction schemes is affected by various factors. The richness in flexibility and emergence of an agent-based simulation makes it strong in model behaviors and goals of single nodes. A circular road setup in the grid forms the simulation scenario, where vehicles at different speeds cycle around the road and communicate with each other or with the RoadSide Unit (RSU) when in close proximity.

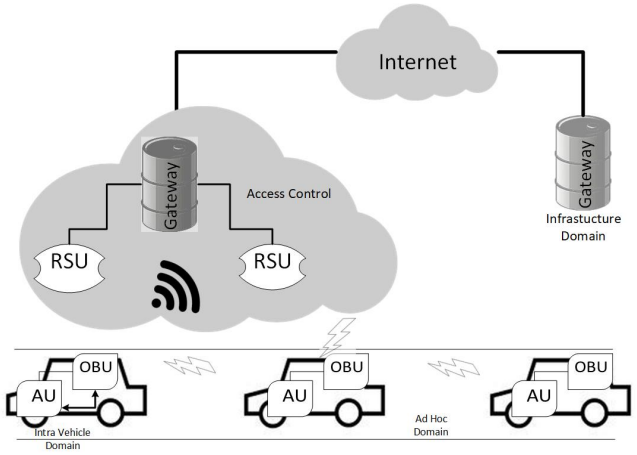

FIG. 3. Visualization of a VANET

The information gets transferred to the CA by RSU. The node-eviction scheme and frequency of contact are implicit in our model. The average time, risk, and utility measures under dynamic environment conditions should be optimized by any node eviction scheme. The node eviction process gets modeled as a set of states and transitions. Eventually all nodes are separated into two subnets depending to their good or bad state. When a node moves from Subnet I to Subnet II, a state transition occurs. Finally, Subnet I or Subnet II will converge into the same kind of nodes. The system is modeled as a network message exchange, certificate- controlled. A List of other nodes Valid Certificates (LVC) is formed by each node. The procedure concludes when good and bad nodes are separated with insignificant risk. However, it gets complicated all the bad nodes to get captured in time by the individual police node. In parallel, multiple bad nodes pop up simultaneously at different spots, as the percentage of bad nodes increases. Moreover, it is possible some bad nodes never being caught, meaning a high risk [35].

The VANET applications are based on providing drivers with precise information. Notwithstanding, serious security threats are included in VANET content delivery. Without common metrics to measure the effectiveness of different techniques, though, consumers cannot be assured, especially regarding critical road safety concerns. Unfortunately, security measurement is difficult and different from other kinds of measurement such as quality of service in wireless multimedia. A security metric is an Asymmetric Profit-Loss Markov (APLM) model. In brief, incidents of detecting data disasters are considered as profits and those of accepting corrupted data as damages.

Similar to the VANET, we could analyze the Medical Cyber Physical Systems (MCPS) that monitor patients' physiological dynamics with distributed computing processes and a wired communication network.

VIII. Security Protocols for IoT Access Networks

Nowadays, we may refer to four main pillars that represent the main technologies. The last ones enable the most common vertical applications related to automation or machine interaction formulate IoT architecture (Figure 4) [36]:

1. The the most disseminate technology is radiofrequency ID (RFID) with target the objects identification and tracking through tags spared in the environment or attached to an object.
2. Machine-to-Machine (M2M) communications.
3. Wireless Sensor Networks (WSN), a constitution of several sensors widely splited in the environment, with the ability of monitoring physical values and wireless communication in a multi hop mode. Its reference standard is the IEEE802.15.4 [25].
4. Supervisory Control and Data Acquisition (SCADA), an autonomous system for real-time smart systems monitoring. heterogeneity of terminals and the necessary guarantee for the data security [37].

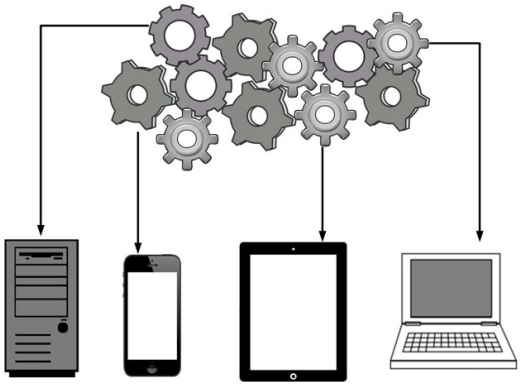

FIG. 4. Machine-to-Machine (M2M) Communications

To conclude, the cognitive security is introduced and applied to the time-based security solution. It highlights the main parameters that need to be monitored and measured by actors to strengthen the security in a parti-coloured and variable scenario like the IoT [38].

IX. Hardware, Devices And IoT

The IoT is developing at a rapid pace thanks to the explosion in the availability of small, low-cost computing hardware. IoT prototyping kits and development boards combine microcontrollers and processors with wireless chips and other components. They come in almost infinite configurations, from tiny battery-powered chips that chirp intermittently over Bluetooth to credit card-sized computers with USB power supplies and high-bandwidth Wi-Fi radios. The abundance of accessories for IoT systems arises questions regarding the appropriate ones that should be used.

Two exemplary IoT hardware implementations are Arduino and Rasberry Pi (Figure 5). The Raspberry Pi was developed in the United Kingdom by the Raspberry Pi Foundation. It constitutes a low cost, credit-card sized computer among a series of single-board computers. The goal of its development was the encouragement of basic computer science knowledge transfer in educational institutions. The original model went beyond expectations, with outrageous sales of its target market, i.e. in robotics. Peripheral devices (i.e. keyboards, mice and cases) are not attached to the Raspberry Pi, with the occasional exception of certain accessories. Through its lifetime, the Raspberry Pi hardware has been revised several times in the form of memory capacity and peripheral-device support improvements.

FIG. 5. Raspberry-Pi Hardware Platform

Arduino was created in the Ivrea Interaction Design Institute as a means of teaching students with no background in computer science (Figure 6). It is an open-source platform used for building electronic projects. Its effectiveness is focused on its ability to read inputs (a finger on a touchscreen or a Facebook message) and return the appropriate outputs (making a sound on a speaker or publishing something online). This is accomplished by sending certain instruction to the microcontroller on the board. The Arduino Software (IDE), based on processing, and the Arduino programming language (based on wiring), are essential for the above successful performance.

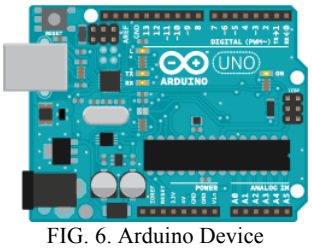

FIG. 6. Arduino Device

New needs and challenges arising in the wider community, have urged Arduino board to adapt to them, modifying its substance from 8-bit boards to products for IoT applications, wearable, 3D printing, and embedded environments.

X. IoT, Full Implementation Platforms

A full IoT implementation platforms is Udoo Kits technologies [3]. Actually, it is a single-board computer, Arduino-compatible, that can perform Android or Linux OS. It is characterized by its ease-to-use, with minimum knowledge requirements (Figure 7). It is combining different computing methods, emphasizing on the proper and weak points of each. Udoo Dual/Quad focuses on educational purposes [3]. Its use may create a well-trained team of developers, designers, engineers, etc. that can built-up new applications and projects, using a low-cost and user-friendly platform. Thus, institutions and companies may have a useful tool for high-standards implementations.

IoT may be successfully implemented following the rules of trust and authentication. As the technology evolves, networks and systems have more and more requirements. IoT systems are vicarious in bridging and preserving complex systems in any appearance of real life.

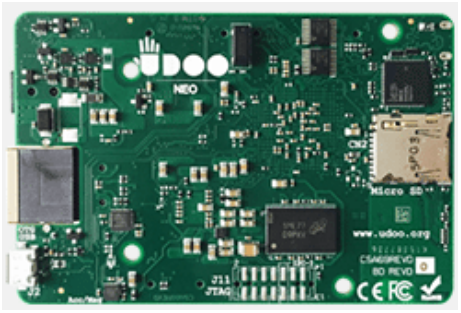

FIG. 7. Udoo Kit: An IoT Implementation Platform

XI. Computational Security For The IoT and Beyond

In terms of the life complexities that have changed over the years, the subject complex systems are often thought as networks of interconnected subunits or as networks capturing interdependencies and relationships [36]. Actually, most instances of our daily life, from socioeconomic infrastructures to road networks depict the development of network science. All the implementations referred previously, reflect the social and biological systems that are far more complex.

The existing complex systems will approach each other by the IoT with the extension of the Internet into the physical world. In this way, the deeper integration of the human world with nature as well as more efficient resources used by intelligent management of flows of people, goods, and assets will be allowed. The goal is the constitution of reliable, unobtrusive, autonomic, and safe pervasive systems and environments.

Thus, functionality, dynamics, processes, and activities, including security of many -if not all- systems on the earth are

deeply affected by the IoT [37]. The technology plays fundamental role in IoT deployment, especially wireless access and sensor networks. Security and authentication throughout networks may eliminate the malicious information usage, from psychological manipulation to state economies and politically motivated hacking attempts. The network protection is based on threshold of the network infrastructure and the defense mechanisms used within them for its integrity (Figure 8).

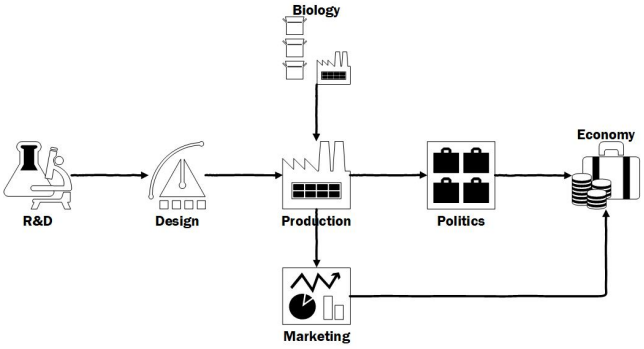

FIG. 8. Complex Systems Connected

Recent telecommunication networks, including IoT sensor networks, use wireless technology. Challenges, as well as opportunities, arise at the lowest protocol level, while using wireless transmissions. Jamming and eavesdropping are considered as the basic wireless transmissions security challenges.

The complexity of biological systems needs to take into account several, hierarchical models based on different spatiotemporal scales. Various "hacks" may be used to reform network models of biological systems. Cellular and subcellular level may be exploited by nanotechnology and nanoscale networks. Additionally, modern healthcare products supported by IoT devices is developing promptly, with applications in fitness, sequel to biological systems are social networks. They are the basic product of brain activity. A typical instance of the social systems hacking is giving and breaking promises. Psychological manipulation is the most common way of social networks attacking. Psychopathia is considered to be a mental function that may control other people's minds. The Internet, along with the IoT sensors, enables traces and digital fingerprints to be left during our life, travel, and daily activities. Human brain is being recently studied due to social states on which humans can be affected due to the privacy of IoT biometric data.

Marketing and sales strategies' evolution has led economies to improvement and creation of challenges and opportunities. As long as the economic globalization has raised competition for resources, many networks are forced to work on low-resource systems, different from supplementary resources systems. Thus, today's economy is strained to achieve geopolitical objectives. IoT systems may assist economic processes to evolve and reach spectacular results. However, IoT systems use will offer area of development for minor or major attacks due to business warfare.

That is where Computer science must mediate and highlight the security significance. The computer cyberwars get more and more the initiate objective for the global competition. Thus, they are not a traditionally assisting component of conventional wars anymore. These wars are considered to be politically and economically motivated. Nowadays, the governments publicly are practicing cyber-attacks strategies equal to their cyber defenses. Cyberwars tend to be connected with other modes of warfare strategies. The IoT is a tool that may increase modern cyber wars by offering special and useful information.

XII. Conclusions And Outlook

Basically, IoT systems have been a significant subject of study, especially the recent years. Thus, the question that arises is whether they should be taught both theoretically and practically. Educational institutes may be the knowledge carriers for the design of secure systems [1-2]. The information and data transmission may be improved via secure systems, like IoT.

IoT is a revolution in secure systems. Its proper usage may lead in the removal of cyber-attacks and use of information by vicious users. Education is the correct level to be pulled for the IoT systems to be studied and developed for the information safe preservation and transmission. Challenges and opportunities always arise. However, education carriers may lead humanity to desirable results and not to devastated situations and events [1-2].

Acknowledgment

This work is under the UMI-Sci-Ed project. This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 710583.

REFERENCES

[1] N. Sklavos, I. D. Zaharakis, "Cryptography and Security in Internet of Things (IoTs): Models, Schemes, and Implementations", IEEE proceedings of the 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS'16), Larnaka, Cyprus, November 21-23, 2016.

[2] I. D. Zaharakis, N. Sklavos, A. Kameas, "Exploiting Ubiquitous Computing, Mobile Computing and the Internet of Things to Promote Science Education", IEEE proceedings of the 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS'16), Larnaka, Cyprus, November 21-23, 2016.

[3] Udoo Kits, www.udoo.org, 2017.

[4] G. Guo, J. Zhang, Improving PGP web of trust through the expansion of trusted neighborhood. IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT), 2011, University of Saskatchewan, Canada.

[5] A. Arsenault, S. Turner, Internet X.509 public key infrastructure PKIX roadmap, IETF Roadmap, September 8, 1998.

[6] J. A. Buchmann, E. Karatsiolis, A. Wiesmaier, Introduction to Public Key Infrastructures. New York: Springer Verlag, 2013.

[7] M. Bourlakis, I. P. Vlachos, V. Zeimpekis (editors), Intelligent Agrifood Chainsand Networks, Wiley-Blackwell, 2011.

[8] Y.Li, Naming in the Internet of Things, Washington University in St. Louis, 2013.

[9] J. Li, Y. Zhang, K. Nagaraja, D. Raychaudhuri, Supporting efficient machine-to-machine communications in the future mobile internet, Wireless Communications and Networking Conference Workshop (WCNCW), 2012, IEEE, New York.

[10] N. Sklavos, "Cryptographic Algorithms on A Chip: Architectures, Designs and Implementation Platforms", proceedings of the 6th Design and Technology of Integrated Systems in Nano Era (DTIS'11), Greece, April 6-8, 2011.

[11] N. Sklavos, "On the Hardware Implementation Cost of Crypto-Processors Architectures", Information Systems Security, The official journal of (ISC)2, A Taylor & Francis Group Publication, Vol. 19, Issue: 2, pp. 53-60, 2010.

[12] N. Sklavos, R. Chaves, G. Di Natale, F. Regazzoni, *Hardware Security and Trust*, Springer, ISBN: 9783319443188, 2017.

[13] L. Chen, R. Lu, and Z. Cao, "Pdaft: A privacy-preserving data aggregation scheme with fault tolerance for smart grid communications," Peer-to-Peer Networking and Applications, vol. 8, no. 6, pp. 1122–1132, 2015.

[14] Haiyong Bao and R. Lu, "A new differentially private data aggregation with fault tolerance for smart grid communications," IEEE Internet of Things Journal, vol. 2, no. 3, pp. 248–258, 2015.

[15] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: an efficient and privacy-preserving aggregation scheme for secure smart grid communications," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 9, pp. 1621–1631, 2012.

[16] J.Won, C. Y. Ma, D. K. Yau, and N. S. Rao, "Proactive fault-tolerant aggregation protocol for privacy-assured smart metering," in INFOCOM 2014. IEEE, 2014, pp. 2804–2812.

[17] W. Jia, H. Zhu, Z. Cao, X. Dong, and C. Xiao, "Human-factor-aware privacy-preserving aggregation in smart grid," IEEE System Journal, pp. 1–10, 2013.

[18] J. Shannon, H. Melvin, A. G. Ruzzelli, Dynamic flooding time synchronization protocol for WSNs, IEEE GLOBECOM, 2012.

[19] M. Seyedi, B. Kibret, D. Lai, and M. Faulkner, "A Survey on intrabody communications for body are a network applications," IEEE Trans. Biomed. Eng., vol. 60, no. 8, pp. 2067–2079, 2013.

[20] J. Liu, Z. Zhang, X. Chen, and K. Kwak, "Certificateless remote anonymous authentication schemes for wireless body area networks," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 332–342, 2014.

[21] T. Ma, P. L. Shrestha, M. Hempel, D. Peng, H. Sharif, and H. Chen, "Assurance of energy efficiency and data security for ECG transmission in BASNs," IEEE Trans. Biomed. Eng., vol. 59, no. 4, pp. 1041–1048, 2012.

[22] Z. Zhang, H. Wang, A.V. Vasilakos, and H. Fang, "ECG-cryptography and authentication in body area networks," IEEE Trans. Inf. Technol. Biomed., vol. 16, no. 6, pp. 1070–1078, 2012.

[23] A. Banerjee, K. Venkatasubramanian, T. Mukherjee, and S. Gupta, "Ensuring safety, security, and sustainability of mission-critical cyber–physical systems," Proceedings of the IEEE, vol. 100, no. 1, pp. 283–299, 2012.

[24] J. Biswas, J. Maniyeri, K. Gopalakrishnan, L. Shue, J. Phua, H. Palit, Y. Foo, L. Lau, and X. Li, "Processing of wearable sensor data on the cloud – a step towards scaling of continuous monitoring of health and well-being," in Proc. 2010 Annual Int'l Conf. of the IEEE Engineering in Medicine and Biology Society (EMBC), September 2010, pp. 3860–3863.

[25] H. Tseng, S. Sheu, and Y. Shih, "Rotational listening strategy (rls) for IEEE 802.15.4 wireless body networks," IEEE Sensors J., vol. 11, no. 9, pp. 1841–1855, 2011.

[26] M. Quwaider, J. Rao, and S. Biswas, "Body-posture-based dynamic link power control in wearable sensor networks," IEEE Commun. Mag., vol.48, no. 7, pp. 134–142,2010.

[27] K. Venkatasubramanian, A. Banerjee, and S. Gupta, "Pska: Usable and secure key agreement scheme for body area networks," IEEE Trans. Inf. Technol. Biomed., vol. 14, no. 1, pp. 60–68, 2010.

[28] K. Vu, R. Zheng, and J. Gao. Efficient algorithms for k-anonymous location privacy in participatory sensing. In Proc. of IEEE INFOCOM12, 2012, pp. 2399–2407.

[29] I. Boutsis and V. Kalogeraki. Privacy preservation for participatory sensing data. In Proc. of 2013 IEEE International Conference on Pervasive Computing and Communications (PerCom '13), pp. 103–113,2013.

[30] D. Christin, C. Rosskopf, M. Hollick, L.A. Martucci, and S.S. Kanhere. Incognisense: An anonymity-preserving reputation framework for participatory sensing applications. In Proc. of 2012 IEEE International Conference on Pervasive Computing and Communications (PerCom '12), pp. 135–143,2012.

[31] C. Costa, C. Laoudias, D. Zeinalipour-Yazti, and D. Gunopulos. Smart trace: Finding similar trajectories in smartphone networks without disclosing the traces. In Proc. of 2011 IEEE 27th International Conference on Data Engineering (ICDE '11), pp. 1288–1291, 2011.

[32] S. Gao, J. Ma, W. Shi, G. Zhan, and C. Sun. Trpf: A trajectory privacy preserving framework for participatory sensing. IEEE Transactions on Information Forensics and Security, vol. 8, no. 6, pp. 874–887, 2013.

[33] M. Groat, B. Edwards, J. Horey, W. He, and S. Forrest. Enhancing privacy in participatory sensing applications with multidimensional data. In Proc. of 2012 IEEE International Conference on Pervasive Computing and Communications (PerCom '12), pp. 144–152,2012.

[34] Jonathan Andrew Larcom and Hong Liu, Authentication in GPS-directed mobile clouds, in Proceedings of IEEE Global Communications Conference 2013 (IEEE GLOBECOM 2013), pp. 470–475, Atlanta, GA, 9–13 December 2013.

[35] Arzad Kherani and Ashwin Rao, Performance of node-eviction schemes in vehicular networks, IEEE Transactions on Vehicular Technology, vol. 59, no. 2, pp. 550–558, 2010.

[36] P. Kasinathan, C. Pastrone, M.A. Spirito, and M. Vinkovits, "Denial-of Service detection in 6LoWPAN based Internet of Things," in Proc. Of IEEE 9th Intl. Conf. on Wireless and Mobile Computing, Networking and Communications (WiMob), 2013, pp. 600–607,7–9 October 2013.

[37] M.R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L.A. Grieco, G. Boggia, and M. Dohler, "Standardized protocol stack for the Internet of (important) Things," IEEE Communications Surveys & Tutorials, vol. 15, no. 3, pp. 1389–1406,2013.

[38] J. Tan, and S.G.M. Koo, "A survey of technologies in Internet of Things," in Proc. of IEEE Intl. Conf. on Distributed Computing in Sensor Systems (DCOSS), 2014, vol., no., pp. 269–274,26–28 May 2014.