Cloud Manufacturing: Security, Privacy, and Forensic Concerns

OVER THE LAST FEW DECADES, THE WAY MANUFACTURING ENTERPRISES HAVE BEEN MANAGED HAS UNDERGONE A RADICAL RETHINKING.[1] This has led to the so-called Industry 4.0, or the fourth industrial revolution, and traditional management models have been progressively abandoned. A concrete example of this trend is the European Factories of the Future Research Association, a public-private partnership under Horizon 2020.[2] EFFRA has produced a roadmap to pave the way for introducing innovation-driven transformations within the European manufacturing sector.

Christian Esposito and Aniello Castiglione
University of Salerno

Ben Martini
University of South Australia

Kim-Kwang Raymond Choo
University of Texas at San Antonio

Such a tremendous boost for innovation in manufacturing arises from the current economic environment, which is extremely volatile and globalized. Enterprises need to rapidly respond to changing or uncertain market demands, provide customized products and services, and compete at the international level by targeting multiple potential markets around the world. Enterprises are deemed successful if they can provide a wide variety of high-quality products while keeping manufacturing and distribution costs low to meet customer expectations and needs. Moreover, the contemporary need to target multiple markets in different countries requires enterprises to expand their production capability by setting up multiple manufacturing sites around the world.

The *networked manufacturing* framework,[3] illustrated in Figure 1, interconnects the strategic centers of an enterprise, enabling it to operate at a worldwide scale. This is different from a logistic network, where products are exchanged to lower production costs. The networked manufacturing framework envisions the exchange of products, associated services, and knowledge to improve productivity, flexibility, and competitiveness. Networked manufacturing is a concrete realization of distributed manufacturing where a network is used to integrate production and shipping facilities, with the headquarters playing the role of centralized manager for the overall network by monitoring and adjusting the day-to-day contingencies and activities.

Models such as networked manufacturing started as intrafirm organizational models to address the globalization needs of enterprises, but later evolved into a collaborative approach between firms. The issues and challenges of the current economic environment are making it more difficult to run small and medium enterprises (SMEs), since they don't have the skills and resources required to compete against larger enterprises. Therefore, SMEs are joining efforts and capabilities to overcome their limitations through collaboration, which can be short term or more stable and durable.

The collaborative networked manufacturing model, depicted in Figure 2, has paved the way for more advanced organizational structures, such as

2325-6095/16/$33.00 © 2016 IEEE

virtual enterprises or virtual organizations, which allow businesses or public services to join forces to better respond to business opportunities and needs. Both intrafirm and interfirm collaborative networks are giving rise to novel forms of organizations and establishing a more pervasive role for information sharing within the current manufacturing practice.[4] In fact, most of these collaborative approaches are based on rich and efficient information sharing, which supports proper scheduling and monitoring of facility costs, performance and flexibility, decision making, and management of the network complexity in terms of integrated firms and facilities.

The Advent of Cloud Manufacturing

Smart manufacturing increases competitiveness and efficiency through interconnection and cooperation among companies or among resources within a single company. Recent advances in information and communication technologies (ICT) that support collaboration and cooperation among organizations

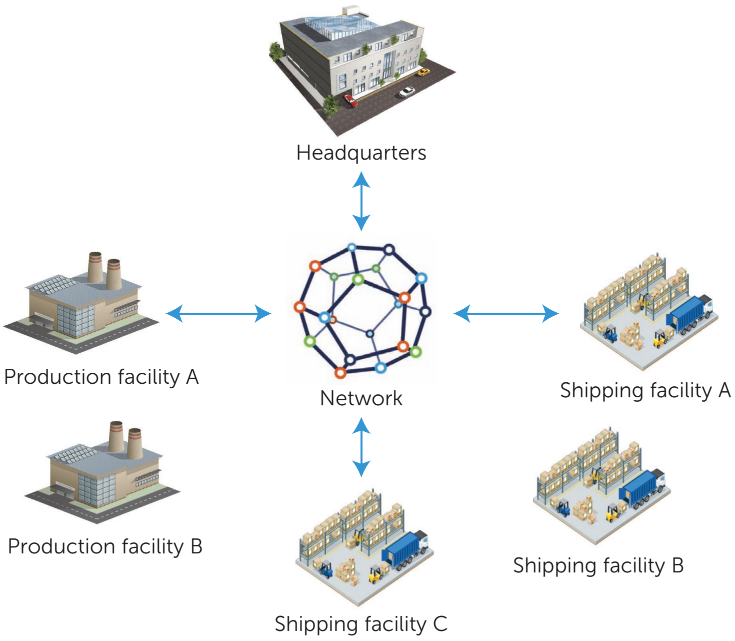

FIGURE 1. Schematic representation of networked manufacturing.

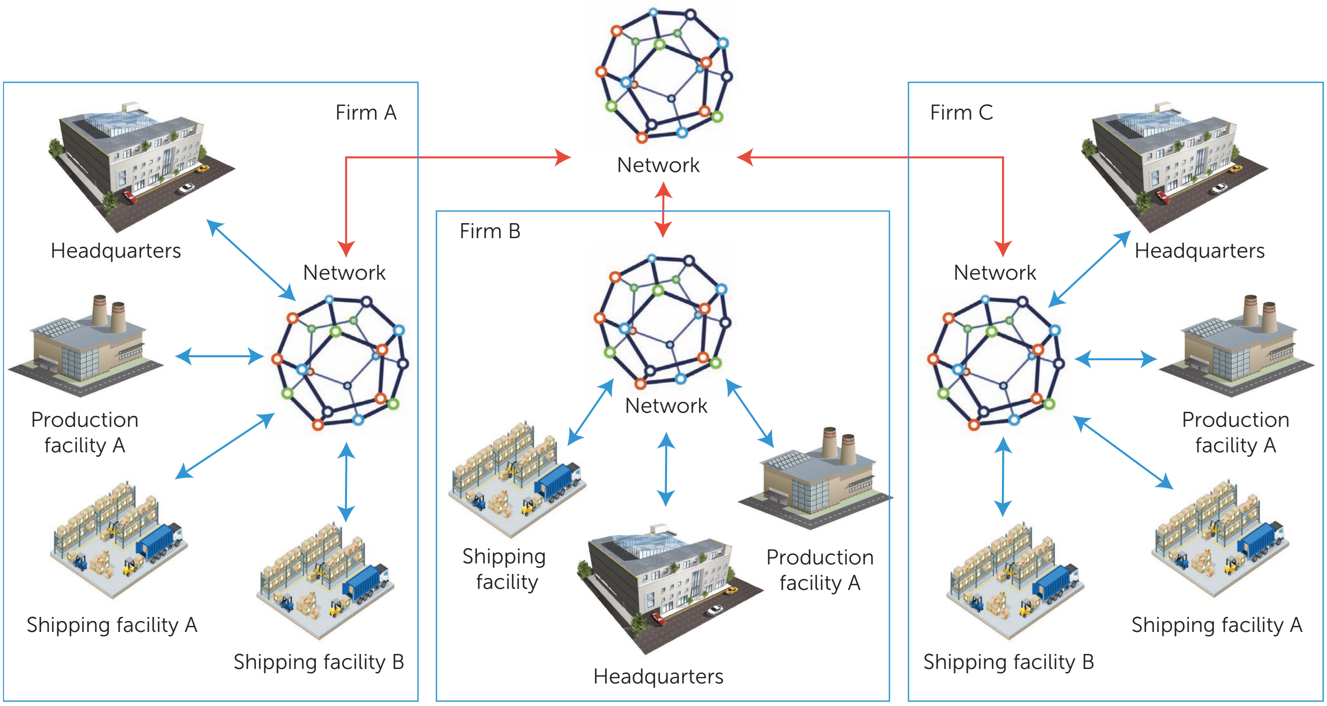

FIGURE 2. Schematic representation of collaborative networked manufacturing.

beyond mere information exchange, to the realization of knowledge and service sharing, have made this vision possible. Open source/Web-based applications are considered key enablers of integrated enterprise practices and strategies for the manufacturing industry due to their flexibility, interoperability, and proliferation.[5] However, the increasing complexity of managing the software needed to deal with these collaborative schemes makes computing extremely expensive for an enterprise, particularly SMEs. Hence, the proliferation of collaborative networked manufacturing solutions within the manufacturing sector is slowing.

The emergence of cloud computing within the business environment offers a solution.[6] Cost is the main driver of enterprises' adoption of cloud computing. The cloud's pay-per-use cost model lets enterprises reduce capital investments in information technology, leading to significant cost savings. However, cloud computing does more than provide cost-effective computing; it also provides for the flexible provisioning of ICT resources, with its elasticity allowing for rapid scaling to the dynamic and ever-changing needs of enterprises.

Two approaches for adopting cloud computing within the manufacturing domain have emerged as most promising:

- the naïve and direct use of cloud platforms as data sharing and storage enablers to support collaboration schemes, as exemplified in the collaborative networked manufacturing model; and
- cloud manufacturing, where distributed resources within the networked manufacturing framework participating in a manufacturing business process are modelled and encapsulated as cloud services and managed in a centralized manner.[7]

Such a solution is increasingly being applied within industrial practice. An IBM industry survey revealed that two-thirds of mid-sized companies have already implemented or are about to migrate to a cloud-based storage model.

Figure 3 shows a cloud manufacturing application model, which can be realized using a layered service-oriented architecture. At the lowest level is a set of manufacturing resources (the physical facilities or capabilities) within a firm or across multiple firms, required to move the product through the development lifecycle. The next layer contains cloud services that virtualize, encapsulate, and identify the underlying manufacturing resources, which are responsible for executing manufacturing tasks while ensuring high production quality and reliability. The service layer encompasses cloud services built on top of the virtualized manufacturing resources to implement remote monitoring, scheduling, and control of manufacturing resources. The last level is the application layer, which presents a set of services acting as interfaces for users to the cloud manufacturing solutions. The provided operations allow designers and administrators to model manufacturing processes, perform these processes by properly integrating and composing virtual resources, and monitor a running manufacturing process by visualizing some measures of merit.

The radical rethinking of the manufacturing industry from the traditional production-oriented approach to the service-oriented one envisioned by the networked manufacturing framework, collaborative networked manufacturing, and cloud manufacturing faces some obstacles in the current industry environment.[8] Foremost are the safety and security issues such collaborative schemes present. The networks used to support collaborations and cooperation convey business-critical information, while the virtualization and service orientation of manufacturing resources make enterprises vulnerable to a new series of attacks not seen in traditional manufacturing approaches.

Today, security is a key concern when using cloud computing in mission-critical scenarios, including the manufacturing domain. A cloud manufacturing solution could be compromised, and critical data could be stolen or altered by amateur attackers. Experts, perhaps hired by competitors, could also compromise a cloud system, significantly affecting an organization's productivity and reputation. Therefore, equipping cloud manufacturing solutions with proper security management mechanisms and policies is critical to avoid possible threats to both the solution and consumers.

Secure Cloud Manufacturing

As a recent Cloud Security Alliance (CSA) report noted, data breaches are among the most frequent se-

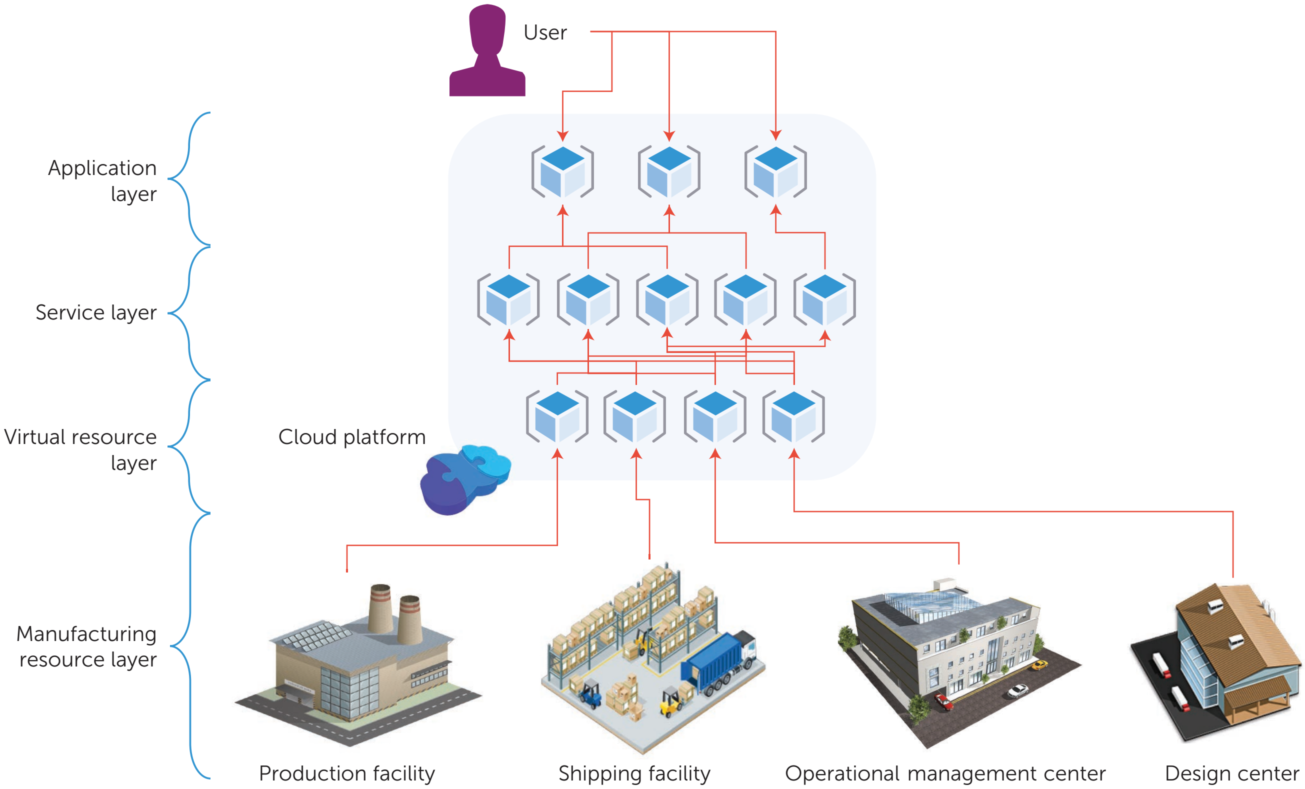

FIGURE 3. Layered architecture of cloud manufacturing.

curity compromises[9] and have proved to have tremendous consequences from both legal and economic viewpoints. A cloud data breach is an unauthorized or illegal access to data hosted within the cloud, in terms of both retrieving and modifying data. This is a particular concern within the context of cloud manufacturing, where a data breach can result in the loss of sensitive corporate information, such as trade secrets or contract details, and consequently negatively affect the company's reputation. Encryption, the most common solution to prevent data breaches,[10,11] is offered in several cloud platforms.

However, encrypting data that's outsourced to the cloud doesn't solve the problem. Within the context of cloud manufacturing, sources of data breaches are typically within the company rather than outside it. In fact, a malicious insider, such as a current or past employer, a system administrator, a contractor, or a business partner, might be the culprit, as the CSA report indicates.[9] Some cloud platforms facilitate the use of encryption keys controlled by their customers. This isn't effective in case of malicious insiders, who might possess the correct keys for the decryption. Manufacturers using cloud services therefore need to also adopt proper key management best practices that go beyond the technical aspects to consider organizational and social perspectives for security assurance.[12] Such best practices are typically a set of reasonable guidelines and considerations for an effective strategy over all seven phases of a key management process, as Figure 4 illustrates.

- A key should be produced using a cryptographic module with at least FIPS 140-2[13] compliance for memory, strength, and secrecy requirements.
- An appropriate key distribution approach must be used to distribute the key to all authorized users to ensure its secrecy.[14]
- Users can choose to persistently store keys in key stores that provide secrecy guarantees.

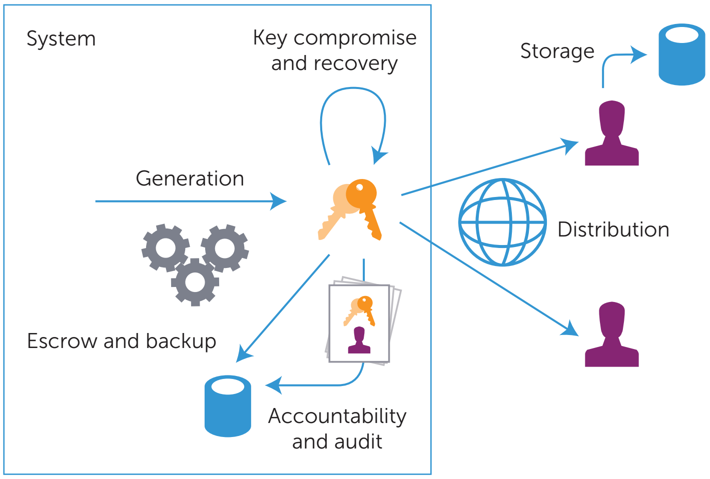

FIGURE 4. Phases of key management.

- Because keys can be lost, systems with data at rest for long periods need to have a key recovery plan.
- To prevent key compromises or reduce their impact when detected, a system should document which entity received or had control of a certain key.
- When a key is known to have been compromised, it must be revoked and new keys generated and distributed to authorized entities.

A strategy for managing cryptographic keys is only the first defense against data breaches. Because data breaches are almost inevitable, systems must be equipped with a means to identify and document them and to notify relevant personnel. Specifically, it's necessary to have means to determine that data has been read or changed by an unauthorized entity, to inform the data owner that a breach has occurred, and to collect and store, in a forensically sound manner, all the information related to the breach and the suspected culprit. Recent laws and regulations for data protection have detailed how to notify and document data breaches, highlighting the importance of this concern. The ePrivacy Directive (2002/58/EC), for example, introduced a European data breach notification requirement for the electronic communication sector.[15]

An effective cloud manufacturing data loss solution should support the four stages of prevention, identification, notification, and documentation of data breaches. Such a solution could be deployed as software as a service (SaaS), as Figure 5 illustrates, to be easily integrated into current operational processes in the manufacturing domain (in fact, it can be easily extended to other domains with similar requirements). Specifically, such a solution should be equipped with a module for breach notification and one for documentation according to relevant standards and regulations. To facilitate seamless and simple notifications, we envision the use of a secure publish/subscribe service—that is, a middleware solution for the asynchronous and confidential exchange of breach information with interested parties.[16]

Criminal data breaches would be of particular interest to law enforcement, and specifically digital forensic practitioners. This issue is important to manufacturing companies, since data breaches can ruin their reputation and market opportunities and give their competitors an advantage. Companies must be able to defend their copyrights in court and successfully prosecute the culprits behind data breaches. Companies could use digital forensic techniques to ensure that evidence collected as part of a data breach event remains forensically sound (that is, suitable to be upheld as original evidence in court). This process starts with initial preservation (that is, collection) and continues through transmission to law enforcement, and ultimately presentation in court. The large body of digital forensic literature can assist in the development of this part of the process.[17,18]

Another module should be devoted to the application of an effective key management strategy, according to given standards and regulations, such as the one issued by the US National Institute for Standards and Technology.[19] Key management is a serious concern in the manufacturing domain, since it's the main factor allowing data breaches. As previously stated, malicious insiders could obtain valuable documents and trade secrets related to a company's products and manufacturing processes, share them with competitors, or use them to start their own business. Preventing such breaches requires a proper key management system to record which employees hold certain keys and revoke the keys when employees don't need them. Key management should be stringent to avoid the possibility of violations, but not so strict that employees can't do their jobs effectively.

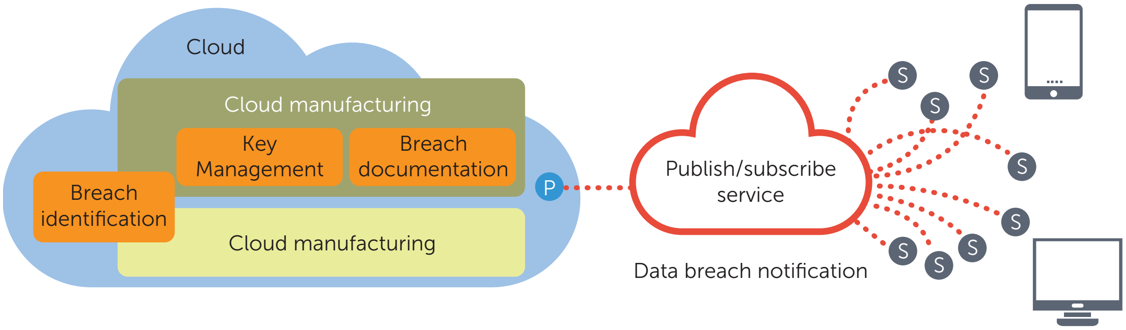

FIGURE 5. Software-as-a-service (SaaS) solution for defending against data breaches in cloud manufacturing.

Despite all of the preventive measures put in place by a company, a data breach can still occur. A manufacturing company must be able to promptly detect a data breach to prevent malicious insiders and competitors from further exploiting the vulnerability to obtain company documents and secrets. The last module in the SaaS solution we envision is responsible for identifying such breaches. The breach identification module will monitor the data exchanged and stored within clouds when a given manufacturing process is performed, checking the correct flow of data within the overall infrastructure.

Breach identification remains an open research issue, and lacks a substantial body of literature. One possible solution is to use digital watermarking and other steganography-based approaches on the data held by the cloud manufacturing solution. The principle is to include data that can be used to detect possible unauthorized modifications or access resulting from a data breach.

FUTURE WORK IN THIS AREA INCLUDES IMPLEMENTING A PROTOTYPE OF OUR SOLUTION IN A REAL-WORLD ENVIRONMENT WITH THE AIMS OF EVALUATING OUR SOLUTION, AND REFINING IT IF NECESSARY. Other possible future research directions include investigating reliability and fault-tolerance issues in cloud manufacturing, the relationship or influence reliability and fault-tolerance issues have on security issues, and the possibility of a holistic approach for these two complementary aspects.

References

1. Y. Koren, *The Global Manufacturing Revolution: Product-Process-Business Integration and Reconfigurable Systems*, John Wiley & Sons, 2010.
2. European Factories of the Future Research Association, *Factories of the Future: Multi-Annual Roadmap for the Contractual PPP under Horizon 2020*, report, 2013; www.effra.eu/attachments/article/129/Factories%20of%20the%20Future%202020%20Roadmap.pdf.
3. B. Montreuil, J.-M. Frayret, and S. D'Amours, "A Strategic Framework for Networked Manufacturing," *Computers in Industry*, vol. 42, nos. 2–3, 2000, pp. 299–317.
4. S. D'Amours et al., "Networked Manufacturing: The Impact of Information Sharing," *Int'l J. Production Economics*, vol. 58, no. 1, 1999, pp. 63–79.
5. L.M. Camarinha-Matos et al., "Collaborative Networked Organizations: Concepts and Practice in Manufacturing Enterprises," *Computers & Industrial Eng.*, vol. 57, no. 1, 2009, pp. 46–60.
6. S. Mareston et al., "Cloud Computing: The Business Perspective," *Decision Support Systems*, vol. 51, no. 1, 2011, pp. 176–189.
7. X. Xu, "From Cloud Computing to Cloud Manufacturing," *Robotics and Computer-Integrated Manufacturing*, vol. 28, no. 1, 2012, pp. 75–86.
8. D. Wu et al., "Cloud Manufacturing: Strategic Vision and State-of-the-Art," *J. Manufacturing Systems*, vol. 32, no. 4, 2013, pp. 564–579.
9. Cloud Security Alliance, *The Treacherous 12:*

Cloud Computing Top Threats in 2016, tech. report, Top Threats Working Group, Feb. 2016; https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf.

10. L. Townsend, “How to Prevent a Data Breach in the Cloud,” blog, Townsend Security, 2016; http://info.townsendsecurity.com/bid/63294/How-to-Prevent-a-Data-Breach-in-the-Cloud.
11. B. Grobauer, T. Walloschek, and E. Stocker, “Understanding Cloud Computing Vulnerabilities,” *IEEE Security & Privacy*, vol. 9, no. 2, 2011, pp. 50–57.
12. Open Web Application Security Project, “Key Management Cheat Sheet,” 2016; www.owasp.org/index.php/Key_Management_Cheat_Sheet.
13. US Nat’l Inst. for Standards and Technology, *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards Publication, May 2011, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.
14. K.-K.R. Choo, *Secure Key Establishment*, Advances in Information Security vol. 41, Springer, 2009; http://dx.doi.org/10.1007/978-0-387-87969-7.
15. European Parliament and the Council of the European Union, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), July 2002; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML.
16. C. Esposito and M. Ciampi, “On Security in Publish/Subscribe Services: A Survey,” *IEEE Comm. Surveys and Tutorials*, vol. 17, no. 2, 2015, pp. 966–997.
17. B. Martini and K.-K.R. Choo, “An Integrated Conceptual Digital Forensic Framework for Cloud Computing,” *Digital Investigation*, vol. 9, no. 2, 2012, pp. 71–80.
18. D. Quick, B. Martini, and K.-K.R. Choo, *Cloud Storage Forensics*, Syngress Publishing/Elsevier, 2013.
19. US Nat’l Inst. for Standards and Technology, *Recommendation for Key Management*, NIST Special Publication 800-57, July 2012; http://dx.doi.org/10.6028/NIST.SP.800-57p1r3.

CHRISTIAN ESPOSITO *is adjunct professor at the University of Naples “Federico II,” Italy, and a research fellow at the University of Salerno, Italy. His research interests include information security and reliability, middleware, and distributed systems. Esposito has a PhD in computer engineering from the University of Naples “Federico II.” Contact him at christian.esposito@dia.unisa.it.*

ANIELLO CASTIGLIONE *is adjunct professor at the University of Salerno, Italy, and at the University of Naples “Federico II,” Italy. His research interests include security, communication networks, information forensics and security, and applied cryptography. Castiglione has a PhD in computer science from the University of Salerno, Italy. He is member of several associations, including IEEE and ACM. Contact him at castiglione@ieee.org.*

BEN MARTINI *is a research fellow at the University of South Australia. His research interests include cybersecurity and digital forensics, focusing on contemporary technologies such as cloud computing and mobile devices. Martini has a PhD in digital forensics from the University of South Australia. Contact him at ben.martini@unisa.edu.au.*

KIM-KWANG RAYMOND CHOO *holds the Cloud Technology Endowed Professorship in the Department of Information Systems and Cyber Security at the University of Texas at San Antonio. His research interests include cyber and information security and digital forensics. Choo has a PhD in information security from Queensland University of Technology, Australia. He’s a senior member of IEEE and a Fellow of the Australian Computer Society. Contact him at raymond.choo@fulbrightmail.org.*