Secure and Scalable Inter-organizational Process Mining through Trusted Execution Environments

Davide Basile[1 [0000−1111−2222−3333]], Luca Barbaro[2,3 [1111−2222−3333−4444]], and Valerio Goretti[3 [2222−−3333−4444−5555]]

Sapienza University of Rome

Abstract. ...

1 Introduction

In today's interconnected business landscape, organizations are constantly seeking ways to enhance their operational efficiency, increase their performance, and gain valuable insights to improve their processes. In this context, the availability of worthwhile information plays a key role. One of the primary obstacles lies in securely and reliably accessing and utilizing data from various companies or business units, ensuring that all involved parties can derive substantial benefits from it. Traditional approaches to sharing sensitive data across organizational boundaries often involve concerns related to privacy, data integrity, and the need for mutual trust. This paper introduces a novel approach that leverages Trusted Execution Environment (TEE) technology to facilitate the exchange of event logs among different companies or business units. TEE provides a secure and isolated environment within a computer system, ensuring the confidentiality, integrity, and privacy of data and code execution. By utilizing TEE, organizations can exchange event logs in a trusted and privacy-preserving manner, enabling them to harness valuable information from external processes to enhance, monitor, or modify their own processes effectively.

The proposed methodology combines the power of TEE with process mining techniques to unlock the potential of inter-organizational event log exchange. Process mining is a data-driven approach that extracts knowledge and insights from event logs to gain a comprehensive understanding of business processes. By incorporating external event logs from trusted sources, organizations can obtain a broader and more accurate view of the end-to-end processes they are involved in, leading to better process optimization, performance monitoring, and decision-making. By bridging the gap between different organizations, the utilization of TEE-enabled event log exchange for process mining offers promising opportunities for collaborative learning, benchmarking, and continuous process improvement. The findings and insights derived from this research have the potential to revolutionize the way organizations approach process optimization and enable them to make more informed decisions based on a holistic view of their processes.

2 Related Work

The application of process mining in an inter-organizational scenario is infrequent due to concerns related to privacy and confidentiality, integrity and data heterogeneity. To overcome these problems, a large number of techniques have been proposed. Federated process mining [WVDAlst??] aims to effectively manage the problem of privacy-preserving. Using federated data sources, event data can be transparently mapped between multi-source autonomous provider to monitor, analyze, and improve processes across organizations. Once the data exchange has taken place, it is critical that the data be stored in a trusted part of the consumer's device. Davide et al. [1] in their study created a framework called Regov that allows for the exchange of sensitive information in a decentralized web context, ensuring usage control-based data access and usage. To ensure control over the consumer's device, Davide et al. use trusted execution environment that allows storage and utilization management of retrieved resources.

3 Motivating Scenario

4 High level Architecture

In the following section we present the high level architecture underlying our solution. Therefore, we take into account each component individually. Once introduced the architecture, we provide an overview on the main interactions taking place between the introduced components.

4.1 Main components

Our architecture involve networks of nodes controlled by different `Organization`s exchanging their event logs. `Organization`s in the same network collaborate to reach a common objective sharing one or more business processes. The Hospital and Specialized Clinic, mentioned in the running example, provide an example of partner organizations.

In section 4.1, we propose an high level schematization of our solution. Each organization embeds three main components: the `EMS Interface`, the `Log Provider` and the `Trusted Miner`. In the next paragraph, we address the newly mentioned components.

EMS Interface Collects the logic to interact with the Environmental Management System (EMS) of the organization.

Log Provider The `Log Provider` component deliver on-demand data to partner organization's systems.

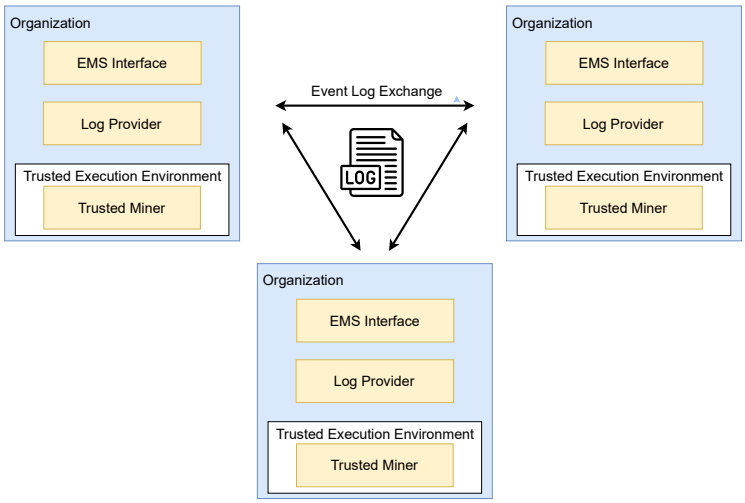

Fig. 1. High-level architectural overview of the framework.

Trusted Miner The `Trusted Miner` executes process mining algorithms inside the `Trusted Execution Environment` using event log retrieved from partner organizations.

4.2 Workflow

Initialization

Data Exchange

Data Elaboration

5 Implementation

5.1 Event Log Generation

5.2 Trusted Miner and Log Provider

6 Evaluation

6.1 Discussion

Privacy

Security

Integreatebility

6.2 Convergence Study

Settings

Results

7 Conclusion and Future Work

Limitations:

- Both producer and consumer act fairly (so we do not expect to have enjected data)
- We do not manage TEE crashes
- We assume perfect communication channel (no loss, no snap, no corrupted bits)
- Universal clock for event timestamps (cite Event log cleaning for business process analytics by Andreas Salti)

Future Work:

- Declarative models adaptation
- Output inside the TEE, interactions through trusted applications
- Real world event log data
- Usage policies integration

References

1. D. Basile, C. D. Ciccio, V. Goretti, and S. Kirrane, "Blockchain based resource governance for decentralized web environments," *Frontiers in Blockchain*, vol. 6, may 2023.