Securing Cloud Transaction through blockchain

Group Members

Srejan Kumar Bera 19103011

Vaibhav Chawla 19103027

Akarsh Puri 19103028

SUPERVISOR
Dr. Taj Alam

PROBLEM STATEMENT

- Cloud computing has proven to be a key technology for delivering infrastructure and service at a low cost. The rapid growth in the use of this technology has been observed but the security issues related to it have still not been addressed completely.
- Some of the major security issues related to cloud are On/Off attack, Collusion Attack, Sybil Attack, DoS attack and theft of data.
- Further, small scale cloud services cannot ensure proper security, therefore, in order to make them stand a chance in this industry an alternative to current scenarios must be formulated.

INTRODUCTION

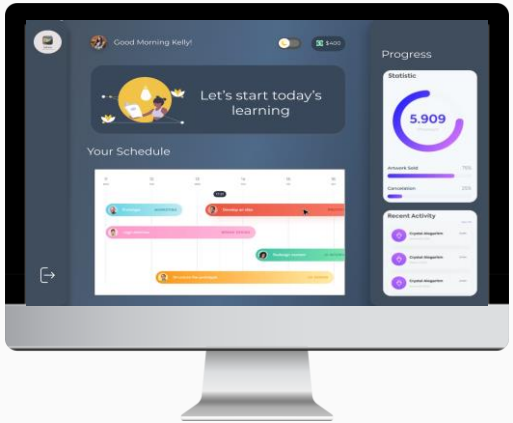
- We intend to make use of Ethereum blockchain to prevent the malicious use of cloud services. Issues related to data leakage and credential exposure are implicitly handled by the blockchain further placing usage logs in the blockchain and checking them from the blockchain via APIs in the website, helps to check any malicious use.
- We are working towards making a dummy cloud with two services which have a maximum limit of users. One service is made for individual use and other for group use. The client asks for service from the server and based on the availability the server provides the service, basic entries like user, start time etc, are placed into the blockchain. When the client exits the service the end time is noted.
- Based on these entries we can point out the malicious behavior we observe through the logs. Further metrics of all the users will be provided to the admin with an option to blacklist/block any user in order to flag/block his/her transactions in future

MAJOR ATTACKS TO BE MANAGED

- Sybil Attack - A Sybil attack is a kind of security threat on an online system where one person tries to take over the network by creating multiple accounts, nodes or computers. This can be as simple as one person creating multiple social media accounts. In really large-scale Sybil attacks, where the attackers manage to control the majority of the network computing power or hash rate, they can carry out a 51% attack.
- On/Off Attack – Here the attacker behaves well and badly alternatively in system. Thus, a new trust management and redemption scheme needs to be developed that can discriminate between temporary errors and malicious behaviors. It is a new flexible trust management scheme that can well detects and defends against the on/off attacks.

FEATURES

- Login via OTP and Email Verification
- Make use of a user (if available)
- Logs of service use stored permanently in blockchain
- Check your usage with help of graphs
- Admin monitors the use of both services
- Admin can block/blacklist malicious users by checking their logs and observing malicious behaviour
- Use of blockchain resolves cloud security issues like Sybil Attack



TOOLS & TECHNOLOGIES USED

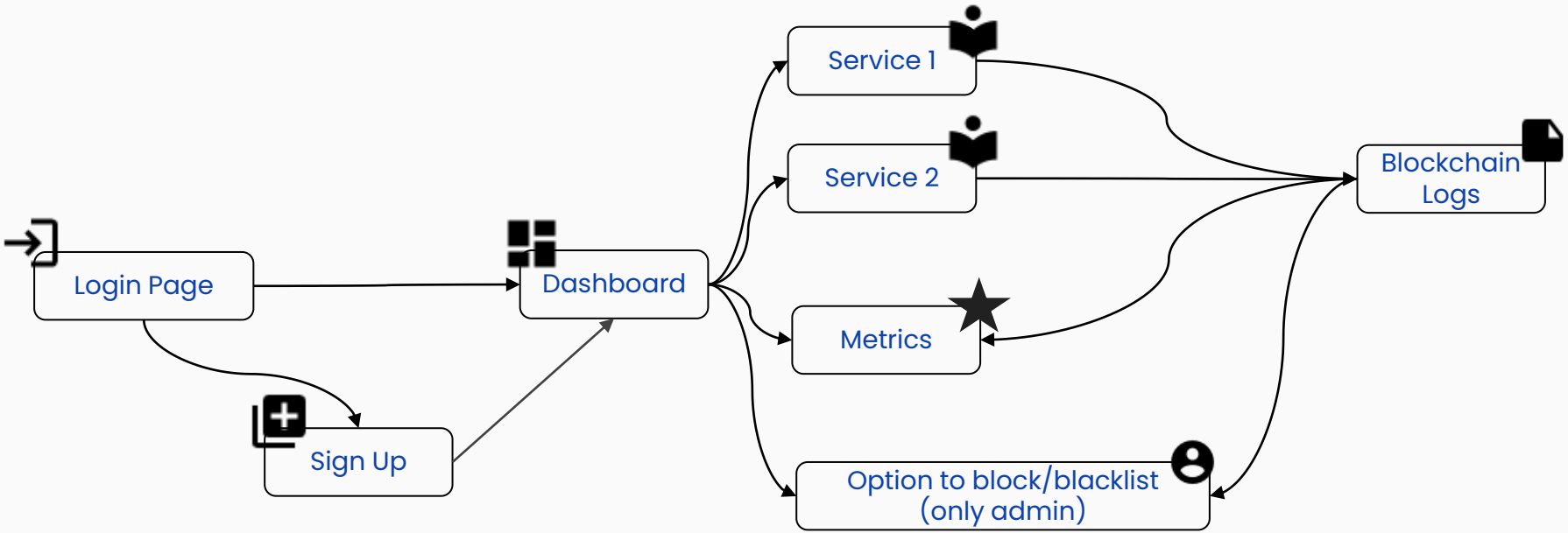
TECHNOLOGIES USED

- React JS
- Node JS
- Express JS
- Mongoose JS
- Ethereum blockchain

TOOLS USED

- VSCode
- Node Package Manager
- Ethereum (Solidity) Compiler
- MongoDB

FLOWCHART


Service 1
Service 2
Blockchain Logs
Login Page
Dashboard
Metrics
Sign Up
Option to block/blacklist (only admin)

FUTURE SCOPE

- Adding the AWS/GCP services directly through the website, to provide the extra-layer of blockchain security
- Using blockchain technology to store data on the cloud in the blockchain

REFERENCES

[1] The Byzantine Generals Problem LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE SRI International

[2] DOLEV, D. The Byzantine generals strike again. J. Algorithms 3, 1 (Jan. 1982).

[3] PEASE, M., SHOSTAK, R., AND LAMPORT, L. Reaching agreement in the presence of faults. J. ACM 27, 2 (Apr. 1980), 228-234.

[4] https://www.geeksforgeeks.org/benefits-and-applications-of-blockchain-in-cloud-computing/

[5] ISC2 Cloud Security Report 2021