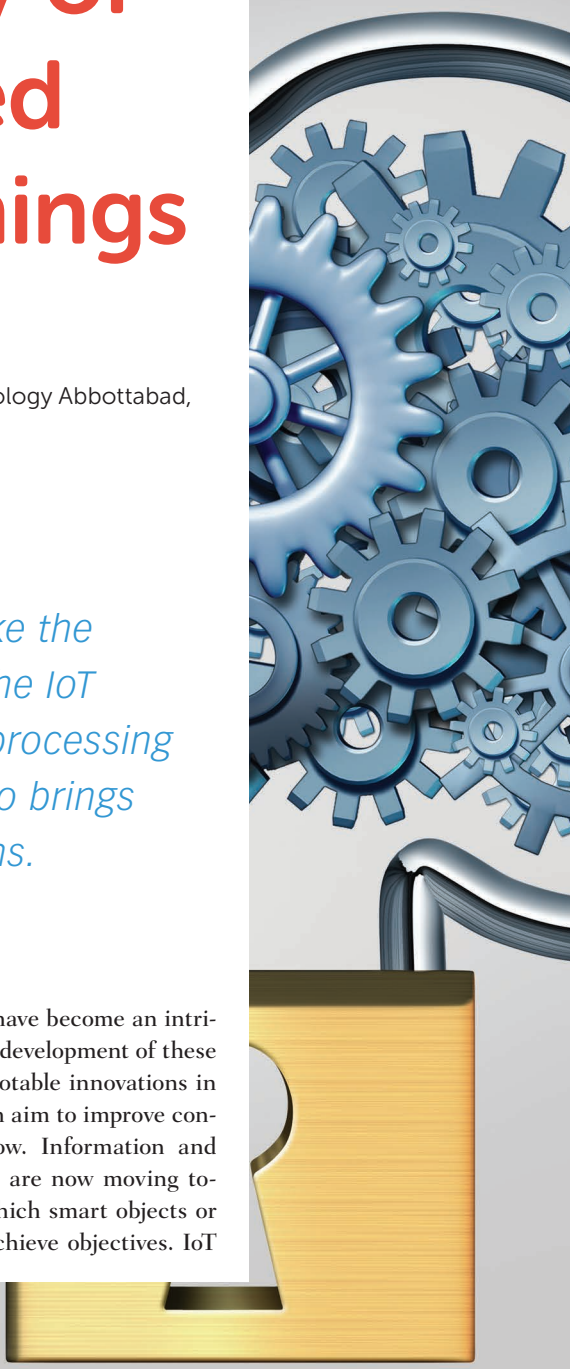
Security and Dependability of Cloud-Assisted Internet of Things

Mazhar Ali, COMSATS Institute of Information Technology Abbottabad, Pakistan
Samee U. Khan, North Dakota State University
Albert Y. Zomaya, University of Sydney, Australia

Cloud computing promises to make the billions of low-profile "things" in the IoT resource rich by enhancing their processing and storage capabilities, but it also brings forth security and privacy concerns.



Over the past decade, smart devices have become an intricate part of our everyday lives. The development of these devices has also led to numerous notable innovations in communication technologies, which aim to improve connectivity and accelerate traffic flow. Information and communication technologies (ICT) are now moving toward the Internet of Things (IoT), a new paradigm in which smart objects or "things" interact with each other and with humans to achieve objectives. IoT

2325-6095/16/$33.00 © 2016 IEEE

is envisioned as transforming the physical world into its representative digital world. It has gained considerable attention within the research community and has opened pathways to many applications that can benefit society. Moreover, the IoT will enable the development of smart and autonomous environments by allowing billions of things to communicate to provide services in fields such as business, healthcare, social networks, logistics, agriculture, and e-commerce.

However, the ubiquitous interconnection of these things will also generate a gigantic amount of data. This generated data needs to be stored and processed in a flexible and rapid manner into information that can then be used for various purposes. Smart devices usually have low processing and computational power and limited ability to handle significant data generation. In addition, these resource-limited devices can't handle security-oriented protocols and cryptographic methodologies that involve intensive computations. Cloud computing could prove to be the perfect platform for meeting the processing and storage demands of smart devices. By integrating heterogeneous service models and devices into a cohesive system, IoT exhibits tremendous potential to meet the information-processing demands of smart environments. Similarly, the pervasive nature of cloud computing promises to make low-profile things resource rich by enhancing their processing and storage capabilities.

Nonetheless, the concept of cloud computing for IoT brings forth security and privacy concerns. The comprehensive connectivity topographies of these technologies leave them open to malicious attacks and destabilization of normal processes and trust. In addition, the heterogeneity and ubiquity of the things intensify the complexity of design and deployment of security methodologies. Architectures for integrating IoT and the cloud, protocols for communication and interoperability, and data processing mechanisms need new methodologies and approaches for security and dependability.

The Articles

This special issue provided a platform for the research community and industry to present novel research on the development and deployment of architectures and methodologies to strengthen the security and dependability of cloud computing for the IoT. Submissions to the issue were each reviewed by three experts in the field; we selected three for inclusion in the special issue. We've also included a roundtable discussion on security issues in the cloud-assisted IoT. Participants of the roundtable are active researchers in the field of cloud-assisted IoT and have a diversity of experiences to share with *IEEE Cloud Computing* readers.

In "Encrypted Data Management with Deduplication in Cloud Computing," Zheng Yan, Mingjun Wang, Yuxiang Li, and Athanasios Vasilakos approach the problem of secure data access to IoT-generated data stored in the cloud. Their methodology considers deduplication of encrypted data to save cloud storage space, reduce storage costs, and provide green cloud storage services by using the hash values of previously generated data. Different keys are used to provide different cryptographic services. If the storage request is from the data owner and the same data is already present on the cloud (verified by comparing hash values of stored and incoming data), the owner is notified and data isn't stored again. If the storage request is from some other user, a request is sent to the data owner for verification. If the other user is allowed to access the data, it's reencrypted by the owner with a new set of policies and sent to the cloud. The cloud service deletes the old copy, saving the new one. Data from the requesting user isn't stored on the cloud. However, a new set of policies allows the user to download and decrypt the owner's copy of the data. The scheme uses attribute-based encryption (ABE) to provide privacy and deduplication by employing an explicit access control mechanism over secured data. The cryptographic operations are performed using various ABE-based generated keys. The data owned by any particular entity is encrypted by the same key. The generated hash code ensures deduplication of the same data at the cloud end. The scheme can implement both ciphertext policy ABE (CP-ABE) and key policy ABE (KP-ABE). The authors implemented their approach, and their results demonstrate the approach's security and effectiveness.

As an emerging field, IoT has many open issues that need to be addressed. A lot of work is being done on the security and dependability of cloud-assisted IoT in industry and academia. In "The Quest for Privacy in the Internet of Things," Pawani Porambage, Mika Ylianttila, Corinna Schmitt, Pardeep Kumar, Andrei Gurtov, and Athanasios Vasilakos provide a holistic

overview of privacy issues faced by IoT applications and technologies. They discuss the layered architecture of IoT technologies and detail IoT privacy issues in different application domains, such as healthcare, smart homes, public safety, and supply management. They categorize the privacy issues into four key areas: user privacy, data mining, underlying IoT technologies, and legal regulations regarding IoT. The article presents existing security frameworks and solutions proposed by the research community as well as open issues and future directions in the field. The authors conclude that privacy by design is a more stable and trustworthy solution than patching security solutions with existing applications.

Heshan Kumarage, Ibrahim Khalil, A. Alabdulatif, Zahir Tari, and Xun Yi discuss motivations to integrate cloud and IoT for provision of better services and identify issues pertaining to cloud-assisted IoT in the invited article, "Secure Data Analytics for Cloud-Integrated Internet of Things Applications." They advocate the use of fully homomorphic encryption (FHE) to perform big data analytics with cloud-integrated IoT. The authors identify three application areas that can use FHE securely to implement data analytics services in the context of cloud-assisted IoT: smart grid billing services, sensor data anomaly detection, and secure patient classification and diagnosis for e-health systems. They outline three frameworks and data analytic models. We believe that the presented work will accelerate new dimensions in research on secure data analytics in integrated cloud-IoT architectures.

A roundtable discussion in support of this special issue, available as a Web Extra (https://extras.computer.org/extra/mcd2016020024s1.pdf), centers on security concerns associated with cloud-assisted IoT. Roundtable participants Ravi Sandhu, Mark Hagerott, Martin Carlisle, and Weisong Shi—all experts in the field and active in cloud-assisted IoT research—agree that security is of paramount importance for IoT in general and cloud-assisted IoT in particular. An interesting viewpoint that came up during the discussion is that IoT security extends beyond the digital world and into the physical world. The roundtable participants also point out that the absence of privacy by design introduces considerable risk in the IoT. Moreover, conventional security methodologies don't provide adequate security in this altogether new technology. They caution that governments should chalk out policies and procedures related to IoT before the world faces major security threats due to this new technology.

We hope this special issue will prove beneficial for the community in clarifying the concepts underlying cloud-assisted security and dependability. We believe that these articles can serve as a source of future research directions and will help lead to refined and effective security methodologies. We thank all of the researchers who submitted their work and pay special tribute to the reviewers who helped to bring the presented works to their current form. We're also grateful to the *IEEE Cloud Computing* editorial board and staff for their support of this special issue.

MAZHAR ALI *is an assistant professor in the Department of Computer Science at COMSATS Institute of Information Technology in Abbottabad, Pakistan. His research interests include information security, formal verification, social network analysis, modeling, the Internet of Things, and cloud computing systems. Ali has a PhD in information security from North Dakota State University. Contact him at mazhar@ciit.net.pk.*

SAMEE U. KHAN *is an associate professor of electrical and computer engineering at North Dakota State University in Fargo. His research interests include optimization, robustness, and security of cloud, grid, cluster and big data computing, social networks, wired and wireless networks, power systems, smart grids, and optical networks. Khan has a PhD from the University of Texas, Arlington. He's a senior member of IEEE, a fellow of the Institution of Engineering and Technology, and a fellow of the British Computer Society. Contact him at samee.khan@ndsu.edu.*

ALBERT Y. ZOMAYA *is the chair professor of high-performance computing in the School of Information Technologies at the University of Sydney, Australia. His research interests include complex systems, parallel and distributed computing, and green computing. He's a fellow of IEEE, the Institution of Engineering and Technology, and the American Association for the Advancement of Science. Contact him at albert.zomaya@sydney.edu.au.*