Information & Security

Published since 1998

N. Mengidis, T. Tsikrika,
S. Vrochidis & I. Kompatsiaris
vol. 43, no. 1 (2019): 21-33
https://doi.org/10.11610/isij.4302
ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Blockchain and AI for the Next Generation Energy Grids: Cybersecurity Challenges and Opportunities

Notis Mengidis (✉), Theodora Tsikrika,
Stefanos Vrochidis, Ioannis Kompatsiaris

Centre for Research and Technology-Hellas (CERTH), Thessaloniki, Greece
https://www.certh.gr/

ABSTRACT:

Renewable energy sources and the increasing interest in green energy have been the driving forces behind many innovations in the energy sector, such as how utility companies interact with their customers and vice versa. The introduction of smart grids is one of these innovations in what is basically a fusion between the traditional energy grid with the IT sector. Even though this new combination brings a plethora of advantages, it also comes with an increase of the attack surface of the energy grid, which becomes susceptible to cyberattacks. In this work, we analyse the emerging cybersecurity challenges and how the ensuing risks could be alleviated by the advancements in AI and blockchain technologies.

ARTICLE INFO:

RECEIVED: 20 JUN 2019
REVISED: 2 SEP 2019
ONLINE: 14 SEP 2019

KEYWORDS:

cybersecurity, blockchain, AI, energy grid, smart grid, smart contracts

Creative Commons BY-NC 4.0

✉ Corresponding Author: E-mail: nmengidis@iti.gr

Introduction

In past decades, the development of power grids has not been keeping pace with industrial and societal advancements that have created an increased demand of power supply. According to Ratner and Glover, during the period from 1950 to 2014, just in the US, energy production and consumption increased more than two and three times respectively.[1] With this increased demand of electricity, issues like voltage spike and sags, blackouts, and overloads have increased as well, resulting in availability issues which consequently lead to revenue losses for the energy industry. As an example, a study conducted by Knapp and Samani in 2013 indicated that the American economy loses annually approximately $ 150 billion due to power interruptions.[2] Furthermore, the power industry alone produces up to 40 percent of United States' carbon dioxide emissions,[3] a percentage slightly lower within the European Union.[4]

To cope with the aforementioned shortcomings of the energy industry, the need to efficiently manage a variety of energy sources became evident. It also became clear that legacy power systems can no longer meet the requirements of modern society in terms of reliability, scalability, manageability, and cost-effectiveness. These needs gave birth to *smart grid*, a dynamic and interactive infrastructure with new energy management capabilities, which however inevitably created a system with potential vulnerabilities in terms of cybersecurity. In this paper, we present some of the most emerging cybersecurity challenges related to smart grid and discuss mitigation techniques based on blockchain and artificial intelligence (AI).

Background

The smart grid can be considered as the next evolution step in today's power grid technology and smart meters specifically are the corner stone of this evolution. In case an energy provider decides to shift towards a smart grid implementation, the first step is to install a smart meter in every customer and premises. Smart meters are devices that offer the capability both to the provider and to the customer real-time (or near real-time) monitoring of electricity consumption or production, in the case of e.g. photovoltaic cells. They also offer the possibility to read the measurements locally and remotely, and additionally allow the provider to limit or terminate the supply of electricity where appropriate.

The National Institute of Standard and Technology (NIST) defines the smart grid as a composition of seven domains: bulk generation, transmission, distribution, customers, markets, service providers, and operations.[5] The first three domains are responsible for the power flow, whereas the last four correspond to the part of the energy grid responsible for data collection and power management. In order to interconnect the aforementioned domains, a backbone network is required which can be broken down to smaller local-area networks. Figure 1 illustrates how this interconnection takes place in a logical as well as in a network level.

On a higher level, a smart grid consists of four main components; the Advanced Metering Infrastructure (AMI), the Supervisory Control and Data Acquisition (SCADA), the plug-in hybrid vehicle (PHEV), and various communication protocols.[6] AMI's role is measuring and analysing energy usage and allows a two-way communication between the consumer and the utility company.

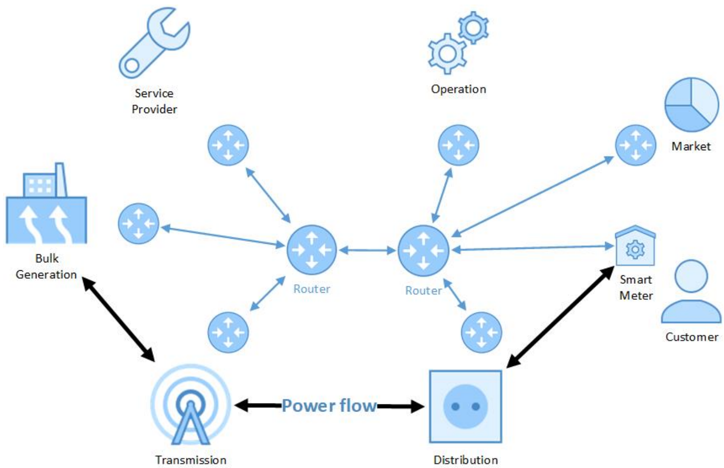

Figure 1: Network architecture of the Smart Grid.

Smart meters communicate with the AMI headend, which aggregates the information from a large number of meters, and relay the aggregated data to the Meter Data Management System (MDMS). Communication between the smart meters and the AMI headend is usually achieved through wireless links such as Wireless Sensor Networks (WSN),[7] cellular systems,[8] or even cognitive networks.[9]

As a result of the highly-distributed nature of the AMI network and the openness of the wireless communication medium, we are motivated to examine the cybersecurity challenges that arise due to the increased attack surface and investigate the opportunities that this early stage of smart meters' adoption has to offer.

Cybersecurity Challenges

Cybersecurity poses one of the largest and multifaceted challenges that the smart energy grid and the IoT ecosystem in general will have to address in the years to come. Given the number of interconnected sensors, devices and networks that constitute a smart grid, it becomes evident that it is susceptible to online probing, espionage, and constant exploitation attacks by malicious actors aiming at disrupting the stable and reliable energy grid operation, obtaining sensitive customer information, as well as threatening the CIA triad (confidentiality, integrity and availability) of the network.[10] In order to have a clearer picture of the dangers posed by the integration of smart energy meters in the traditional energy grid, we will examine the security requirements of a smart grid and analyse the most high-profiled challenges from a cybersecurity perspective.

Cybersecurity Requirements and Objectives in the Smart Grid

According to NIST, the main criteria required to ensure the security of information in any given information system, thus smart grid as well, are *confidentiality*, *integrity* and *availability, also known as the CIA triad*.[11] It is also widely accepted that *accountability* is another important aspect of security, therefore it will also be included as an additional criterion below.[12]

Confidentiality

Generally, confidentiality is the preservation of authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Once an unauthorised entity, individual, or process gains access to proprietary information, we consider that the confidentiality of the specific system is lost. In the context of the smart energy grid, information such as the past and present measurement values of a meter, consumption usage, and billing information are considered confidential and hence must be protected. Most utility providers nowadays offer electronic bills and some of them even web portals with real-time statistics of energy usage for each customer individually. With this increased accessibility of consumer data on the internet, confidentiality is starting to become increasingly significant.[13]

Availability

Availability is defined as the provision of timely and reliable access to and use of information and services. In the case of the smart grid, availability can arguably be considered as the first priority since an availability loss in the grid can potentially have a serious adverse effect on organisational operations, organisational assets and individuals. An availability attack takes place in the form of traffic flooding, where the attacker aims to delay or disrupt message transmission,[14] or buffer flooding where the malicious actor aims to overwhelm the AMI's buffer with false events.[15] Both attacks fall under the umbrella of Denial of Service (DoS) and the main objective of the attacker is to exhaust the computational resources of the smart grid and degrade the network communication performance of the grid.

Integrity

Integrity in smart grid is ensuring that there will be no kind of violation of data, including destruction, modification or loss of information while maintaining consistency and accuracy.[16] In smart grids, malicious alteration and tampering of critical data in sensors, meters, and command centres can be divided into three major categories. First, there is the integrity of the information in the network, which includes price information and power consumption. In addition, there is the integrity of the software running on the devices, and finally there is the integrity of the hardware which is somewhat of a more cyber-physical challenge. For instance, a set of compromised smart meters whose readings have been altered by the attacker can be considered as an integrity attack.[17]

Accountability

Accountability is ensuring that every action in any given system can be traced back to the person or entity that performed it. This way, all the information can be used as evidence without anyone being able to dispute the chain of custody of the information or question the non-repudiation of the system. An example of an accountability attack concerns the monthly electricity bill of the consumers. Typically, a smart meter is able to determine and report the customer's power consumption on a daily basis. However, if a meter is under attack and its readings are altered, then the customer will end up with two separate readings, one from the meter and one from the utility company.

Cybersecurity Threats and Weaknesses

In this section, we will identify four of the most prevalent cybersecurity challenges that stem from the integration of IT with traditional energy grid systems. Also, we will see how most of the challenges emanate from our need to defend the CIA triad which we analysed in section 3.1.

Cyber-attacks

Cyber-attacks on smart grids are a very commonly discussed topic due to the vulnerabilities existing in the grids' communication, networking, and physical entry points. Attacks in the smart grid environment can be categorised into two broad categories [18]:

- *Passive attacks*: these are attacks that do not intend to affect system resources and their sole purpose is to extract system information.[19] In these kinds of attacks, the attacker's objective is to learn or use information that it is transmitted, or to retrieve information stored in the system. Generally, passive attacks are relatively hard to detect, since no alteration of data takes place, thus the best defence against them is prevention through solid security mechanisms.
- *Active attacks*: these attacks are aimed towards a system's resources and attempt to either modify or disrupt them. The most common actors in these kinds of attacks are malicious users, spyware, worms, Trojans, and logic bombs.[20] According to Li et al., the most ordinary types of these attacks are device attacks, data attacks, network availability attacks, and privacy attacks,[21] whereas Wang and Lu classify the attacks as those targeting availability, those targeting integrity, and finally those targeting confidentiality.[22]

Trust

Varying requirements exist for operations performed in smart grids. The system consists of the power grid itself, the communication network, and the devices controlling the process.[23] Honesty and trustworthiness are essential behaviours in the relationship between the consumer and the utility company, thus the validity of the energy bill of the consumed energy is of vital importance from the consumer point of view, whereas the energy provider needs a trustworthy and fully auditable reporting tool for each operating device in the grid. These demands create new challenges that need to be addressed in an environment that all entities cannot be considered as trusted. Therefore, a trusted intermediary entity needs to decide upon the status validity of the devices and manage the access policies for the network, in a way that can authentically report the current state of the network to third parties.

Single Point of Failure

From a reliability perspective, it is well documented that a single point of failure is one of the biggest concerns in a master-slave architecture. In smart grids, a DDoS attack could disrupt, delay, or prevent the flow of data and eventually even collapse the AMI network. This denial of data exchange means a loss of control messages and may affect the power distribution to the customers in the smart grid.

From a scalability perspective, the number of the clients is limited by the capacity of the AMI network in terms of bandwidth and routing capabilities, and the latency is determined by the round-trip time (RTT) between the AMI head-end and the devices in the network. In addition, as related research by Rodrigues, Guerreiro, and Correia shows,[24] there is an exponential growth of IoT devices, a trend that will likely be followed by smart energy meters as well. Therefore, scalability is emerging as one of the key factors for energy grid development and exploitation, considering the technical challenges connected with the geographical distribution over broad areas and the connectivity and resource availability in general.[25]

Identity and Access Management

One particular issue with smart meters in smart grids is the management of the cryptographic keys that are required by every meter for cryptographic computations, such as the encryption of the transmitted data. Before the deployment of the AMI, the confidentiality of customer privacy and customer behaviour, as well as message authentication for meter reading, and control messages must be ensured. This can be solved by encryption and authentication protocols which depend on the security provided by cryptographic keys. The current industry standard is the use of a X.509 certificate for identification and for establishing a secure connection during data transmission. However, these cryptographic keys remain static for the whole life-cycle of the meter, and a key management mechanism that would allow manufacturers to periodically update or revoke them does not seem to be currently implemented. Furthermore, since such keys are also considered a form of strong device recognition, an attacker could possibly abuse the private key of the device [26] and enable access to the device by unauthorised parties, or even potentially impersonate the device in the network.

Based on the requirements set by NIST regarding cryptographic keys, e.g., a fixed cryptoperiod (i.e., expiration date) or the existence of a key recovery function,[27] we consider that such a generic approach cannot be applied in an intelligent environment such as a smart grid, since the keys remain static and vulnerable and even though some functional requirements can be met, stricter security requirements cannot be fulfilled. A zero trust design philosophy is required in order to inspire confidence in the validity of the secure keys and certificates.

Opportunities

The emergence of technologies such as Blockchain and Artificial Intelligence (AI) has created a new field for research and innovation, while at the same time offering opportunities in the field of smart energy grids. In the following section, we will attempt to identify some of these opportunities and envision how to apply these technologies in order to countermeasure the aforementioned cybersecurity challenges.

Blockchain Application for Cyber Resiliency

Blockchain is defined as a distributed data base or *digital ledger* that records transactions of value using a cryptographic signature that is inherently resistant to modification.[28] In a move towards a cyber-resilient energy grid, Blockchain could commoditise trust and also potentially support auditable multi-party transactions between energy providers and customers.

The blockchain is the equivalent of a book maintained by a bank, which contains all the accounts and each transaction made. One of the most interesting aspects of blockchains is that they contain the records of every transaction made since the beginning, also known as *genesis block*, by using a peer-to-peer distributed timestamp server which generates computational proof of the chronological order of the transactions.[29]

The use of blockchain presents numerous potential cybersecurity benefits to the electricity infrastructure:

- *Identity of Things*: As mentioned in Section 3.2.4, identity and access management of the devices in the grid is an issue that needs to be addressed efficiently. The ownership of a device can change during its lifetime or even be revoked in case a consumer is not consistent with his financial obligations towards the energy provider. Apart from ownership, there are also attributes that each device has, such as manufacturer, type, deployment GPS coordinates etc. Blockchain is able to address these challenges since it can register and provide identity to connected devices along with a set of attributes that can be stored on the blockchain distributed ledger in a fully auditable manner.[30]
- *Data integrity*: As per blockchain's design, every transmitted block in the network, thus all data transmitted by the devices in the grid, are cryptographically signed and proofed by the sender. Each node has its own unique

public and private key and thereby it is ensured that the data are encrypted and cannot be tampered. Finally, all blocks are recorded and timestamped on the chain and cannot be changed in a later time, therefore ensuring the accountability and the integrity as described in Sections 3.1.4 and 3.1.3 respectively.

- *Securing communications*: The most commonly used network communication protocols, such as HTTP, MQTT and XMPP, are not secure by design and thus have to be wrapped within TLS at the application layer. However, protocols such TLS or IPSec rely on complicated and centralised certification authorities for the management of the keys, mainly through a public key infrastructure (PKI). With blockchain, there is no longer the need to rely on a centralised authority, since each node in the network receives a Universally Unique Identifier (UUID), as soon as it joins the network, and also creates an asymmetric key pair. This allows to simplify the handshake procedure and use light-weight protocols, such as TinyTLS, without handling and exchanging PKI certificates during the initial phase of the connection.[31] This way we are able to tackle the challenge described in Section 3.2.4 in an efficient manner without the added overhead of complex PKIs.

AI and Smart Contracts

Despite the fact that blockchain solutions add a layer of cryptography in communications and digital transactions, in complex IoT environments such smart energy grids, many complex cybersecurity challenges remain. An example is the patch management of the smart meters or their improper configuration. Especially in the first case, the timing between the discovery of a new vulnerability and the deployment of the patch to the affected devices is crucial. In such a scenario, a public repository could be queried periodically in order to check whether a new patch is available. The process could be performed with a blockchain-based *smart contract*, which would validate the transportation of the correct patch and provide an incentive for updating. Such a smart contract could operate on the basis of device-specific information, mainly model and firmware version of the device. According to this data, the contract would decide on whether an update is necessary and instruct the device to perform the update. In case the device is compromised and refuses to update, its trust score could start to decline and the energy provider would be notified regarding the misbehaving device.

Whereas the distributed public ledger of blockchain may assist in increasing the trustworthiness, AI-enabled smart contracts could add unique value in the timely response to emerging cyber threats like an emergency response to a naturally occurring weather event or a cyber-physical hybrid attack.[32] That way, some functions of the power grid would become self-healing and resilient.

Additionally, through the combination of AI and blockchain, we could achieve an almost real-time security response to unauthorised attempts to change configurations or network and sensor settings. Anomaly-based intrusion detection systems assisted by Machine Learning (ML), could be an effective method to detect intrusions and attacks, which have not been previously detected. Such a system, combined with the immutability of blockchain, could reduce the overhead of the forensics investigation in case of a security incident, by providing a well-established timeline of events for evidence-analysis.

Conclusions

Smart grid is a system composed of various distributed components with the primary goal to intelligently deliver electricity, while at the same time allows the easy integration of new features and metrics in the traditional grid. Cybersecurity in the smart grid is a relatively new area of research and in this paper, we presented an initial survey of security requirements and challenges. This was followed by a discussion on opportunities and mitigation techniques based on disruptive technologies such as blockchain and AI. Even though the proposed solutions still remain an uncharted territory in smart grid applications, the advancements in blockchain and AI make them the more attractive technologies thus far in the pursuit of building a secure and resilient smart grid.

Acknowledgement

This work was supported by the ECHO project which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no 830943

References

1 Michael Ratner and Carol Glover, "U.S. Energy: Overview and Key Statistics," Congressional Research Service, *CRS Report* R40187, June 27, 2014, https://fas.org/sgp/crs/misc/R40187.pdf.

2 Eric D. Knapp and Raj Samani, *Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure* (Waltham, MA: Syngress, 2013).

3 Jing Liu, Yang Xiao, Shuhui Li, Wei Liang, and CL Philip Chen, "Cyber Security and Privacy Issues in Smart Grids," *IEEE Communications Surveys & Tutorials* 14, no. 4 (2012): 981-997.

4 Johan Rootzén, "Reducing Carbon Dioxide Emissions from the EU Power and Industry Sectors – An Assessment of Key Technologies and Measures," *Research.chalmers.se*, 2012, https://research.chalmers.se/en/publication/157370.

5 Christopher Greer, David A Wollman, Dean E Prochaska, Paul A Boynton, Jeffrey A Mazer, Cuong T Nguyen, Gerald J FitzPatrick, Thomas L Nelson, Galen H Koepke, and Allen R Hefner Jr., "NIST Framework and Roadmap for Smart Grid Interoperability Standards, release 3.0," NIST Special Publication, 2014.

6 Fatemeh Halim, Salman Yussof, and Mohd Ezanee Rusli, "Cyber Security Issues in Smart Meter and Their Solutions," *International Journal of Computer Science and Network Security* 18, no. 3 (2018): 99-109, http://paper.ijcsns.org/07_book/201803/20180313.pdf.

[7] Ramn A. Len, Vijay Vittal, and G. Manimaran, "Application of Sensor Network for Secure Electric Energy Infrastructure," *IEEE Transactions on Power Delivery* 22, no. 2 (2007): 1021-1028, https://doi.org/10.1109/TPWRD.2006.886797.

[8] Salman Mohagheghi, J. Stoupis, and Z. Wang, "Communication Protocols and Networks for Power Systems – Current Status and Future Trends," *2009 IEEE/PES Power Systems Conference and Exposition*, Seattle, WA, 2009, pp. 1-9, https://doi.org/10.1109/PSCE.2009.48401742009.

[9] A. Ghassemi, S. Bavarian, and Lutz Lampe, "Cognitive Radio for Smart Grid Communications," *2010 First IEEE International Conference on Smart Grid Communications*, Gaithersburg, MD, 2010, pp. 297-302, https://doi.org/10.1109/SMARTGRID.2010.56220972010.

[10] SGC Committee, "Smart Grid Cybersecurity Strategy Architecture and High-Level Requirements," The Smart Grid Interoperability Panel, Technical Report, 2014, https://www.hsdl.org/?view&did=758327.

[11] SGC Committee, "Smart Grid Cybersecurity Strategy Architecture and High-Level Requirements."

[12] Jing Liu, Yang Xiao, and Jingcheng Gao, "Achieving accountability in smart grid," *IEEE Systems Journal* 8, no. 2 (2014): 493-508, https://doi.org/10.1109/JSYST.2013.2260697.

[13] Y. Yang, Tim Littler, Sakir Sezer, Kieran McLaughlin, and H.F. Wang, "Impact of Cyber-Security Issues on Smart Grid," *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, Manchester, 2011, pp. 1-7. https://doi.org/10.1109/ISGTEurope.2011.6162722.

[14] Lu, Xiang Lu, Wenye Wang, and Cliff Wang, "Review and Evaluation of Security Threats on the Communication Networks in the Smart Grid," *2010 – MILCOM 2010 Military Communications Conference*, San Jose, CA, 2010, pp. 1830-1835, https://doi.org/10.1109/MILCOM.2010.5679551.

[15] Dong Jin, David M. Nicol, and Guanhua Yan, "An Event Buffer Flooding Attack in DNP3 Controlled SCADA Systems," *Proceedings of the 2011 Winter Simulation Conference (WSC)*, Phoenix, AZ, 2011, pp. 2614-2626, https://doi.org/10.1109/WSC.2011.6147969.

[16] Kostas Siozios, Dimitrios Anagnostos, Dimitrios Soudris, and Elias Kosmatopoulos, eds., *IoT for Smart Grids* (Springer, 2019).

[17] Annarita Giani, Eilyan Bitar, Manuel Garcia, Miles McQueen, Pramod Khargonekar, and Kameshwar Poolla, "Smart Grid Data Integrity Attacks: Characterizations and Countermeasures," *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Brussels, 2011, pp. 232-237, https://doi.org/10.1109/SmartGridComm.2011.6102324.

[18] Elias Bou-Harb, Claude Fachkha, Makan Pourzandi, Mourad Debbabi, and Chadi Assi, "Communication Security for Smart Grid Distribution Networks," *IEEE Communications Magazine* 51, no. 1 (2013): 42-49, https://doi.org/10.1109/MCOM.2013.6400437.

[19] Shuguang Cui, Zhu Han, Soummya Kar, Tung T. Kim, H. Vincent Poor, and Ali Tajer, "Coordinated Data-injection Attack and Detection in the Smart Grid: A Detailed Look

at Enriching Detection Solutions," *IEEE Signal Processing Magazine* 29, no. 5 (2012): 106-115, https://doi.org/10.1109/MSP.2012.2185911.

20 M. Zekeriya Gunduz and Resul Das, "Analysis of Cyber-attacks on Smart Grid Applications," *2018 International Conference on Artificial Intelligence and Data Processing (IDAP)*, Malatya, Turkey, 2018, pp. 1-5, https://doi.org/10.1109/IDAP.2018.8620728.

21 Xu Li, Xiaohui Liang, Rongxing Lu, Xuemin Shen, Xiaodong Lin, and Haojin Zhu, "Securing Smart Grid: Cyber Attacks, Countermeasures, and Challenges," *IEEE Communications Magazine* 50, no. 8 (2012): 38-45, https://doi.org/10.1109/MCOM.2012.6257525.

22 Wenye Wang and Zhuo Lu, "Cyber Security in the Smart Grid: Survey and Challenges," *Computer networks* 57, no. 5 (2013): 1344-1371, https://doi.org/10.1016/j.comnet.2012.12.017.

23 Patrick McDaniel and Stephen McLaughlin, "Security and Privacy Challenges in the Smart Grid," *IEEE Security & Privacy* 7, no. 3 (2009): 75-77, https://doi.org/10.1109/MSP.2009.76.

24 Luis Rodrigues, Joel Guerreiro, and Noélia Correia, "RELOAD/CoAP Architecture with Resource Aggregation/Disaggregation Service," *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Valencia, 2016, pp. 1-6, https://doi.org/10.1109/PIMRC.2016.7794607.

25 Paolo Bellavista and Alessandro Zanni, "Towards Better Scalability for IoT-cloud Interactions via Combined Exploitation of MQTT and CoAP," *2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI)*, Bologna, 2016, pp. 1-6, https://doi.org/10.1109/RTSI.2016.7740614.

26 Todd Baumeister, "Adapting PKI for the Smart Grid," *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Brussels, 2011, pp. 249-254, https://doi.org/10.1109/SmartGridComm.2011.6102327.

27 Elaine Barker, "Recommendation for Key Management," NIST Special Publication 800-57 Part 1, Revision 4, http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4.

28 Nicole Radziwill, "Blockchain Revolution: How the Technology behind Bitcoin is Changing Money, Business, and the World," *The Quality Management Journal* 25, no. 1 (2018): 64-65, https://doi.org/https://doi.org/10.1080/10686967.2018.1404372.

29 Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008, https://bitcoin.org/bitcoin.pdf.

30 Minhaj Ahmad Khan and Khaled Salah, "IoT Security: Review, Blockchain Solutions, and Open Challenges," *Future Generation Computer Systems* 82 (2018): 395-411, https://doi.org/10.1016/j.future.2017.11.022.

31 Khan and Salah, "IoT Security: Review, Blockchain Solutions, and Open Challenges."

32 Michael Mylrea, "AI Enabled Blockchain Smart Contracts: Cyber Resilient Energy Infrastructure and IoT," 2018 AAAI Spring Symposium Series, https://www.aaai.org/ocs/index.php/SSS/SSS18/paper/view/17593/15392.

About the Authors

Notis **Mengidis** received his Computer Science degree from the Aristotle University of Thessaloniki (2015), and in 2018 he received his MSc in Telecommunications and Cybersecurity, from International Hellenic University. Since January 2019, he works as a research assistant at the Informatics and Telematics Institute (ITI) of the Centre of Research & Technology Hellas (CERTH). His research interests among others include: Cybersecurity, botnets, penetration testing, malware analysis and blockchain technologies.

Dr. Theodora **Tsikrika** received the Degree in Computer Science from University of Crete, Heraklion, the MSc degree in Advanced Methods in Computer Science from Queen Mary, University of London, and the PhD degree in Computer Science also from Queen Mary, University of London. She is a postdoctoral research fellow with CERTH-ITI and has previously worked as a postdoctoral researcher at CWI (Amsterdam, the Netherlands), the University of Applied Sciences Western Switzerland (Sierre, Switzerland), and the Royal School of Library and Information Science (Copenhagen, Denmark). Her research interests focus on the fields of Information Retrieval and Data Mining, and include Web search, domain-specific data discovery, Web and social media mining, multimodal analytics and evaluation, with particular focus on security applications. Theodora Tsikrika has participated as WP and task leader in several European Security research projects (e.g., ECHO, CONNEXIONs, PROPHETS, TENSOR, and HOMER) and in several European ICT research projects (e.g., MULTISENSOR, PROMISE, and VITALAS), and has co-authored more than 60 publications in refereed journals and international conferences.

Dr. Stefanos **Vrochidis** received the diploma degree in electrical engineering from Aristotle University of Thessaloniki, a master's degree in radio frequency communication systems from the University of Southampton, and a PhD in electronic engineering from Queen Mary, University of London. He is a senior researcher with CERTH-ITI and co-founder of Infalia Private Company. His research interests include semantic multimedia analysis, information retrieval, semantic search, data mining, multimedia search engines and human interaction, computer vision and robotics, open source intelligence and security applications. Dr Vrochidis has participated in more than 25 National and European projects in 4 of which he has been the Project (or deputy) Coordinator and in four – the Scientific/Technical Manager. He has been the organizer of various workshops and has served as regular reviewer in several scientific journals and conferences. He is also the co-author of more than 130 conference, journal and book chapter articles.

Dr. Ioannis (Yiannis) **Kompatsiaris** is a Researcher Director at CERTH-ITI, the Head of Multimedia Knowledge and Social Media Analytics Laboratory and Deputy Director of the Institute. His research interests include multimedia, big data and social media analytics, semantics, human computer interfaces (AR and BCI), eHealth, security and culture applications. He is the co-author of 129 papers in refereed journals, 46 book chapters, 8 patents and more than 420 papers in international conferences. Since 2001, Dr. Kompatsiaris has participated in 59 National and European research programs including direct collaboration with industry, in 15 of which he has been the Project Coordinator and in 41 the Principal Investigator. He has been the co-organizer of various international conferences and workshops and has served as a regular reviewer, associate and guest editor for a number of journals and conferences currently being an associate editor of IEEE Transactions on Image Processing. He is a Senior Member of IEEE and member of ACM.