ClaimChain: Secure Blockchain Platform for Handling Insurance Claim Processing

George Stafford, Masrik Dahir*, Roshan Neupane, Naga Ramya Bhamidipati, Varsha Vakkavanthula, Prasad Calyam
University of Missouri-Columbia, *Virginia Commonwealth University
Point-of-contact: calyamp@missouri.edu

July 2021

Problem Motivation

- Traditional Insurance claims processing is manual/slow due to co-ordination of multi-domain entities (e.g., police, repair shops, adjudicators, …)
- Blockchain technology-based solutions can significantly help with intelligent automation but are vulnerable to fraud claims, and cyber-attacks such as Sybil attack

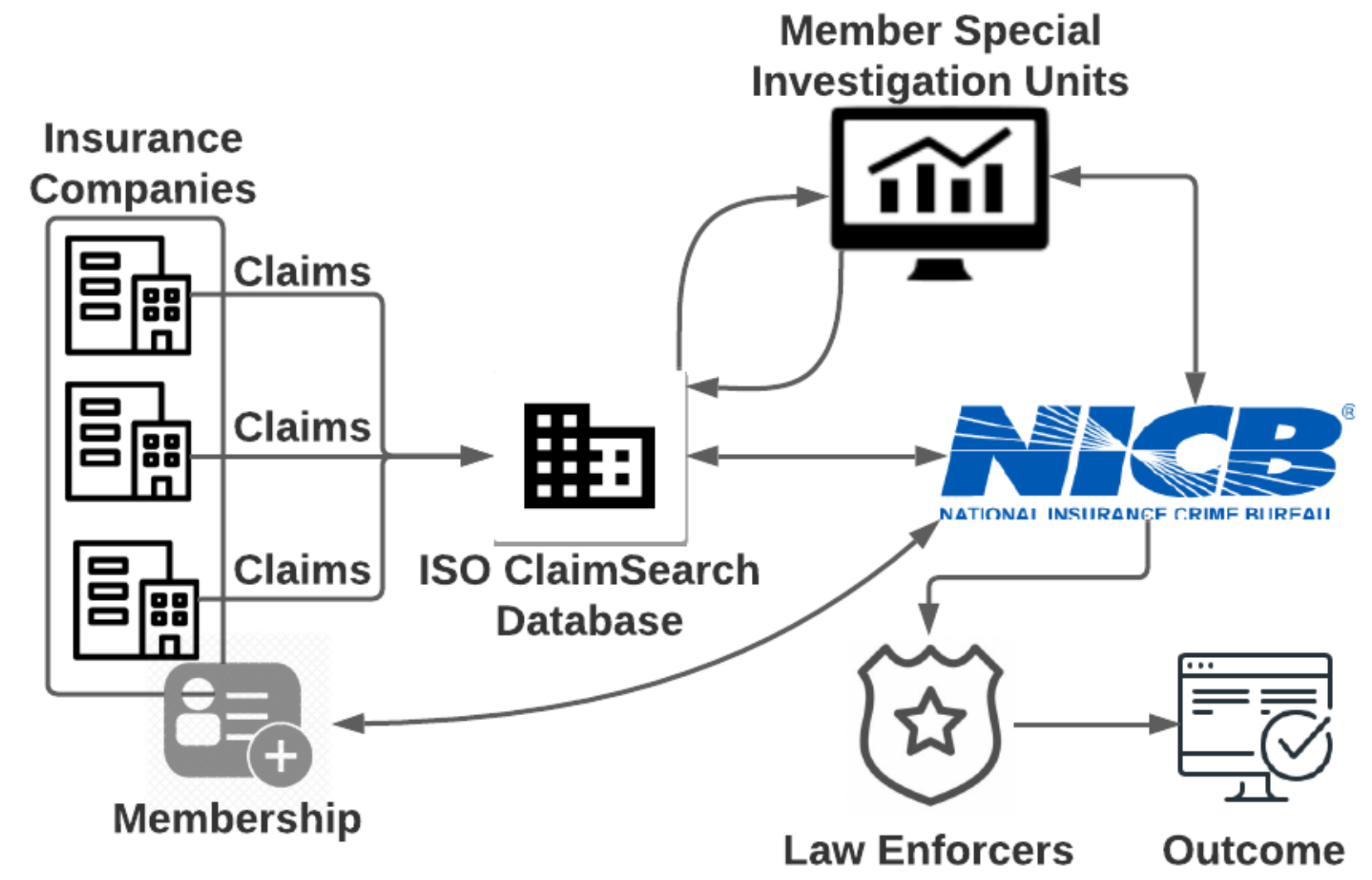


Figure 1: ***Traditional paradigm for monitoring claim fraud, organizations must be a member to access the NICB database.***

Challenge: To create a secure Blockchain-based solution for insurance claim processing with data-driven methods and risk assessment

Solution and Novelty

- We design and implement a novel consortium Blockchain i.e., *ClaimChain* to facilitate insurance claims processing
- We present a formal threat modeling of attacks realizable in *ClaimChain* through attack trees
- We utilize red flags identified by NICB and use ML models to detect fraudulent activities with significant accuracy

Attributes	NICB Database	ClaimChain
Authority	The database is centralized in nature	*ClaimChain* uses blockchain which is **decentralized**
Transparency	NICB administrators only decide what data to be made public	*ClaimChain* offers **transparency**
Integrity	NICB uses database that can be altered by malicious actors and can lose data integrity	*ClaimChain* supports **integrity** in data as any update made is validated through consensus algorithm
Data Handling	The data can be erased or replaced as databases utilize CRUD (Create, Read, Update, Delete)	*ClaimChain* offers **immutability** meaning no data tampering is possible within the network

Figure 2: ***Blockchain VS NICB Database.***

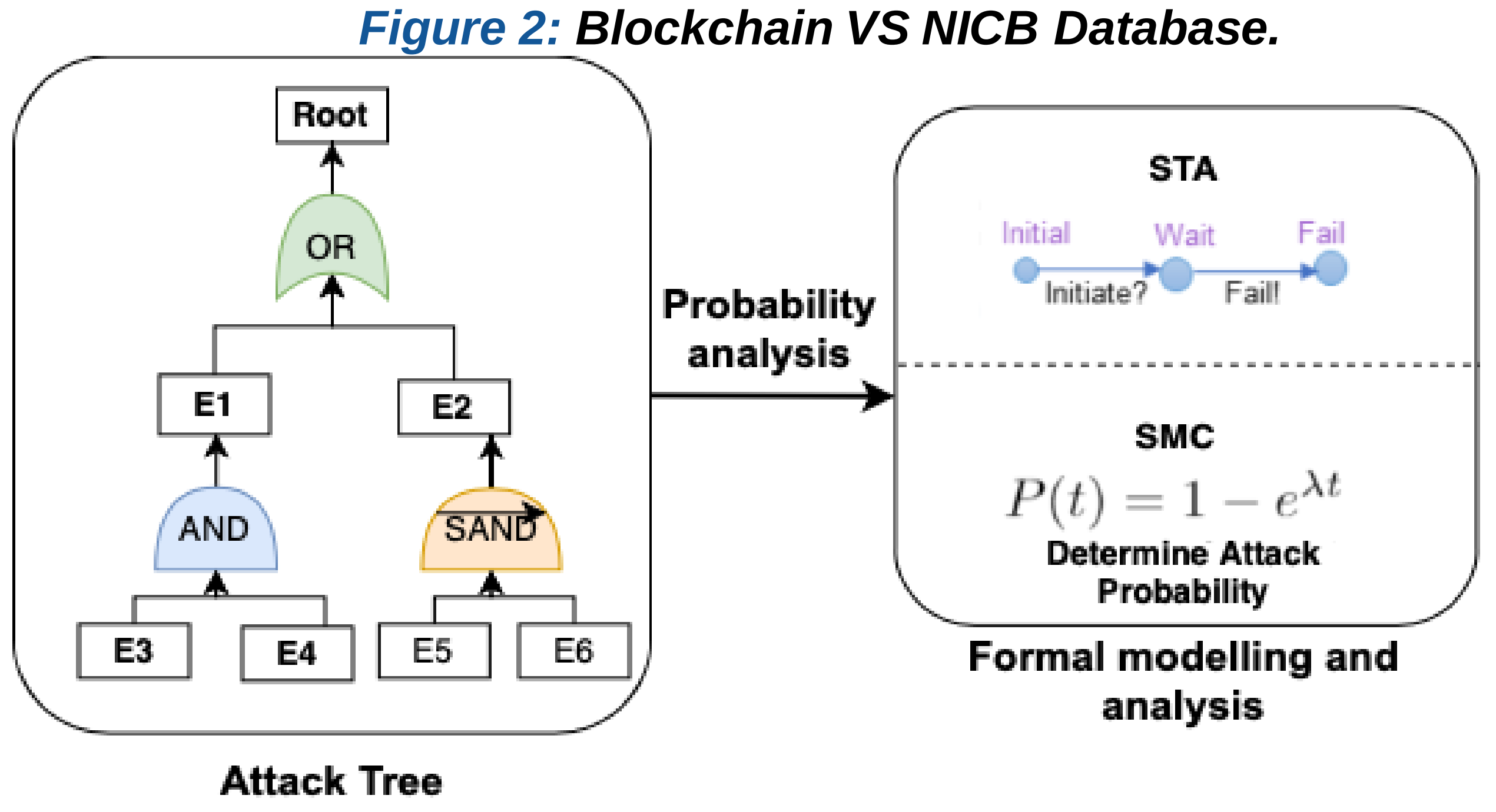


Figure 3: ***Formal threat modeling using attack trees and quantitative probability analysis using Statistical Model Checking.***

Contribution 1: *ClaimChain* for Claim Processing

- Utilizes consortium Blockchain to track the entire population of claims across participating agencies
- Offers built-in fraud detection via our fraud model that checks e.g., duplicate claim information present and creates alerts based on NICB red-flags

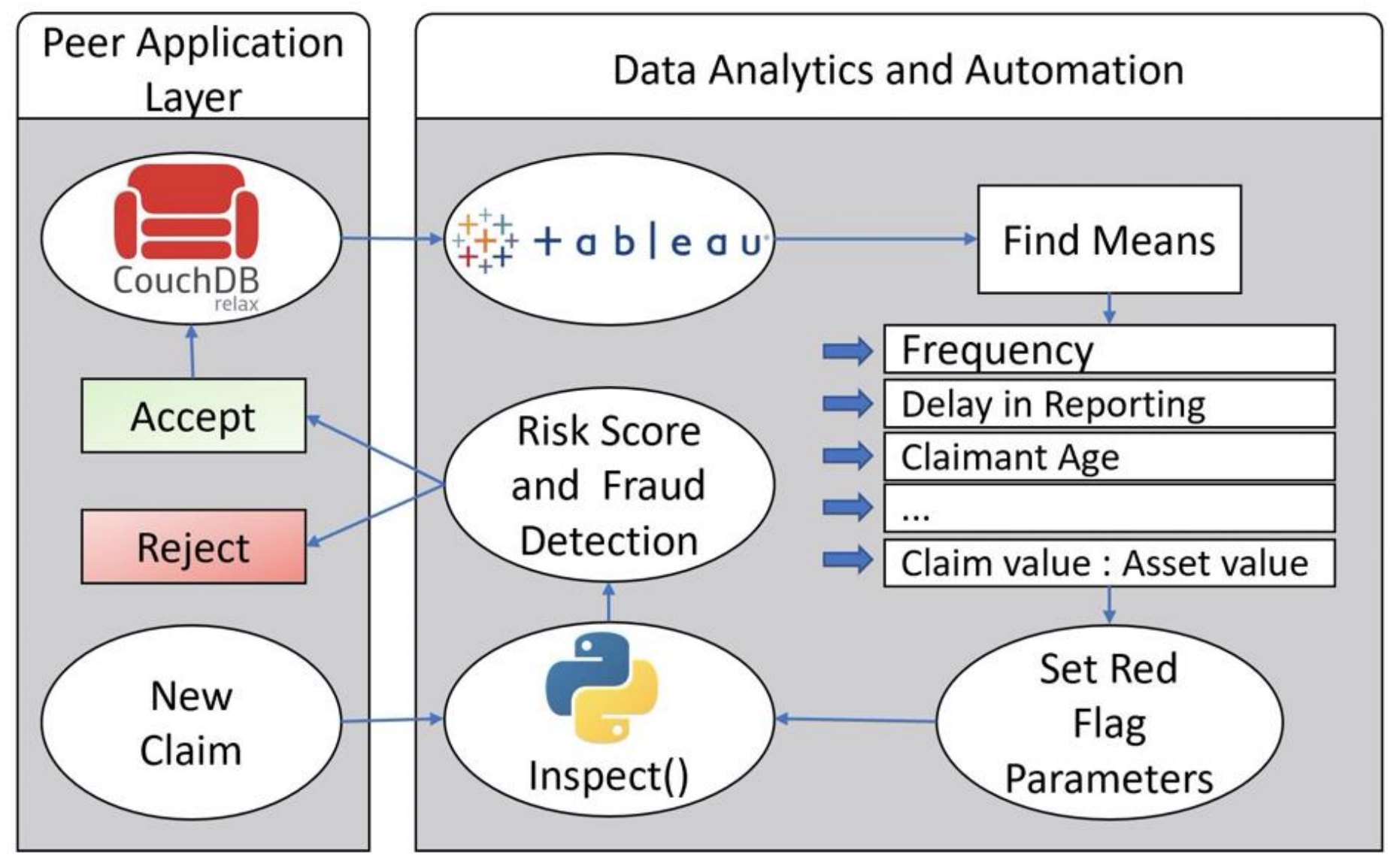
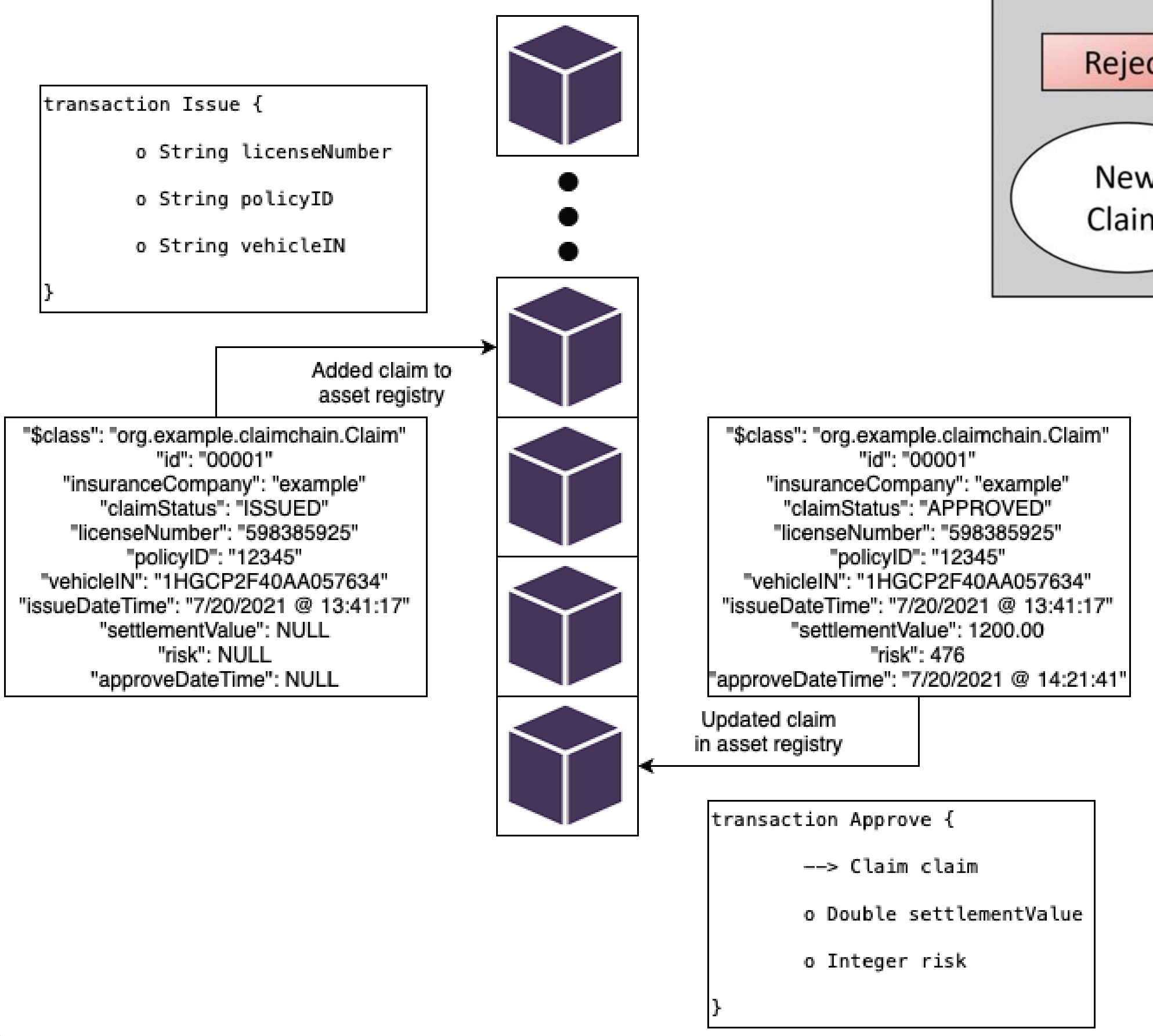


Figure 4: ***Fraud Detection unit uses machine learning models to detect fraudulent activities through red flags identified by NICB.***



```
transaction Issue {
        o String licenseNumber
        o String policyID
        o String vehicleIN
}
```

```
"$class": "org.example.claimchain.Claim"
"id": "00001"
"insuranceCompany": "example"
"claimStatus": "ISSUED"
"licenseNumber": "598385925"
"policyID": "12345"
"vehicleIN": "1HGCP2F40AA057634"
"issueDateTime": "7/20/2021 @ 13:41:17"
"settlementValue": NULL
"risk": NULL
"approveDateTime": NULL
```

```
"$class": "org.example.claimchain.Claim"
"id": "00001"
"insuranceCompany": "example"
"claimStatus": "APPROVED"
"licenseNumber": "598385925"
"policyID": "12345"
"vehicleIN": "1HGCP2F40AA057634"
"issueDateTime": "7/20/2021 @ 13:41:17"
"settlementValue": 1200.00
"risk": 476
"approveDateTime": "7/20/2021 @ 14:21:41"
```

```
transaction Approve {
        --> Claim claim
        o Double settlementValue
        o Integer risk
}
```

Figure 5: ***Snapshot of ClaimChain 'Issue' and 'Approve' transactions; 'Issue' creates a claim object with passed claim information, marks it as 'ISSUED', and inserts it into the claim registry; 'Approve' retrieves the claim from the registry, updates it with settlement value and risk score, and marks the claim as 'APPROVED'.***

Contribution 2: Security Design Principles

- We create attack trees to model different attacks in terms of Loss of Integrity by decomposing their execution into individual goals
- The statistical modeling checking tool i.e., UPAAAL tool provides the quantitative analysis of different attacks on the system
- Recommended design principles help in reduction of probability of attacks on the ClaimChain system

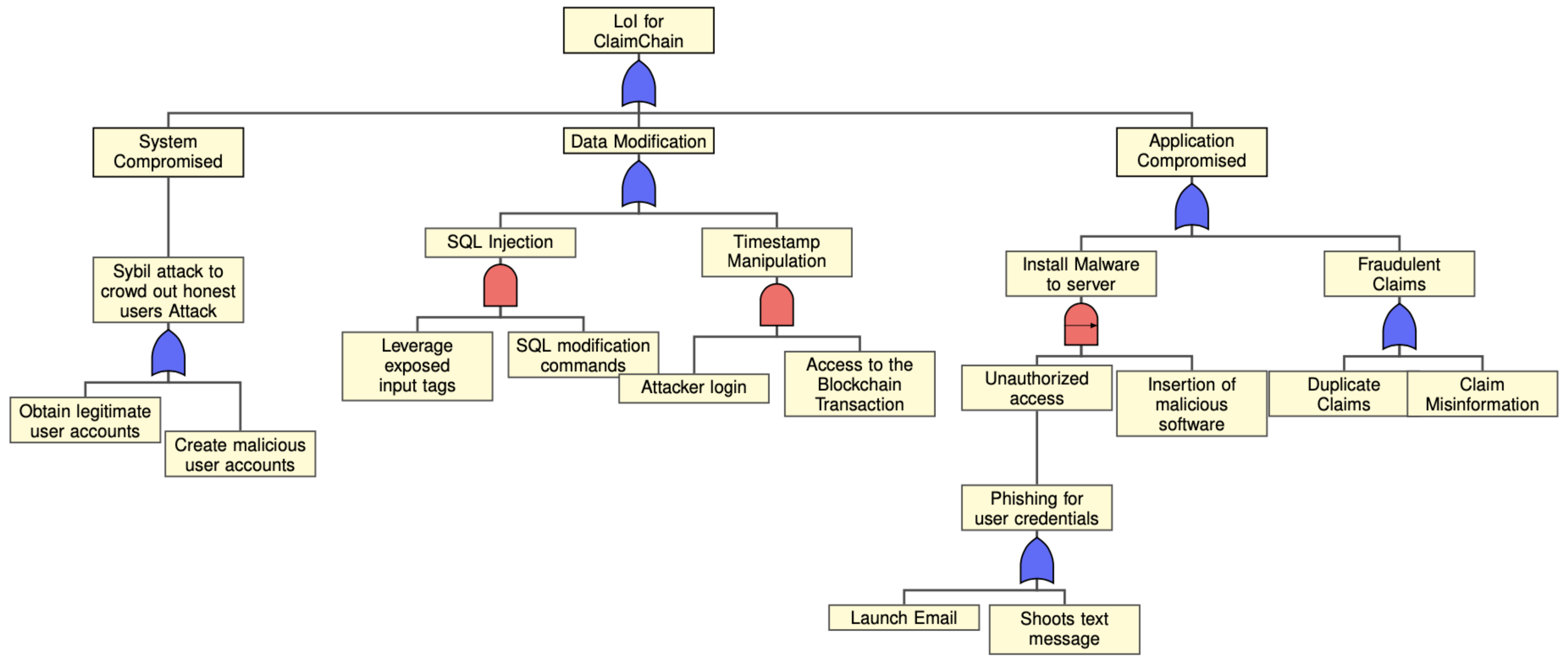

LoI for ClaimChain
System Compromised
Data Modification
Application Compromised
Sybil attack to crowd out honest users Attack
Obtain legitimate user accounts
Create malicious user accounts
SQL Injection
Leverage exposed input tags
SQL modification commands
Timestamp Manipulation
Attacker login
Access to the Blockchain Transaction
Install Malware to server
Unauthorized access
Insertion of malicious software
Phishing for user credentials
Launch Email
Shoots text message
Fraudulent Claims
Duplicate Claims
Claim Misinformation

Figure 6: ***Security Attack tree for Loss of Integrity for ClaimChain application***

Performance Evaluation

Goal: To understand the impact of different attack scenarios on the *ClaimChain* system and show the effectiveness of fraud detection module in our system.

- We use a dataset with 15,430 claims out of which 924 are fraudulent claims and each claim comprises of 33 attributes.
- In Hyperledger composer, as the number of accounts increases, the processing time to invoke chaincode functions increases, from 0 to 240 seconds.
- We evaluated our system by showing the reduction of probability of Loss of Integrity attacks by considering suitable design principles.

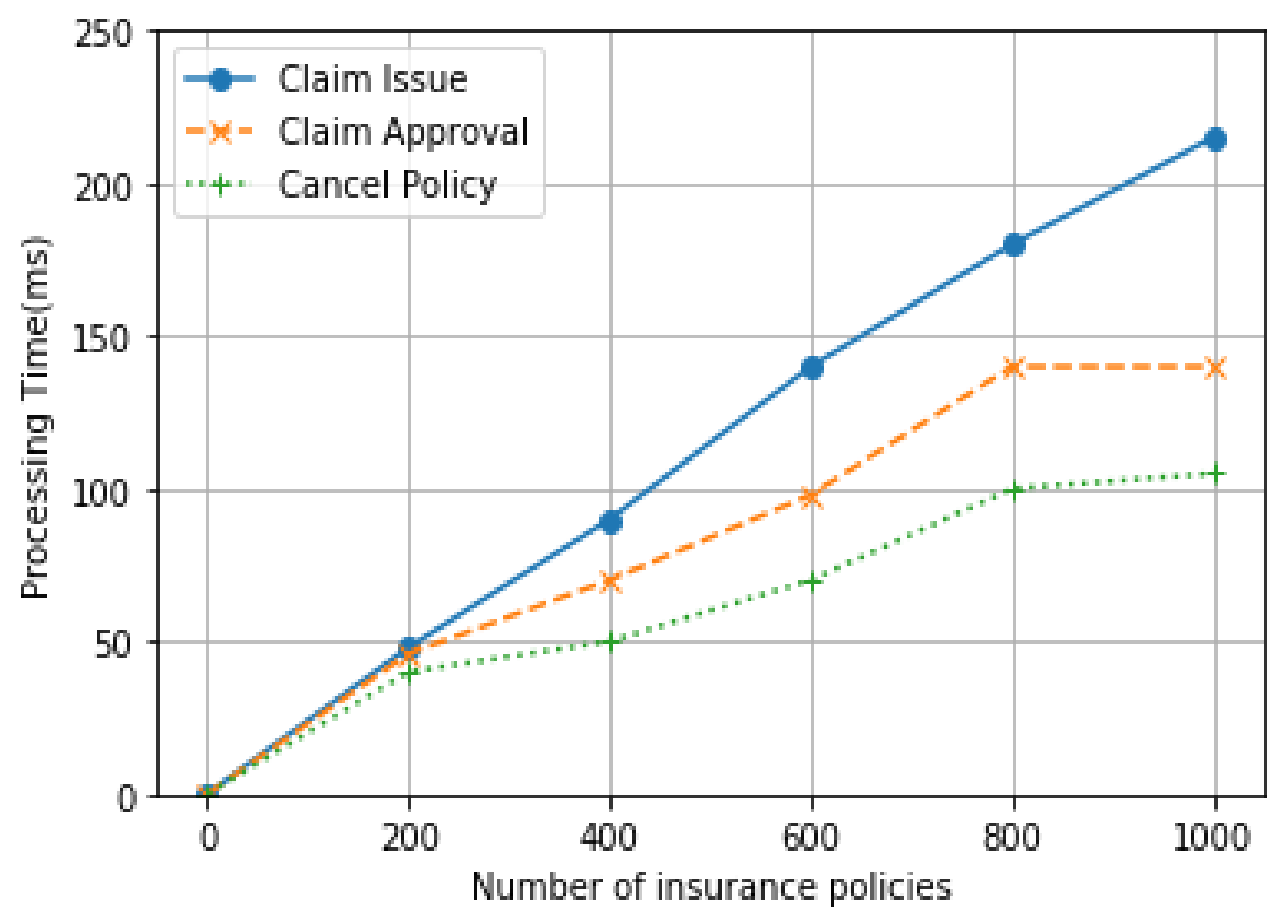


Figure 8: ***Scalability overhead for 1000 policy holders' insurance policies.***

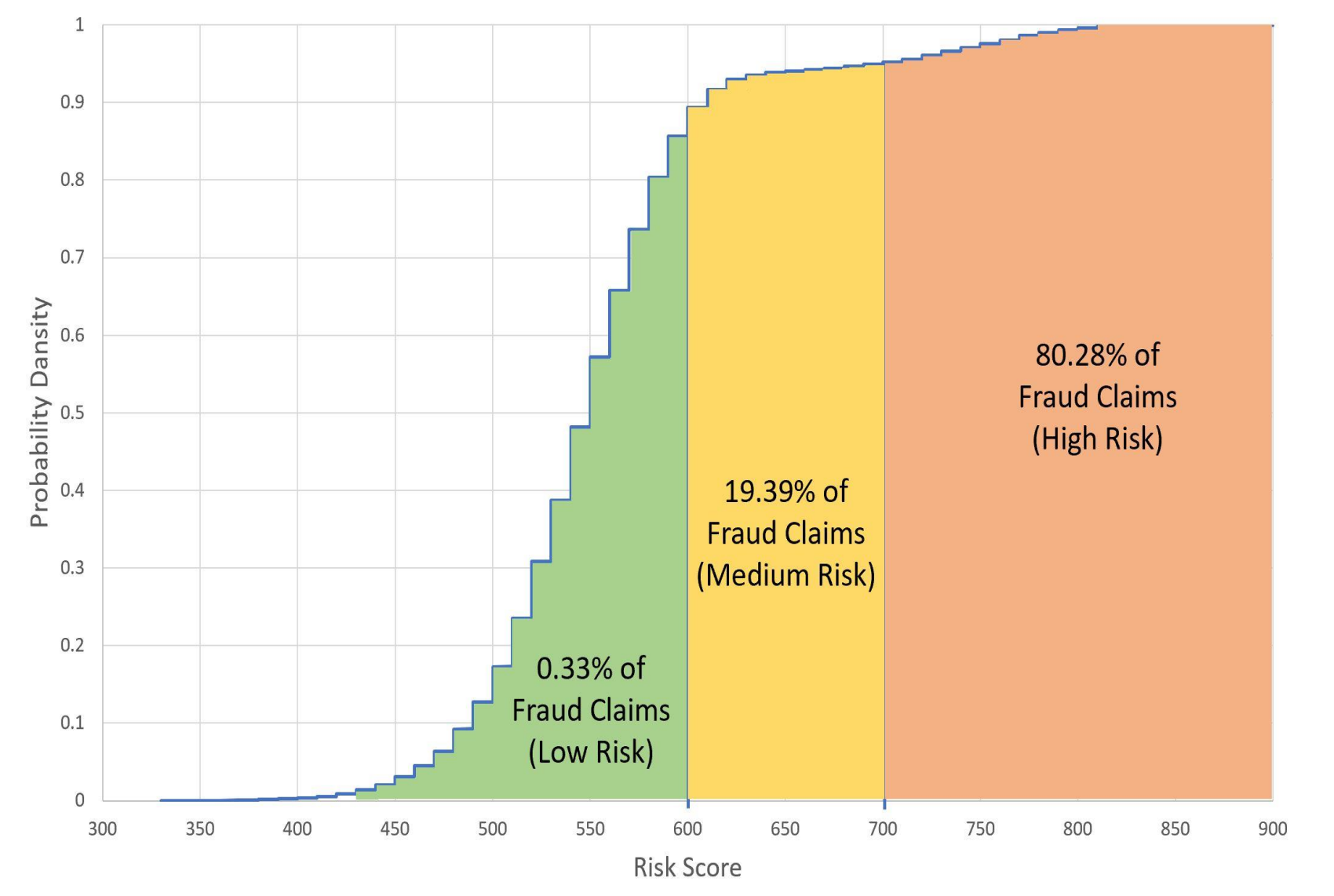


Figure 9: ***Determination of risk of the claims through fraud detection module***

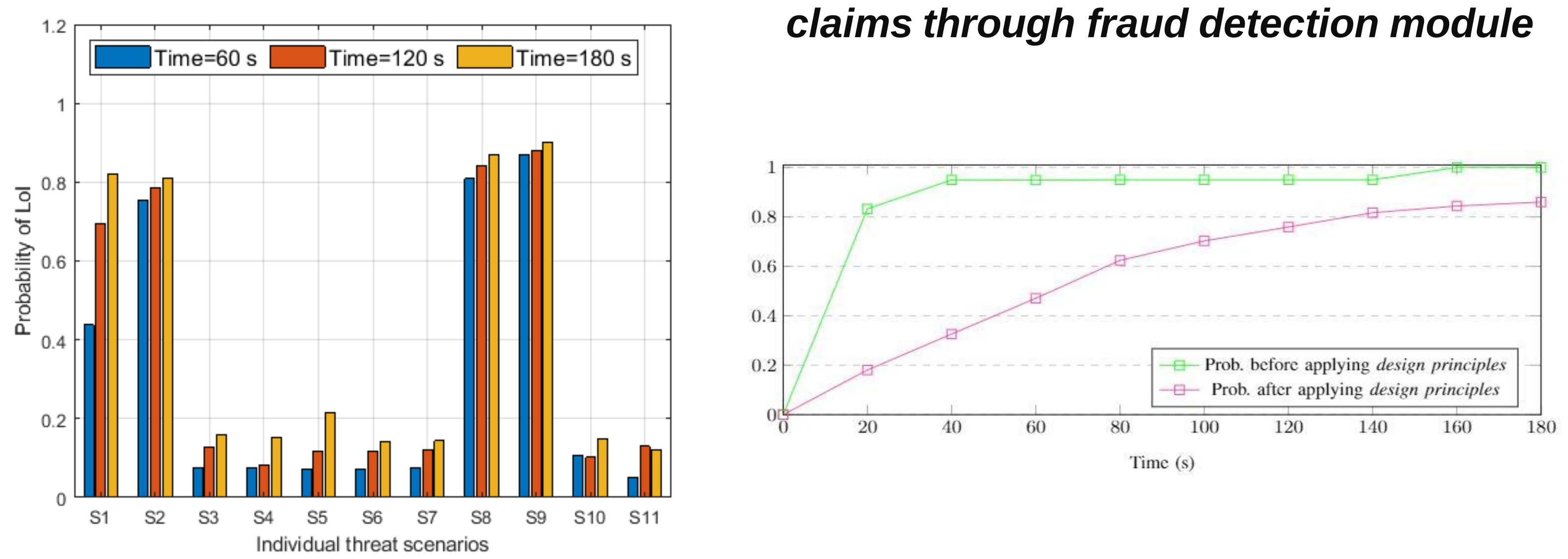


Figure 10: ***Illustration (see left Fig.) of probability for different Loss of Integrity attack scenarios and the probability reduction (see right Fig.) after applying design principles.***

Salient Findings

- *ClaimChain* consortium Blockchain is a futuristic alternative to the NICB's ISO database achieving greater participation, processing efficiency, and trust
- *ClaimChain* fraud model is effective at detecting known red-flags with up to a 98% detection accuracy and effective at combatting duplicate claims among participating agencies
- *ClaimChain* security design principles are effective in protecting insurance claims processing system as seen in reduction of 25% probability of Loss of Integrity before and after application

This material is based upon work supported by the National Science Foundation under Award Number: CNS-1950873 and US State Department under Award Number: 00071769. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the National Science Foundation or US State Department.