УДК 004.738.5:004.75

RESEARCH ON SECURE DATA STORAGE ARCHITECTURE FOR EDGE DEVICES

Xin Song[1], *V.M. Savchenko*[2]

[1] *Master's student, CEP dept., NTU "KhPI", Kharkiv, Ukraine*
[2] *Associate Professor, CEP dept., Cand. Sc. (Engineering), NTU "KhPI", Kharkiv, Ukraine*
xin.song@cs.khpi.edu.ua

Edge computing is an integral component of cloud computing technologies. The migration of computations from a centralized server to edge devices offers the following advantages:

- a significant reduction in latency, enabling operation in near real-time modes;
- reduced network traffic due to preliminary data processing on edge devices before transmission to the cloud server;
- improved system reliability, since edge nodes can continue functioning under unstable network conditions or during disconnections from the central cloud environment;
- optimization of costs, scalability, and architectural flexibility, as well as compliance with local data storage and processing standards.

Given the widespread adoption of such architectures, security assurance within edge systems has become a pressing issue that requires a comprehensive investigation of hardware, software, and organizational aspects, taking into account the continuous evolution of cloud computing technologies.

The objective of this study is to examine security challenges inherent in architectures incorporating edge computing. The paper analyzes current issues in edge-computing security and their impact on architectural design decisions. The main challenges highlighted in recent research include [1-5]:

- physical access to devices, which are often deployed in open or uncontrolled environments;
- limited computational capabilities, resulting in lightweight cryptographic implementations and difficulties in delivering and installing security updates;
- potential software compromise through exploitation of known and zero-day vulnerabilities;
- lack of centralized control, integrity violations, the need for prolonged autonomous operation and local data storage during network outages, possible compromise of cryptographic keys, and generally restricted security resources;
- supply-chain attacks, which threaten firmware and hardware integrity at various production stages.

Thus, to ensure trust and information protection at the edge, it is essential to design a multi-layered security architecture that integrates hardware-based, software-based, and cryptographic mechanisms.

At the hardware layer, the architecture must incorporate a component ensuring software authenticity and integrity, commonly referred to as the Hardware Root of Trust (HRoT). Widely adopted technologies include TPM 2.0 (Trusted Platform Module), ARM TrustZone / OP-TEE, and DICE (Device Identity Composition Engine). The use of a hardware root of trust is fundamental to the operation of all subsequent security mechanisms in edge-computing environments.

Cryptographic protection of data on edge devices depends largely on the available computational resources. In many cases, it is objectively impossible to employ standard, widely accepted encryption algorithms due to hardware limitations and energy constraints.

Among the commonly used approaches are:

• Full-disk encryption (FDE) of storage media (e.g., flash memory) using LUKS2 / dm-crypt, with decryption keys managed through TPM or TrustZone;

• File-based encryption (fscrypt) for granular data protection at the file-system level;

• Self-encrypting drives (SED) compliant with the TCG Opal standard, which perform hardware-level encryption and allow rapid cryptographic erasure through key invalidation.

This group of mechanisms also includes key and identity management. Modern edge operating systems (e.g., Android 11+, Linux Kernel 5.6+) implement hardware-backed keystores such as StrongBox or Keymaster, which provide secure key generation and storage with authorization attributes (e.g., key binding to user authentication or a defined lifespan).

Ensuring a secure system life cycle relies on automated deployment and registration mechanisms, regular software updates, and remote system attestation.

Based on the conducted analysis, a security architecture for edge computing has been proposed (Fig. 1).

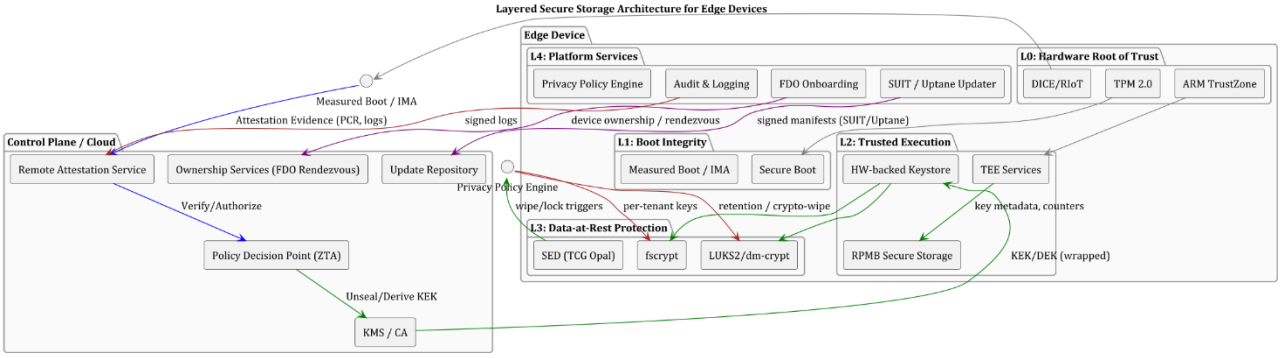

Figure 1 – Edge computing security architecture

The study explores key security issues in edge computing and proposes a comprehensive architectural framework that enhances data protection, integrity, and trust in distributed environments.

References:

1. *Sheikh, A.M.* A Survey on Edge Computing (EC) Security Challenges: Classification, Threats, and Mitigation Strategies. / [A. M. Sheikh, M. R. Islam, M. H. Habaebi, S. A. Zabidi et al.] // Future Internet 2025. 17, no. 4: 175.

2. *Khan, M.* A novel trusted hardware-based scalable security framework for IoT edge devices / [M. Khan, M. Hatami, W. Zhao, S. Qaisar et al.] // Discover Internet of Things. – 2024. – Т. 4, № 4. – DOI: [10.1007/s43926-024-00056-7.

3. *Arora, S.* Fortifying critical infrastructures: secure data management with edge computing / S. Arora, A. Tewari // *International Journal of Advanced Research in Science, Communication and Technology*. – 2023. – № 8. – С. 946–955. – DOI: 10.48175/IJARSCT-12743E.

4*. Liu, J.* Modern network intrusion detection systems / J. Liu, O. Mnushka // *Theoretical and Practical Research of Young Scientists: The Abstracts of the XVIII International Scientific and Practical Conference of Undergraduate and Postgraduate Students (19–22 November 2024)* / ed. by Prof. E. I. Sokol. – Kharkiv: NTU “KhPI”, 2024. – С. 36–37.

5. *Zhao, J.* Network cybersecurity situational awareness / J. Zhao, O. Mnushka // *Theoretical and Practical Research of Young Scientists: The Abstracts of the XVIII International Scientific and Practical Conference of Undergraduate and Postgraduate Students (19–22 November 2024)* / ed. by Prof. E. I. Sokol. – Kharkiv: NTU “KhPI”, 2024. – С. 38–39.