CS731 : Project Specification

Supervised by : Prof. Sandeep Kumar Shukla

Aneet Kumar Dutta(18111401)
Bidya Sarkar(18111011)
Gourav Takhar(18111265)
Komal Kalra(18111032)
Manish Mazumder(18111038)

Indian Institute of Technology Kanpur
Department of Computer Science
Engineering

March 28, 2019

Title: Blacklisting URL within an Organization Network

Abstract

This project aims at developing an URL blacklisting system in blockchain using HyperLedger composer. Our work focuses on blacklisting malicious urls within an organizational network(consider a network of users in an University). This will prevent the users within the organization from falling in victim of phishing attacks and downloading malwares which will result in infecting the large part of the network. In conventional systems the blacklisting urls within an organization solely depends on the network administrator but here we tried to develop this system using blockchain so that we do not have to put our trust on the network administrator. The solution is developed for particular organization so using permissioned blockchain will be more useful.

Introduction

An URL blacklisting system such that anyone can propose an URL to be blacklisted but it has to be endorsed according to endorsement policy, and anyone can query the blacklist but once included in blacklist the process of removal from blacklist may have a process of endorsement again.

The utility of this project is to Protect users of the network from phishing attacks or visiting malicious/banned websites. Also we can implement role based access to certain URLs. For example : Certain URLs(solution to the assignments) can be accessed by faculties only and not by students.

So the need to have Blockchain Technology is that addition or removal of urls should pass through an endorsement policy in blockchain instead of some centralized administrative authority. The centralized authority may not be trusted and can perform malicious addition or removal of URLs from the blacklist.

Considering the scenario where a malicious system administrator removes a malicious URL from the list and convince the users in the network to visit that malicious URL. This will infect the large number of users in the network.

Blockchain platform used is - **Hyperledger composer**.

We are trying to deploy this solution within an organizational network. This requires everyone to have proper credentials to log in the network. Membership Service Provider(MSP) of Hyperledger allows us to implement authentication of member identity and roles. That's why we have chosen Hyperledger over Ethereum.

System Architecture

There are three major components in this Hyperledger :

1. Assets
    - URLs
    - IP
2. Participants
    - Faculty
    - Students
    - Network Admin
3. Transactions - Transaction will change the state of the assets to either blocked or unblocked.

Database- Couch DB

- URL list (URL, Blocked by, Blocked/ Unblocked)
- Participant (Auth-Id, Role, Active/Non active)

Node Creation- Nodes will be in same machine.

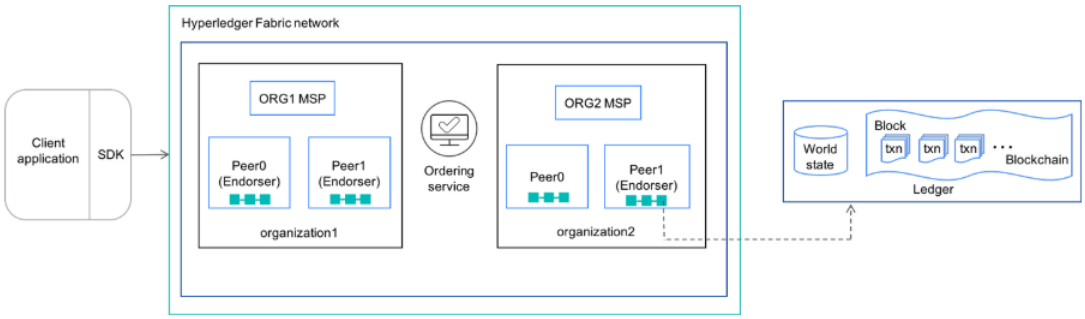
Endorsement - There are three types of Endorsement peer in our Endorsement policy.

- Representative from Faculty
- Representative from Student
- Network admin

Our Endorsement policy will ensure that the transaction need to be signed by endorsing peer from all endorsing peers from network admin, student and faculty.The number of endorsing peers required from each organization depends on discretion of the developer.

The work flow of the system is as follows :

- Client SDK will initiate transaction(blocking or unblocking any particular URL/IP) proposals to the endorsing peers.
- Endorsing peers will verifies the client's signature, executes the transaction and sends an endorsement signature.
- If the transaction is endorsed, the client submits the transaction to the ordering service.
- The ordering service orders and delivers the transaction to the peers.
- The Ledger is then updated.



Feature List

- Add student: To add a student entity in the network.
- Add Faculty: To add a faculty member entity in the network.
- Blocking/Unblocking proposal: An entity will initiate a transaction for blocking/unblocking an URL.
- Download from external feed and block: Malicious urls from external feed() is downloaded and transaction is initiated for each of these urls.
- Show List: Every participant in the blockchain will be able to see the updated list of urls and its status.

Our first priority feature will be Blocking/Unblocking proposals and the advanced feature that we implement is to Download from external feed and block.

Testing

Participant	**if endorsed**	**if not endorsed**
Participant1(Student or Faculty) request URLs for blocking	List update	Cannot update list • URL already exists • Doesn't satisfy endorsement
Participant1(Student or Faculty) requests for unblocking URLs	Change the state of the URLs from blocking to unblocking	Cannot unblock
Participant1(Student or Faculty) show list	List is shown as there is no need for endorsement	
Network admin requests for feed update	Update list	Cannot update
Student or Faculty requests for feed update	Transaction will not get endorsed	Cannot update the list as Endorsement will be false
Feed update by Network Admin	Ignore the URLs which are already in the list and update others	Cannot be updated
Add Participants	No endorsement is needed here and Add Participants will be added	

TimeLine

Time-Frame	**Task**
March 29 - 31	System setup
April 01 - 07	Basic Functionality implementation
April 08 - 10	Basic functionality testing
April 11 - 14	Improvement in functionality and complete testing

Caveats

The main challenge of this project is to frame the correct endorsement policy based on the participants. Though we mentioned our endorsement policy here in the document. This policy might not be realistic enough because the endorsers may not have any stake in the transaction(suppose a faculty/student is not bothered at all about blocking an url).