

Web of Science™

1 record(s) printed from Clarivate Web of Science

Record 1 of 1

Title: Securing IoT edge: a survey on lightweight cryptography, anonymous routing and communication protocol enhancements

Author(s): Gusita, B (Gusita, Bianca); Anton, AA (Anton, Alin A.); Stângaciu, CS (Stangaciu, Cristina S.); Stanescu, D (Stanescu, Daniela); Gaina, LI (Gaina, Lucian I.); Micea, MV (Micea, Mihai V.)

Source: INTERNATIONAL JOURNAL OF INFORMATION SECURITY **Volume:** 24 **Issue:** 3 **Article Number:** 149 **DOI:** 10.1007/s10207-025-01071-7 **Published Date:** 2025 MAY 31

Times Cited in Web of Science Core Collection: 1

Total Times Cited: 2

Usage Count (Last 180 days): 5

Usage Count (Since 2013): 6

Cited Reference Count: 150

Abstract: In a technological landscape marked by the accelerated expansion of the Internet of Things (IoT), securing edge communications is becoming essential for ensuring trust, confidentiality and data integrity. The constant evolution of cyber attacks, combined with the resource limitations of IoT devices, requires the development of effective, adaptable and scalable security solutions. This paper provides a comprehensive review of recent advances and persistent challenges in securing edge communications in the IoT, with a focus on lightweight cryptographic algorithms (ASCON, PRESENT, SIMON, SPECK) and on authentication mechanisms adapted to resource-constrained devices. The trade-offs between performance and security are emphasized, besides the need for IoT-specific Anonymous Overlay Networks(AONs) and Anonymous Routing Protocols(ARPs) capable of providing protection against traffic analysis and user anonymity. The study includes a detailed classification of 18 ARPs protocols, along with a presentation of the metrics used in evaluation. It also exposes MQTT-SN protocol vulnerabilities and proposes the development of standardized security frameworks with built-in encryption and authentication for scalable IoT deployments. The main finding of the study highlights the need for further research in developing tailored security solutions for IoT devices, as well as enhancing the security of the MQTT-SN protocol.

Accession Number: WOS:001499232900001

Language: English

Document Type: Article

Author Keywords: IoT Edge Communication Security; Lightweight Cryptographic Algorithms; Resource-Constrained Devices; Anonymous Overlay Networks; Anonymous Routing Protocols; Evaluation Metrics; Privacy and Anonymity in IoT; Security Vulnerabilities in MQTT-SN

KeyWords Plus: OVERLAY NETWORKS; INTERNET; ARCHITECTURE; UNIFICATION; EFFICIENT; ATTACKS; TOR; GR

Addresses: [Gusita, Bianca; Anton, Alin A.; Stangaciu, Cristina S.; Stanescu, Daniela; Gaina, Lucian I.; Micea, Mihai V.] Politehn Univ Timisoara, Dept Comp & Informat Technol, 2 Vasile Parvan Bvd, Timisoara, Romania.

Corresponding Address: Gusita, B (corresponding author), Politehn Univ Timisoara, Dept Comp & Informat Technol, 2 Vasile Parvan Bvd, Timisoara, Romania.

E-mail Addresses: bianca.gusita@cs.upt.ro; alin.anton@cs.upt.ro; cristina.stangaciu@cs.upt.ro; daniela.stanescu@cs.upt.ro; lucian.gaina@cs.upt.ro; mihai.micea@cs.upt.ro

Affiliations: Universitatea Politehnica Timisoara

Author Identifiers:

Author	Web of Science ResearcherID	ORCID Number
GUSITA, Bianca	KAM-7355-2024	0009-0009-3603-2286
Stangaciu, Cristina	AAX-6452-2020	
Micea, Mihai	B-5581-2011	
Anton, Alin	ABA-3452-2021	

Publisher: SPRINGER

Publisher Address: ONE NEW YORK PLAZA, SUITE 4600, NEW YORK, NY, UNITED STATES

Web of Science Index: Science Citation Index Expanded (SCI-EXPANDED)

Web of Science Categories: Computer Science, Information Systems; Computer Science, Software Engineering; Computer Science, Theory & Methods

Research Areas: Computer Science

IDS Number: 3FR6U

ISSN: 1615-5262

eISSN: 1615-5270

29-char Source Abbrev.: INT J INF SECUR

ISO Source Abbrev.: Int. J. Inf. Secur.

Source Item Page Count: 36

Open Access: hybrid

Output Date: 2026-01-31

End of File

 Clarivate