*future internet*

MDPI

*Editorial*

# Special Issue on Security and Privacy in Blockchains and the IoT—3rd Edition

**Christoph Stach [1,*], Clémentine Gritti [2,*] and Iouliana Litou [3,*]**

[1] Institute for Parallel and Distributed Systems, University of Stuttgart, Universitätsstraße 38, 70569 Stuttgart, Germany
[2] CITI Lab, INSA Lyon, Building Hedy Lamarr, 6 Avenue des Art, 69100 Villeurbanne, France
[3] Department of Informatics, Athens University of Economics and Business, Patision 76, 104 34 Athens, Greece
* Correspondence: christoph.stach@ipvs.uni-stuttgart.de (C.S.); clementine.gritti@insa-lyon.fr (C.G.); litou@aueb.gr (I.L.); Tel.: +49-711-68588-433 (C.S.)

The rapid digital transformation of modern society is increasingly driven by the convergence of blockchain technologies and the Internet of Things (IoT), both of which have become foundational pillars of contemporary distributed systems. Blockchain introduces decentralized trust, immutability, and transparency, while IoT enables pervasive sensing, automation, and data-driven decision-making across domains such as healthcare, industry, energy, transportation, and smart cities. Collectively, these technologies promise to reshape digital infrastructures by eliminating single points of failure, improving operational efficiency, and enabling new forms of collaboration among heterogeneous and autonomous entities. However, this convergence also substantially enlarges the attack surface and introduces complex security and privacy challenges that cannot be adequately addressed by traditional centralized protection mechanisms.

IoT environments are inherently heterogeneous, resource-constrained, and often deployed in safety-critical contexts, making them particularly vulnerable to cyber attacks, data manipulation, and unauthorized access. At the same time, blockchain systems, despite their cryptographic foundations, face a wide range of threats including protocol-level attacks, smart contract vulnerabilities, privacy leakage, and emerging risks associated with scalability and quantum computing. The interaction between these two paradigms further amplifies such challenges, as weaknesses in one layer can cascade across the entire system. Ensuring confidentiality, integrity, availability, and accountability in these interconnected ecosystems therefore remains a fundamental research problem.

Beyond purely technical considerations, trust has emerged as a central concept in blockchain- and IoT-based systems. Trust is required not only in the underlying protocols and infrastructures, but also in the data they collect, process, and share, as well as in the autonomous decisions derived from that data. Privacy concerns are equally critical, particularly when sensitive personal, industrial, or societal data are involved and when regulatory requirements such as data protection and accountability must be satisfied. Consequently, security and privacy can no longer be treated as isolated design goals, but must be addressed holistically and throughout the entire system lifecycle.

Against this backdrop, sustained research efforts are required to develop robust security mechanisms, privacy-preserving architectures, and trust-building strategies that are both theoretically sound and practically viable. This Special Issue is motivated by the need to bring together advances from academia and industry that address these challenges from complementary perspectives. By fostering interdisciplinary approaches and bridging foundational research with real-world applications, this Special Issue aims to contribute to the development of resilient, trustworthy, and future-proof blockchain and IoT ecosystems.



Received: 5 February 2026
Accepted: 5 February 2026
Published: 9 February 2026

Building upon the broad relevance of security, privacy, and trust in blockchain- and IoT-enabled systems, this Special Issue focuses on advancing the understanding and practical realization of these concepts in decentralized and data-intensive environments. The scope of this Special Issue reflects the increasing maturity of blockchain and IoT technologies, as well as their growing adoption in real-world, security-critical domains. Rather than treating both paradigms in isolation, this Special Issue emphasizes their combined deployment and the resulting security, privacy, and trust implications across different system layers.

The contributions collected in this volume address security and privacy challenges ranging from foundational analyses to concrete architectural solutions and applied systems. Several papers investigate vulnerabilities, attack surfaces, and mitigation strategies in blockchain and IoT ecosystems, providing structured taxonomies and systematic perspectives on current threats. Others focus on mechanisms that support secure authentication, access control, and key management as integral components of distributed architectures, particularly in heterogeneous and resource-constrained environments.

A central theme of this Special Issue is the protection of data throughout its lifecycle, including privacy-preserving data collection, secure storage, verifiable deletion, and trustworthy sharing across organizational boundaries. In this context, blockchain-based mechanisms for ensuring data integrity, auditability, and non-repudiation play a prominent role. The design and analysis of smart contracts, consensus mechanisms, and off-chain storage strategies are examined with respect to both security guarantees and operational efficiency.

Threat detection and resilience constitute another major focus of this Special Issue. Several contributions explore advanced detection mechanisms based on anomaly detection, graph-based learning, explainable artificial intelligence, and federated learning. These approaches address both technical attacks on infrastructures and human-centric vulnerabilities, highlighting the multifaceted nature of security and trust in decentralized systems. Scalability and performance considerations are explicitly taken into account, reflecting the requirements of large-scale IoT deployments, industrial systems, and next-generation network environments.

In addition to technical mechanisms, this Special Issue includes applied studies and system-oriented frameworks that demonstrate how blockchain-based security solutions can be integrated into domains such as healthcare, digital forensics, smart grids, and enterprise networks. These works implicitly address regulatory, legal, and compliance-related concerns by supporting transparency, traceability, and evidentiary integrity in sensitive application contexts. Through this carefully aligned scope and set of topics, this Special Issue presents a coherent collection of contributions that collectively advance the state of the art while remaining grounded in practical and deployable security and privacy solutions.

The inaugural two volumes of this Special Issue (see Stach [1] and Stach and Gritti [2]) established a solid foundation by addressing core security and privacy challenges in blockchain- and IoT-based systems, with a strong emphasis on data protection, secure data management, and compliance with regulatory requirements. While the first volume primarily focused on privacy-preserving mechanisms, lightweight authentication, and legal considerations in emerging IoT scenarios, the second volume broadened this perspective by offering a holistic view on end-to-end data flows and fundamental security properties such as authenticity, confidentiality, and integrity. Building on these contributions, this third volume shifts the focus toward the increasingly critical notion of trust and its interplay with security and privacy in decentralized and intelligent systems. In contrast to earlier volumes, this edition places greater emphasis on advanced threat models, trust-aware architectures, and data-driven detection mechanisms that reflect the growing complexity of modern blockchain and IoT deployments. Furthermore, emerging technologies such as artificial intelligence, federated learning, quantum-aware security concepts, and large-scale

https://doi.org/10.3390/fi18020090

industrial infrastructures receive increased attention. The current volume also strengthens the link between foundational research and real-world deployment by presenting system-oriented solutions and applied studies in domains such as healthcare, digital forensics, smart grids, and enterprise networks. In this way, this third edition complements and extends the previous volumes by addressing both the maturity of the technologies and the evolving security, privacy, and trust requirements of next-generation distributed systems.

This volume of the Special Issue comprises twelve high-quality contributions that address the overarching theme of security and privacy in blockchain and IoT systems from a wide range of methodological and application-oriented perspectives. Collectively, these papers reflect the diversity and maturity of current research, spanning foundational analyses, advanced security mechanisms, and domain-specific system implementations. For clarity and coherence, the contributions are organized into three thematic blocks, which are outlined in the following paragraphs.

Foundations, Threats, and Privacy Challenges in Blockchain and IoT Ecosystems.

The first thematic block lays the conceptual and analytical foundations of this Special Issue by examining fundamental security, privacy, and trust challenges in blockchain and IoT ecosystems. It brings together comprehensive reviews and surveys that systematically analyze vulnerabilities, attack surfaces, and emerging trends across decentralized systems. By structuring the problem space and identifying persistent research challenges, this block establishes a shared understanding that informs the more solution-oriented contributions that follow.

The paper by Siam et al. [3] provides a comprehensive systematic review of blockchain vulnerabilities, attacks, and mitigation strategies, offering a broad and structured entry point into the security landscape of decentralized ecosystems. Following PRISMA guidelines, the study synthesizes the recent literature to categorize attacks across multiple domains, including network, consensus, smart contracts, transactions, and governance. The authors not only identify dominant threat vectors such as smart contract vulnerabilities and consensus manipulation, but also analyze their underlying causes and real-world implications. By mapping attacks to corresponding countermeasures, the paper highlights gaps between theoretical defenses and practical deployment. Special attention is given to context-specific mitigation strategies for domains such as finance, healthcare, and IoT. The discussion of trade-offs between decentralization, scalability, and security further emphasizes the complexity of secure blockchain design. As such, this work provides a structured baseline for understanding the evolving threat landscape addressed by subsequent contributions.

Complementing this broad perspective, Islam et al. [4] present a layer-oriented survey that decomposes blockchain systems into data, network, consensus, contract, and application layers. This architectural viewpoint enables a more fine-grained analysis of how vulnerabilities manifest at different system levels and how attacks propagate across layers. The paper introduces a detailed taxonomy of detection and mitigation approaches, including formal verification, static and dynamic analysis, and machine learning-based techniques. By systematically linking specific threats to detection methods, the authors provide practical guidance for security tool selection and system hardening. The survey also highlights emerging challenges such as adversarial machine learning and the lack of labeled datasets for intelligent detection. The inclusion of post-quantum threats and explainability considerations extends the relevance of the analysis beyond current-generation systems. This layered perspective deepens the foundational understanding introduced in the preceding paper.

https://doi.org/10.3390/fi18020090

Shifting the focus toward the convergence of blockchain and IoT, Kareem et al. [5] survey emerging blockchain platforms that are explicitly adopted to enhance IoT security. The paper analyzes and compares platforms such as Ethereum, Hyperledger Fabric, IOTA, IoTeX, Algorand, and Multichain with respect to their suitability for resource-constrained environments. By examining consensus mechanisms, cryptographic primitives, and architectural design choices, the study clarifies how blockchain components contribute to IoT security requirements. The authors emphasize the role of permissioned architectures, interoperability, and lightweight cryptography in achieving practical deployments. Scalability limitations and performance bottlenecks are discussed alongside potential optimization strategies. The survey serves as a bridge between abstract security challenges and concrete platform-level design decisions. In doing so, it prepares the study area for the more mechanism-focused and applied contributions in later blocks.

Concluding the first thematic block, Bayan et al. [6] investigate recent trends and privacy concerns in permissionless blockchains within the rapidly evolving Web3 ecosystem. The paper identifies how developments such as high-throughput networks and real-world asset tokenization reshape the security and privacy threat landscape. A systematic analysis of privacy threats, including deanonymization, MEV exploitation, and key compromise, highlights the persistent tension between transparency and confidentiality. The authors critically assess privacy-enhancing technologies such as zero-knowledge proofs, ring signatures, and stealth addresses, discussing their trade-offs in scalability and usability. A notable contribution is the introduction of a secure development lifecycle tailored to decentralized applications, emphasizing security-by-design principles. By grounding the discussion in recent real-world incidents, the paper connects abstract privacy risks to concrete development practices. This forward-looking perspective provides a natural transition from foundational analysis to the design of effective countermeasures.

Threat Detection, Trust, and Intelligent Security Mechanisms.

The second thematic block focuses on concrete mechanisms for detecting threats, establishing trust, and enhancing resilience in blockchain and IoT systems. A unifying theme of this block is the use of data-driven and intelligent techniques to cope with increasingly sophisticated attack scenarios. Together, the contributions demonstrate how advanced analytics, machine learning, and trust modeling can complement traditional security mechanisms.

Pérez-Cano and Jurado [7] investigate fraud detection in cryptocurrency networks through a comparative analysis of unsupervised anomaly detection and supervised graph-based learning. Using large-scale real-world Bitcoin datasets, the study evaluates the effectiveness of classical anomaly detection algorithms and highlights their limitations when structural information is ignored. The introduction of heterogeneous graph transformers enables the exploitation of relational dependencies between transactions and wallets. The paper demonstrates that incorporating graph structure significantly improves fraud detection performance under severe class imbalance. By comparing supervised and unsupervised approaches within a unified framework, the study provides valuable insights into their respective strengths and limitations. The findings underscore the importance of combining intrinsic transaction features with network-level information. This work establishes a strong analytical foundation for intelligent detection mechanisms in decentralized financial systems.

Extending the detection perspective to IoT environments, Lightbody et al. [8] introduce Dragon_Pi, a novel dataset based on side-channel power consumption signals from IoT devices. The paper proposes an unsupervised convolutional autoencoder to detect anomalies without relying on labeled attack data. By focusing on physical power traces rather than

network traffic, the approach captures post-exploitation behavior that is often invisible to traditional monitoring tools. The cross-platform design demonstrates robustness across heterogeneous hardware architectures. The experimental results show that reconstruction error-based detection achieves a strong performance, particularly when combined with signal post-processing. The public release of the dataset addresses a critical gap in IoT security research. This contribution highlights the value of alternative data modalities for resilient intrusion detection.

Addressing the human dimension of security, Fan et al. [9] analyze phishing susceptibility using explainable artificial intelligence. The paper proposes a deep learning model augmented with SHAP-based explanations to identify individual risk factors influencing phishing behavior. By integrating behavioral habits, psychological traits, and demographic information, the study moves beyond population-level analysis toward personalized risk assessment. The use of explainable AI enables the transparent interpretation of model predictions, making the results actionable for security awareness and training. The findings reveal that behavioral factors often outweigh demographic characteristics in determining susceptibility. This human-centric perspective complements system-level detection approaches by addressing social engineering threats. The work demonstrates how trust and security depend not only on technical mechanisms but also on user behavior.

Concluding this block, Alharbi [10] presents a forward-looking framework that integrates blockchain, federated learning, and quantum-inspired trust modeling for industrial IoT in 6G environments. The proposed architecture introduces a quantum trust score to dynamically assess device reliability under Byzantine and poisoning attacks. Blockchain-based sharding ensures the scalable and immutable recording of trust updates. The experimental results demonstrate strong resilience and a high detection accuracy under adversarial conditions. The integration of explainability mechanisms further supports operational transparency. By addressing both current and future threat models, including quantum-era challenges, this work represents a culmination of the intelligent and trust-aware approaches discussed in this block. It also forms a conceptual bridge toward applied, large-scale system deployments.

Secure Blockchain-Based Architectures and Domain-Specific Applications.

The third thematic block emphasizes system-oriented solutions and real-world applications that demonstrate the practical maturity of blockchain-based security mechanisms. The common thread of this block is the translation of security, privacy, and trust concepts into deployable architectures across diverse domains. These contributions illustrate how theoretical principles can be operationalized under real-world constraints.

Aref and Ouda [11] introduce HSM4SSL, a hardware-backed architecture for securing intra-domain communications using hardware security modules. The proposed system unifies certificate management and cryptographic operations across multiple protocols through a modular SaaS design. Performance evaluations demonstrate improvements over conventional software-based solutions in terms of throughput and latency. The abstraction of vendor-specific HSM interfaces enhances flexibility and scalability. Automated certificate lifecycle management reduces operational complexity and human error. By focusing on enterprise-grade deployment, the paper addresses practical security challenges often overlooked in academic research. This contribution establishes a strong architectural foundation for secure system integration.

Focusing on healthcare emergency response systems, Marletta et al. [12] propose a blockchain-based framework for certifying timestamps and ensuring data integrity. By storing cryptographic hashes of critical events on an EVM-compatible blockchain, the system provides immutable and verifiable proof of data authenticity. Off-chain storage strategies

ensure scalability and privacy preservation, and experimental evaluations using real-world datasets demonstrate economic feasibility and reliable transaction confirmation times. The framework supports independent verification in dispute scenarios, strengthening trust among stakeholders. This work exemplifies how blockchain can replace centralized trusted third parties in high-stakes environments, highlighting the role of trust and non-repudiation in safety-critical applications.

In the context of digital forensics, Huang et al. [13] present a blockchain-based framework for OSINT evidence collection and identification. The proposed lifecycle model aligns technical processes with legal standards for evidence admissibility. On-acquisition notarization using a permissioned judicial blockchain ensures integrity and chain of custody. The integration of identity correlation mechanisms addresses attribution challenges in online investigations. AI-assisted tools further enhance evidence quality and reliability. By bridging forensic rigor with decentralized technologies, the framework strengthens trust in digital evidence. This contribution underscores the legal and societal relevance of blockchain-based security solutions.

Concluding this Special Issue, Zhang et al. [14] introduce MCS-VD, an alliance chain-driven multi-cloud storage and verifiable deletion scheme for smart grid data. The framework combines efficient consensus protocols with encrypted multi-cloud storage to address scalability and single-point-of-failure concerns. A dedicated deletion mechanism enables verifiable and permanent data removal, supporting regulatory compliance. The experimental results demonstrate significant performance gains over traditional Byzantine fault-tolerant protocols. The hierarchical design supports large-scale deployment in industrial environments. By addressing the full data lifecycle from collection to deletion, this work provides a comprehensive solution for critical infrastructure security. It offers a strong concluding perspective on the practical realization of secure, privacy-preserving, and trustworthy blockchain–IoT systems.

The twelve papers in this Special Issue offer a comprehensive and multifaceted view of current advances in security, privacy, and trust for blockchain and IoT ecosystems. By combining foundational analyses, intelligent detection mechanisms, and domain-specific system implementations, this Special Issue offers readers a coherent perspective on both the theoretical and practical dimensions of the field. The included survey and review articles establish a structured understanding of threat landscapes, architectural vulnerabilities, and emerging privacy challenges, serving as valuable reference points for researchers entering or extending work in this domain. At the same time, the methodological contributions demonstrate how advanced techniques such as machine learning, graph-based analytics, explainable artificial intelligence, and federated learning can be effectively leveraged to address real-world security threats.

A distinguishing feature of this Special Issue is its balanced integration of technical rigor and practical relevance. Several contributions move beyond conceptual proposals by providing experimentally validated systems, publicly available datasets, and performance evaluations under realistic conditions. This enables practitioners to assess the feasibility and trade-offs of proposed solutions, while offering researchers reproducible foundations for future studies. The strong emphasis on trust, accountability, and data integrity reflects the growing importance of these concepts in decentralized and autonomous systems, particularly in safety-critical and regulated environments.

Furthermore, the diversity of application domains, including healthcare, digital forensics, smart grids, industrial IoT, and enterprise networks, illustrates the broad applicability of blockchain-based security and privacy mechanisms. Readers benefit from insights into how common principles can be adapted to domain-specific constraints and requirements. The Special Issue also highlights emerging trends such as quantum-aware security, side-

channel-based intrusion detection, and privacy-aware development lifecycles, signaling important directions for future research and innovation.

By bringing together contributions from both academia and industry, this Special Issue fosters cross-disciplinary exchange and knowledge transfer. It provides a curated snapshot of the state of the art while simultaneously outlining practical pathways toward more resilient and trustworthy digital infrastructures. As such, this Special Issue is intended not only as a collection of individual research outcomes, but as a cohesive resource that informs, inspires, and supports the ongoing evolution of secure and privacy-preserving blockchain and IoT systems.

Despite the significant progress reflected in this Special Issue, securing blockchain and IoT ecosystems remains an ongoing challenge as these technologies continue to evolve and scale. Open research directions include achieving stronger security and privacy guarantees without compromising scalability, addressing emerging threats driven by artificial intelligence and quantum computing, and developing standardized benchmarks for evaluating trust-aware systems. Furthermore, the integration of human-centric factors, regulatory requirements, and explainable security mechanisms will become increasingly important for real-world adoption. Continued collaboration between academia, industry, and policymakers will therefore be essential to ensure that future decentralized systems are not only technically robust, but also trustworthy and socially acceptable.

As the Guest Editors, we would like to sincerely thank all authors for submitting their high-quality and insightful manuscripts to our Special Issue. Their contributions form the intellectual foundation of this volume and reflect the diversity, rigor, and relevance of current research in this rapidly evolving field. We are also deeply grateful to the reviewers for their careful, constructive, and timely evaluations, which were instrumental to enhancing the scientific quality and clarity of the accepted papers. Their expertise and dedication have been essential to maintaining the high standards of this Special Issue. Finally, we would like to express our sincere appreciation to the MDPI editorial team for their continuous support and efficient coordination throughout the entire editorial process, without which the successful completion of this Special Issue would not have been possible.

**Author Contributions:** All authors have read and agreed to the published version of the manuscript.

**Conflicts of Interest:** The authors declare no conflicts of interest.

## References

1. Stach, C. (Ed.) *Security and Privacy in Blockchains and the IoT*; MDPI: Basel, Switzerland, 2023. [CrossRef]
2. Stach, C.; Gritti, C. (Eds.) *Security and Privacy in Blockchains and the IoT II*; MDPI: Basel, Switzerland, 2023. [CrossRef]
3. Siam, M.K.; Saha, B.; Hasan, M.M.; Hossain Faruk, M.J.; Anjum, N.; Tahora, S.; Siddika, A.; Shahriar, H. Securing Decentralized Ecosystems: A Comprehensive Systematic Review of Blockchain Vulnerabilities, Attacks, and Countermeasures and Mitigation Strategies. *Future Internet* **2025**, *17*, 183. [CrossRef]
4. Islam, M.J.; Islam, S.; Hossain, M.; Noor, S.; Islam, S.M.R. Securing Blockchain Systems: A Layer-Oriented Survey of Threats, Vulnerability Taxonomy, and Detection Methods. *Future Internet* **2025**, *17*, 205. [CrossRef]
5. Kareem, Y.; Djenouri, D.; Ghadafi, E. A Survey on Emerging Blockchain Technology Platforms for Securing the Internet of Things. *Future Internet* **2024**, *16*, 285. [CrossRef]
6. Bayan, T.; Yazici, A.; Banach, R. Permissionless Blockchain Recent Trends, Privacy Concerns, Potential Solutions and Secure Development Lifecycle. *Future Internet* **2025**, *17*, 547. [CrossRef]
7. Pérez-Cano, V.; Jurado, F. Fraud Detection in Cryptocurrency Networks—An Exploration Using Anomaly Detection and Heterogeneous Graph Transformers. *Future Internet* **2025**, *17*, 44. [CrossRef]
8. Lightbody, D.; Ngo, D.M.; Temko, A.; Murphy, C.C.; Popovici, E. Dragon_Pi: IoT Side-Channel Power Data Intrusion Detection Dataset and Unsupervised Convolutional Autoencoder for Intrusion Detection. *Future Internet* **2024**, *16*, 88. [CrossRef]
9. Fan, Z.; Li, W.; Laskey, K.B.; Chang, K.C. Investigation of Phishing Susceptibility with Explainable Artificial Intelligence. *Future Internet* **2024**, *16*, 31. [CrossRef]

10. Alharbi, S. QuantumTrust-FedChain: A Blockchain-Aware Quantum-Tuned Federated Learning System for Cyber-Resilient Industrial IoT in 6G. *Future Internet* **2025**, *17*, 493. [CrossRef]
11. Aref, Y.; Ouda, A. HSM4SSL: Leveraging HSMs for Enhanced Intra-Domain Security. *Future Internet* **2024**, *16*, 148. [CrossRef]
12. Marletta, D.; Midolo, A.; Tramontana, E. A Blockchain-Based Strategy for Certifying Timestamps in a Distributed Healthcare Emergency Response Systems. *Future Internet* **2025**, *17*, 210. [CrossRef]
13. Huang, H.W.; Shih, C.H.; Li, C.Y.; Teng, H.Y. A Blockchain-Based Framework for OSINT Evidence Collection and Identification. *Future Internet* **2025**, *17*, 551. [CrossRef]
14. Zhang, L.; Luo, J.; Yang, Y.; Wang, W. MCS-VD: Alliance Chain-Driven Multi-Cloud Storage and Verifiable Deletion Scheme for Smart Grid Data. *Future Internet* **2026**, *18*, 56. [CrossRef]

## Short Biography of Authors

**Dr. Christoph Stach** holds the Substitute Chair of Data Engineering and heads the Information Systems and Applications working area at the Institute for Parallel and Distributed Systems at the University of Stuttgart. He received his doctorate in 2017, specializing in data security and privacy for mobile applications. His current research focuses on demand-oriented data management at the intersection of big data, data refinement, and data protection. An accomplished researcher with an h-index of 20, Dr. Stach has authored over 70 peer-reviewed publications on this topic. The practical relevance and economic impact of his research are further demonstrated by his leadership in successfully executing five large-scale industrial projects. His extensive service to the academic community includes participating in more than 50 international conference program committees. He serves as Guest Editor for this Special Issue to explore and leverage the synergies between decentralized data management and the security challenges inherent in modern IoT environments.

**Clémentine Gritti** received the M.Sc. degree in computer science from Grenoble Alpes University, France, in 2012, and the Ph.D. degree in computer science from the University of Wollongong, Australia, in 2017. She was a Senior Lecturer at the University of Canterbury, New Zealand, between 2020 and 2023. Thereafter, she was a research fellow at Eurecom, France. In 2024, she joined INSA Lyon, France, as a Professor Junior. Her current research interests include the design and evaluation of public-key cryptographic protocols for applied security and privacy in various contexts, such as Federated Learning, Internet of Things, and blockchain technologies.

**Iouliana Litou** is a computer scientist and researcher primarily focused on social networks, information dissemination, influence maximization, and misinformation analysis. She has pursued her academic career at the Athens University of Economics and Business (AUEB), Department of Informatics, where she completed her B.Sc. and M.Sc. degrees in Computer Science and later completed her Ph.D. in Computer Science under the supervision of Prof. Vana Kalogeraki. Her Ph.D. research centers on Participatory Sensing Systems and modeling information diffusion in online networks. Litou has been involved as a research assistant and software engineer in multiple research projects since 2011, contributing to areas such as real-time information propagation and emergency dissemination through online social platforms. She has co-authored various peer-reviewed publications in international conferences and journals.