Evaluation of a Verifiable DBMS (Database Management System)

Ivan Sérgio Rocha Ribeiro
Master's Student
University of Minho
Braga, Portugal
pg55950@uminho.pt

Francisco Macedo Ferreira
Master's Student
University of Minho
Braga, Portugal
pg55942@uminho.pt

XXXXXX
Master's Student
University of Minho
Braga, Portugal
pgXXXXX@uminho.pt

XXXXXX
Master's Student
University of Minho
Braga, Portugal
pgXXXXX@uminho.pt

***Abstract*—Verifiable database management systems (verifiable DBMSs) aim to provide cryptographic guarantees about the correctness of query answers, allowing users to independently verify the integrity of the underlying data and computations. The PETALL project, developed in collaboration with INCM and awarded under the IN3+ innovation initiative, proposes a set of components that enable such verifiability through zero-knowledge techniques. This work presents an experimental evaluation of these components by integrating them into a prototype application designed for an energy community scenario. Our goal is to assess the suitability, limitations, and practical usability of the PETALL verifiable DBMS when applied to real-world application development. Through this case study, we analyze system behavior, data immutability constraints, adversarial considerations, and user interaction requirements. The results highlight both the potential and the challenges of adopting verifiable DBMS technologies, offering insights into their maturity and applicability in practice.**

***Index Terms*—Verifiable DBMS, Zero-Knowledge Proofs, PETALL, Energy Communities**

I. Introduction

II. Case Study

Residential adoption of solar photovoltaic systems has increased significantly over the past few years. Although these households frequently produce surplus energy, a substantial portion of this energy is wasted due to limitations in storage or local consumption. Energy Communities address this inefficiency by enabling households to share excess production with other members, improving sustainability and reducing collective energy costs.

However, sharing energy fairly within a community is non-trivial. Different households exhibit distinct production and consumption patterns, and a naive distribution mechanism may favor certain members disproportionately. For instance, users who consistently produce more energy could repeatedly contribute more than they receive, resulting in systematic unfairness. The energy distribution must also be provable; otherwise, the energy providers themselves might fabricate or omit data to the user for their own financial gain, possibly controling when energy is shared or sold. These fairness concerns motivate the need for transparent and auditable rules governing energy allocation.

A. Problem

One straightforward solution to guaranteeing fairness is to make all production and consumption records publicly available. If every household can inspect every other household's energy history, then each member can verify whether distributions were performed correctly and whether they have received an equitable share.

While an effective solution, this approach introduces a new problem regarding the privacy of the users. Energy usage patterns may reveal highly sensitive information about the occupancy status of the household, such as when residents are home, asleep, at work, or away on vacation, or the type of devices that are being powered. Such information could be exploited by malicious actors, including burglars or other adversaries seeking to infer schedules, household routines, profile households based on estimated wealth or asset levels, or any other sensitive information. Therefore, any realistic system must balance auditability with strong privacy guarantees.

B. Zero-Knowledge as a Solution

To reconcile fairness with privacy, the case study relies on zero-knowledge proofs (ZKPs). PETALL's verifiable DBMS produces cryptographic proofs over immutable snapshots of the database. These proofs allow each participant to verify the correctness of the computed energy distribution without learning the individual production or consumption values of other households.

For example, if a user contributed 10 kWh to the community, the system can produce a proof that they are entitled to receive at least 10 kWh at a later time, while not revealing to this user how much energy any other user contributed or consumed.

III. Application

A. Components

B. Interactions between components

IV. Key Findings

References

[1] S. Nabipour, V. Vahidinasab, and M. Alizadeh, "Residential solar photovoltaic adoption: An in-depth review on potential, main barriers and related incentives," *Energy and Buildings*, vol. 319, 2025.

[2] S. E. Team, "Residential solar photovoltaics in Europe – statistics & facts." 2025.