future internet

MDPI

Editorial

Special Issue on Security and Privacy in Blockchains and the IoT

Christoph Stach

Institute for Parallel and Distributed Systems, University of Stuttgart, Universitätsstraße 38,
70569 Stuttgart, Germany; christoph.stach@ipvs.uni-stuttgart.de

The increasing digitalization in all areas of life is leading step-by-step to a data-driven society. From an information technology perspective, this process is particularly promoted by the Internet of Things (IoT). Nowadays, a variety of sensors can be embedded in virtually any everyday object, enabling users to continuously quantify a wide range of aspects of life. For instance, a smartwatch can use GPS technologies to determine the current location of its user, an accelerometer and gyroscope to recognize the user's activity, and a microphone to capture and interpret voice messages and spoken instructions of its user. Even special use sensors are installed in those IoT devices, such as a heart rate sensor or sensors for recording insulin levels, which can be used to capture and monitor health data. Additionally, such IoT devices have the ability to communicate with each other and exchange the data they gather. In this way, large amounts of data can be collected. Comprehensive processing and analysis of these data (e.g., in a powerful cloud backend) makes it possible to draw conclusions about the context in which an IoT device is used and generate knowledge about the data subjects. This gained knowledge represents the foundation of any smart service, not only in the private sector but also in the public and industrial sectors, such as in the smart home, eHealth, and Industry 4.0 domains.

This renders data as one of the most valuable assets in the information age. Therefore, it is important to manage data securely. Blockchain technologies are often applied to this end, as they ensure the immutability and tamper-resistance of data when they have to be exchanged between multiple parties that do not entirely trust each other. In additions to these information security measures, such highly sensitive data also pose great challenges with respect to data privacy. Applicable data protection laws, such as the EU's General Data Protection Regulation (GDPR), therefore demand the development and application of technical mechanisms that ensure the protection of any natural person when processing their data. In order to ensure that such protective measures are effective, however, they must be tailored to the IoT and blockchain technologies. In this regard, it must be investigated, e.g., how lightweight and privacy-preserving authentication in the IoT is possible; which trust-building approaches regarding the genuineness and validity of IoT data can be applied; and how blockchain systems can efficiently manage big data.

These and related research questions regarding security and privacy in blockchains and the IoT are addressed by six research articles and two literature reviews in this Special Issue. In the following, these eight papers are briefly outlined.

Articles. Two of the research articles address the question of how security and trust in IoT environments and IoT applications can be increased. Alzahrani and Fotiou [1] address how one-to-many communication—or group communication—can be made more secure in software-defined networking (SDN). SDN enables the self-organization of IoT groups by the IoT devices, which reflects the original IoT vision of a network of autonomous things. However, this poses the risk that such an SDN is flooded with fake messages and instructions from malicious things. To counteract this, the authors present an approach in which only authorized endpoints can send instructions to the network. Linked data signatures are used to prove the validity of the instructions. By means of linked data proofs, the presented approach supports zero-knowledge proofs to reliably secure IoT

check for updates

Citation: Stach, C. Special Issue on Security and Privacy in Blockchains and the IoT. *Future Internet* **2022**, *14*, 317. https://doi.org/10.3390/fi14110317

Received: 27 October 2022
Accepted: 28 October 2022
Published: 1 November 2022

group communications against malicious things. Wei et al. [2] present a different approach to increasing trust in IoT applications. They look at the Social Internet of Things (SIoT), in which smart devices autonomously establish social connections with each other. In this way, whenever necessary, things can become service requesters or service providers on their own, without the need for any human intervention. It is obvious that—similar to real-world services—trust in the service provider is required, e.g., whether it is able to provide the advertised services. While there are approaches that can adequately model this kind of trust in SIoT, these state-of-the-art approaches completely ignore the fact that a service provider has to trust a service requester as well. This work therefore focuses on modeling bidirectional trust in SIoT. This kind of modeling introduces additional complexity due to the fact that trust is context-dependent and can vary depending on the given situation. Based on their bidirectional trust model, the authors discuss a trust-based service delegation method in SIoT, which considers not only the level of trust between a service requester and a service provider but also the utility of the offered service.

Two of the research articles are dedicated to blockchain technologies. While blockchain systems enable secure data management in terms of immutability and tamper resistance, they typically lack comprehensive query capabilities. Przytarski et al. [3] therefore review the current state of query processing in blockchain systems and the future challenges in this research area. For this purpose, they initially investigate in which application domains blockchain technologies are used as part of big data management systems. Based on this, they determine which types of data and which data models are primarily used in this context. They then study the query capabilities of today's blockchain systems and discuss to what extent they meet the requirements of the use cases from the application domains. Furthermore, they give an outlook on how the internal data structures as well as the block structures of a blockchain system have to be adapted in order to efficiently support complex queries, such as history queries over time series data. Qu et al. [4] address another inherent problem in blockchain systems. As the blockchain uses a distributed ledger as its underlying infrastructure, i.e., a replicated, shared, and synchronized data store whose instances are managed by multiple parties, all involved parties have to agree on what data should be added to the blockchain. To synchronize changes, consensus methods such as proof of work (PoW) are used. A major disadvantage of PoW, however, is that it is very computation-intensive and therefore favors parties that have access to powerful computing capacities. In order to provide more fairness in the case of heterogeneous parties, e.g., in IoT environments, the authors interpose edge devices that monitor each computing node participating in PoW. This monitoring is based on a digital twin approach that simulates the normally expected behavior of each computing node. As a result, misbehavior by dishonest participants can be detected, e.g., computing nodes that use extra computing power to outperform their competitors. By means of a proof-of-concept implementation, the authors demonstrate not only the feasibility but also the efficiency of their approach.

The remaining two research articles focus on how blockchain technologies can be applied in the IoT to ensure privacy aspects, namely, access control and privacy-aware data sharing. While IoT applications typically rely on a central data backend that is responsible for the management of the collected data, such an approach poses a risk from a security perspective. Since a single entity operates this backend and thus has full control over the data, tampering is easily possible. Blockchain-based solutions, which manage the data in a distributed manner and are jointly operated by multiple parties, overcome this problem. However, they cause major privacy concerns, as an access policy for confidential data must be reliably applied to all data nodes involved. Khanal et al. [5] therefore introduce a two-pronged approach by which access to sensitive IoT data can only take place with the consent of the data subject. This approach uses a combination of a secure hash function and a key derivation function to encrypt the data. The data in the blockchain can only be decrypted if the data subject has given their consent. With their approach, the authors not only improve reliability but also reduce the computation time compared to state-of-the-art approaches. Gangwani et al. [6] also present an approach with which confidential IoT data can be trustworthily shared among multiple parties using distributed ledger technology. However, their approach relies on IOTA, a distributed-ledger-based communication protocol specifically tailored to the requirements of the IoT. Unlike blockchain-based approaches, IOTA is highly scalable, as restrictions on block size or mining costs are not an issue. As a result, it can also be used to share large amounts of sensor data at a rapid rate. The masked authenticated messaging (MAM) extension for IOTA is used to ensure confidentiality. With MAM, data streams can be sent encrypted as transactions with zero additional cost. Furthermore, MAM provides data subjects with fine-grained access control, allowing them to revoke access to their data at any given time. The authors demonstrate the high potential of IOTA and MAM when dealing with sensitive IoT data by means of an environmental monitoring application.

Reviews. Two literature reviews on in-app activity recognition based on encrypted traffic flow segments and on application areas for blockchain technologies in ambient assisted living wrap up this Special Issue. As the adoption of IoT technologies across all areas of life becomes more and more prevalent, not only the extent of data collection but also the network traffic increases. This is due to the fact that IoT applications do not carry out data processing on the IoT devices themselves, but in a powerful backend. As a result, these applications have to send their data to the backend on a continuous basis. Typically, this data stream is encrypted to ensure that third parties do not gain insight into the transferred payload data. However, even encrypted traffic flow segments still allow conclusions to be drawn about in-app activities, which compromises the privacy of the user. In their review, Pathmaperuma et al. [7] therefore investigate which types of traffic classification exist in the literature. Essentially, there are statistical methods and approaches based on neural networks. In addition to this literature review, the authors also propose their own approach to user activity detection based on in-app data. To this end, they apply an image-based method. Instead of analyzing the network traffic itself, they transform the detected patterns into images, where each pixel stands for features and corresponding feature values of the traffic data. For eight popular mobile applications (e.g., Facebook, Instagram, and WhatsApp), the authors record the network traffic generated by typical in-app activities (e.g., post an image, like an image, and send a short text message). These samples are cleansed, pre-processed, and transformed, resulting in a comprehensive database with characteristic images for each of the in-app activities. A convolutional neural network (CNN) is trained with this image database. The CNN is able to classify activities based on their network traffics with an accuracy of 88 % to 92 %.

One sector that benefits significantly from the IoT and the accompanying comprehensive data collection is the healthcare sector. In particular, recurring routine medical checkups, for instance, in the case of chronic diseases, can be carried out remotely, thus relieving both patients and physicians. As a result of the COVID-19 pandemic, there are increased demands to provide assisted care services remotely. Ambient assisted living (AAL) uses IoT technologies to provide non-intrusive support for the daily lives of elderly or disabled people without the need for a caregiver on site. Since the monitoring required for this purpose collects a large amount of highly personal data, there are justified security and privacy concerns regarding data management. The strategic use of blockchain technologies has the potential to alleviate these concerns. Florea et al. [8] therefore conduct a systematic literature review which aims to identify fields of application for blockchain technologies in the AAL and to highlight advantages and open issues in this context. For this purpose, they selected a literature corpus of 472 scientific papers published in high-quality conferences and journals. In a systematic approach following the PRISM process flow, they condensed this overall corpus to the most relevant papers. Based on these 87 core papers, the authors identify three AAL use cases for which the use of blockchain technologies generates a significant added value. These use cases, which are also further detailed in the review, are IoT-based monitoring and intervention, decentralized patient data management, and AAL system security and privacy. Despite the undeniable benefits that blockchain technologies can provide in these areas, the authors also identify some obstacles that need to be addressed in further research. For instance, there is a need to reduce the transactional and storage costs inherent in managing large amounts of data in blockchain systems, to facilitate the integration of blockchain systems into legacy infrastructures prevalent in many AAL environments, and to ensure the privacy of data managed by a blockchain system.

The eight excellent papers in this Special Issue provide a good overview of security and privacy issues in blockchain systems and the IoT. The research articles present practical solutions to some of these issues. While the literature reviews reveal that there are still several security and privacy issues that need to be addressed in the future, they also show that the use of blockchain technologies and the IoT is beneficial to the daily lives of all of us. It is therefore important to address the questions raised in this Special Issue in the future, in order to make the usage of IoT technologies and blockchain systems as secure and privacy aware as possible.

I would like to thank all the authors for submitting their interesting and informative manuscripts to this Special Issue. I would also like to acknowledge all the reviewers whose thorough and substantial reviews further improved the quality of the manuscripts and without whom this Special Issue would not have been possible. Last but not least, I would like to thank the MDPI editorial team whose support has been instrumental in my work on this Special Issue.

Funding: This research received no external funding.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Alzahrani, B.; Fotiou, N. Securing SDN-Based IoT Group Communication. *Future Internet* **2021**, *13*, 207. [CrossRef]
2. Wei, L.; Yang, Y.; Wu, J.; Long, C.; Lin, Y.B. A Bidirectional Trust Model for Service Delegation in Social Internet of Things. *Future Internet* **2022**, *14*, 135. [CrossRef]
3. Przytarski, D.; Stach, C.; Gritti, C.; Mitschang, B. Query Processing in Blockchain Systems: Current State and Future Challenges. *Future Internet* **2022**, *14*, 1. [CrossRef]
4. Qu, Q.; Xu, R.; Chen, Y.; Blasch, E.; Aved, A. Enable Fair Proof-of-Work (PoW) Consensus for Blockchains in IoT by Miner Twins (MinT). *Future Internet* **2021**, *13*, 291. [CrossRef]
5. Khanal, Y.P.; Alsadoon, A.; Shahzad, K.; Al-Khalil, A.B.; Prasad, P.W.C.; Rehman, S.U.; Islam, R. Utilizing Blockchain for IoT Privacy through Enhanced ECIES with Secure Hash Function. *Future Internet* **2022**, *14*, 77. [CrossRef]
6. Gangwani, P.; Perez-Pons, A.; Bhardwaj, T.; Upadhyay, H.; Joshi, S.; Lagos, L. Securing Environmental IoT Data Using Masked Authentication Messaging Protocol in a DAG-Based Blockchain: IOTA Tangle. *Future Internet* **2021**, *13*, 312. [CrossRef]
7. Pathmaperuma, M.H.; Rahulamathavan, Y.; Dogan, S.; Kondoz, A. CNN for User Activity Detection Using Encrypted In-App Mobile Data. *Future Internet* **2022**, *14*, 67. [CrossRef]
8. Florea, A.I.; Anghel, I.; Cioara, T. A Review of Blockchain Technology Applications in Ambient Assisted Living. *Future Internet* **2022**, *14*, 150. [CrossRef]