International Journal of Digital Crime and Forensics
Volume 18 • Issue 1 • January-December 2026

Formal Verification of Access Control Policies for Critical IoT Systems

Waleed A. Alrodhan
http://orcid.org/0009-0009-1287-5633
Imam Mohammad Ibn Saud Islamic University, Saudi Arabia
Received: April 12th, 2026 | **Accepted:** May 29th, 2026

ABSTRACT

This paper proposes a formally verifiable access control framework that integrates structured eXtensible access control markup language policy specification with finite-state abstraction and symbolic model checking using NuSMV. To evaluate the proposed framework, a simulated 150-node Internet of Things-based critical infrastructure environment was developed in MATLAB. The framework models three operational states, namely normal, abnormal, and emergency, while incorporating a contextual risk threshold of 0.8 for role-based authorization involving operator, emergency responder, adversary, and policymaker roles. Access control policies were transformed into a finite-state transition system and formally verified for safety, liveness, and non-interference properties. Experimental validation across five consecutive verification runs confirmed that all specified properties were satisfied without counterexamples. Performance evaluation demonstrated an average authorization latency of 0.154 ms, mean CPU utilization of 58%, and average energy consumption of 1.5 J.

KEYWORDS

Formal Verification, Access Control Policies, Critical Infrastructure, IoT, XACML, Finite-State Modelling

INTRODUCTION

Access control policies govern interactions among subjects, between subjects and resources, and under specific conditions to maintain system security and trust (Singh & Singh, 2023). Modernization of critical infrastructure has accelerated the large-scale adoption of Internet of Things (IoT) devices in smart grid environments. Smart grids rely on distributed sensors, intelligent electronic devices, automated controllers, and communication networks to support real-time monitoring and adaptive control of power generation and distribution (Ullah et al., 2023). Although this connectivity improves efficiency, resilience, and operational visibility, it also expands the grid's attack surface (Badar et al., 2022). Unauthorized access to control channels, circuit breakers, or monitoring data can destabilize the grid and potentially trigger cascading failures or widespread blackouts (Mijwil, 2025). Because smart grids operate within safety-critical and time-sensitive environments, security breaches may result in severe economic and societal consequences. Consequently, maintaining grid integrity, availability, and trustworthiness requires stringent and reliable access control mechanisms. Conventional security testing alone is insufficient to verify system correctness across all possible operational states (Krichen, 2023). This limitation has increased the need for mathematically rigorous assurance techniques for enforcing access control policies.

DOI: 10.4018/IJDCF.412447

Various access control models have been implemented in distributed systems, including role-based access control (RBAC), attribute-based access control (ABAC), usage control (UCON), capability-based access control (CapBAC), and policy languages such as EPAL and APPEL. RBAC simplifies authorization management through role assignment but lacks the contextual awareness required in dynamic IoT-driven smart grids (Mehra, 2024). ABAC offers greater flexibility through the use of attributes; however, policy management becomes increasingly complex and error-prone when scaled across heterogeneous devices (Waheed et al., 2025). UCON supports continuity and mutability of attributes, although its implementation on resource-constrained IoT nodes introduces considerable computational overhead (Akpakwu et al., 2025). CapBAC is well suited for decentralized authorization but faces challenges related to revocation and delegation management in critical infrastructure environments (Khan et al., 2022). Despite their advantages, these approaches cannot guarantee correctness across all possible system states.

IoT environments use lightweight authorization and token-based systems to regulate network communication and device authorization (Yang et al., 2023). Risk-adaptive and context-aware models attempt to issue permissions dynamically based on environmental and behavioral factors (Li et al., 2024). Although these approaches improve system responsiveness, they are often heuristically driven and lack formal correctness guarantees. As a result, policy conflicts, privilege-escalation paths, and unintended information flows may remain undetected until deployment (Harsha Vardhan ReddyKavuluri, 2024). Furthermore, scalability challenges emerge when verifying interactions among hundreds of smart grid nodes. Most existing solutions prioritize performance optimization over the verification of safety and liveness properties. Consequently, they lack formal assurances regarding non-interference and emergency intervention mechanisms. This limitation is particularly critical in safety-sensitive infrastructures such as smart grids.

To address these limitations, the proposed framework introduces a formally verifiable access control architecture for critical infrastructure IoT systems through structured policy specification and model-checking techniques. The framework translates access control policies into temporal logic and verifies safety, liveness, and non-interference properties through finite-state modeling. By systematically examining all reachable system states, the approach detects policy conflicts and hidden privilege-escalation paths before deployment. The novelty of this study lies in integrating policy specification with automated formal verification while accommodating smart grid operational requirements, including emergency overrides and risk-sensitive decision-making. Unlike heuristic or test-based validation methods, the framework provides mathematical correctness guarantees while maintaining acceptable latency and energy overhead. In addition, the proposed framework supports forensic procedures by facilitating the detection of access control policy violations through rigorous verification techniques. This study makes several important contributions to the development and formal verification of access control mechanisms for safety-critical smart grid IoT environments:

- Develop a formally defined access control framework for safety-critical smart grid IoT environments.
- Establish a systematic approach for translating policy specifications into temporal logic verification models.
- Verify safety, liveness, and non-interference properties through model-checking techniques.
- Evaluate framework performance in terms of latency, energy consumption, and scalability across distributed smart grid nodes.

Problem Statement

Discretionary access control models allow resource owners to determine who can access their resources. Although DAC provides flexibility, it suffers from weak propagation control because permissions can easily be transferred or inherited without strict regulation (Boehme & Mourtgos,