Developing a distributed processing cloud platform using Fully Homomorphic Encryption

Scientific coordinator:
Lecturer Ph.D. Andrei TOMA

Graduate:
Mihai TURCU

Overview

- Problem formulation
- Solution architecture
- Solution implementation
- Conclusions

1. Problem formulation

Cloud privacy & Cloud processing conflict

Cloud processing

- Flawed from the start
- User uploads data => decryption necessary for processing
- FHE safeguards data during processing

2. Solution Architecture

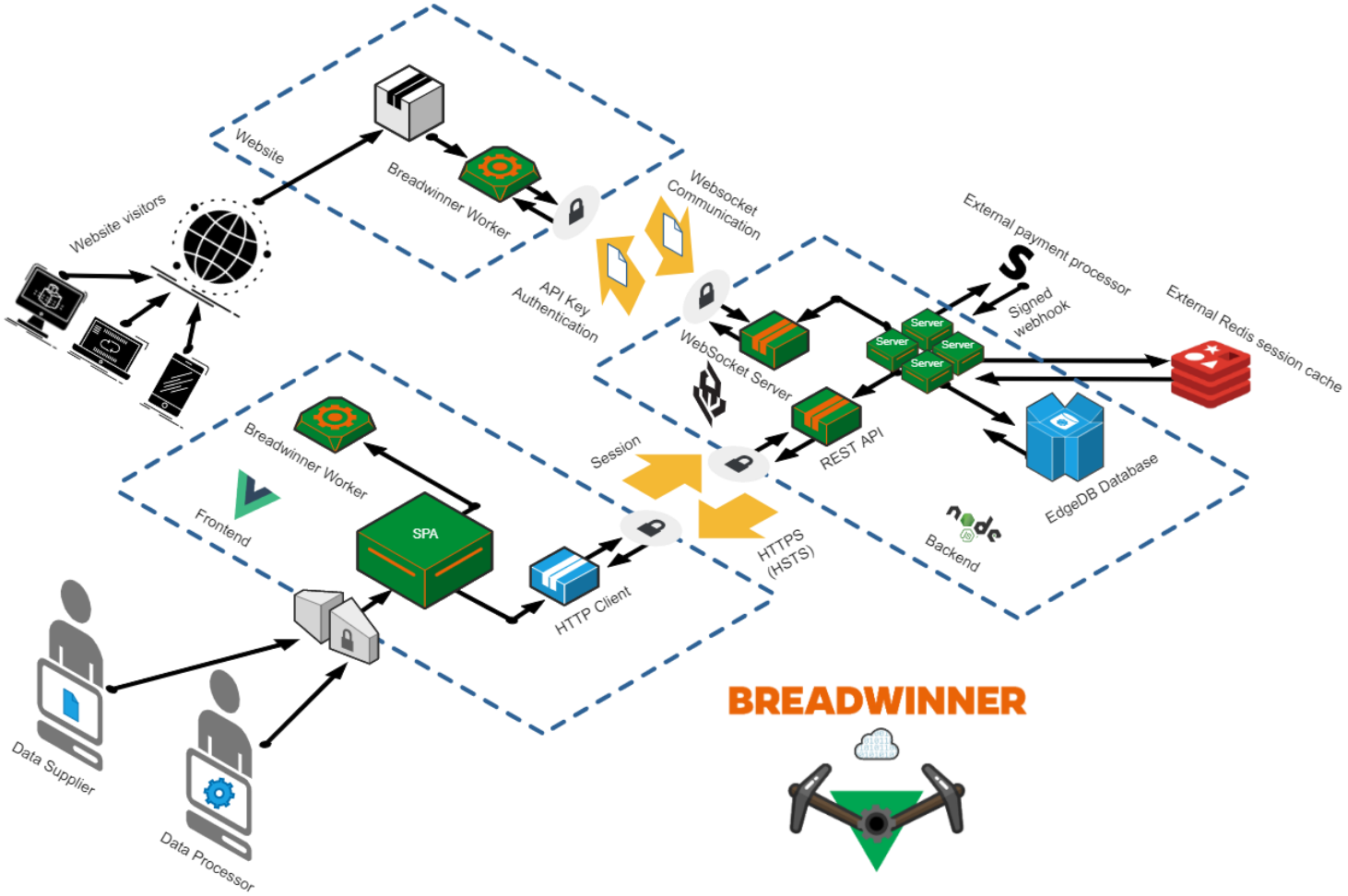
Actors & modules

What is Breadwinner?

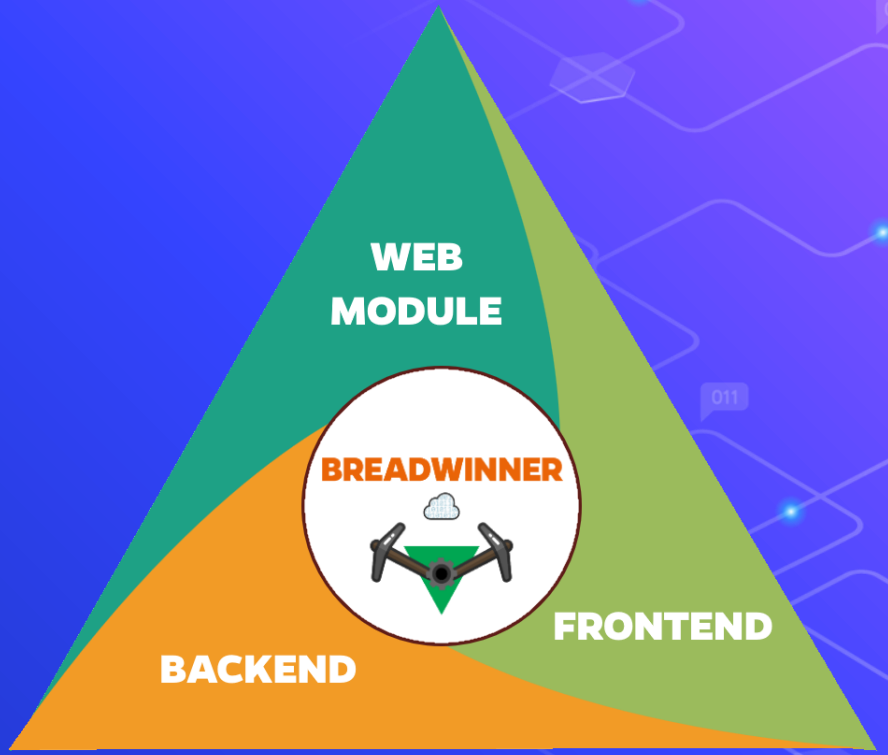
- Secure distributed & outsourced processing cloud platform
- Uses Fully Homomorphic Encryption to solve cloud privacy & processing conflict
- Offers alternative web monetization scheme

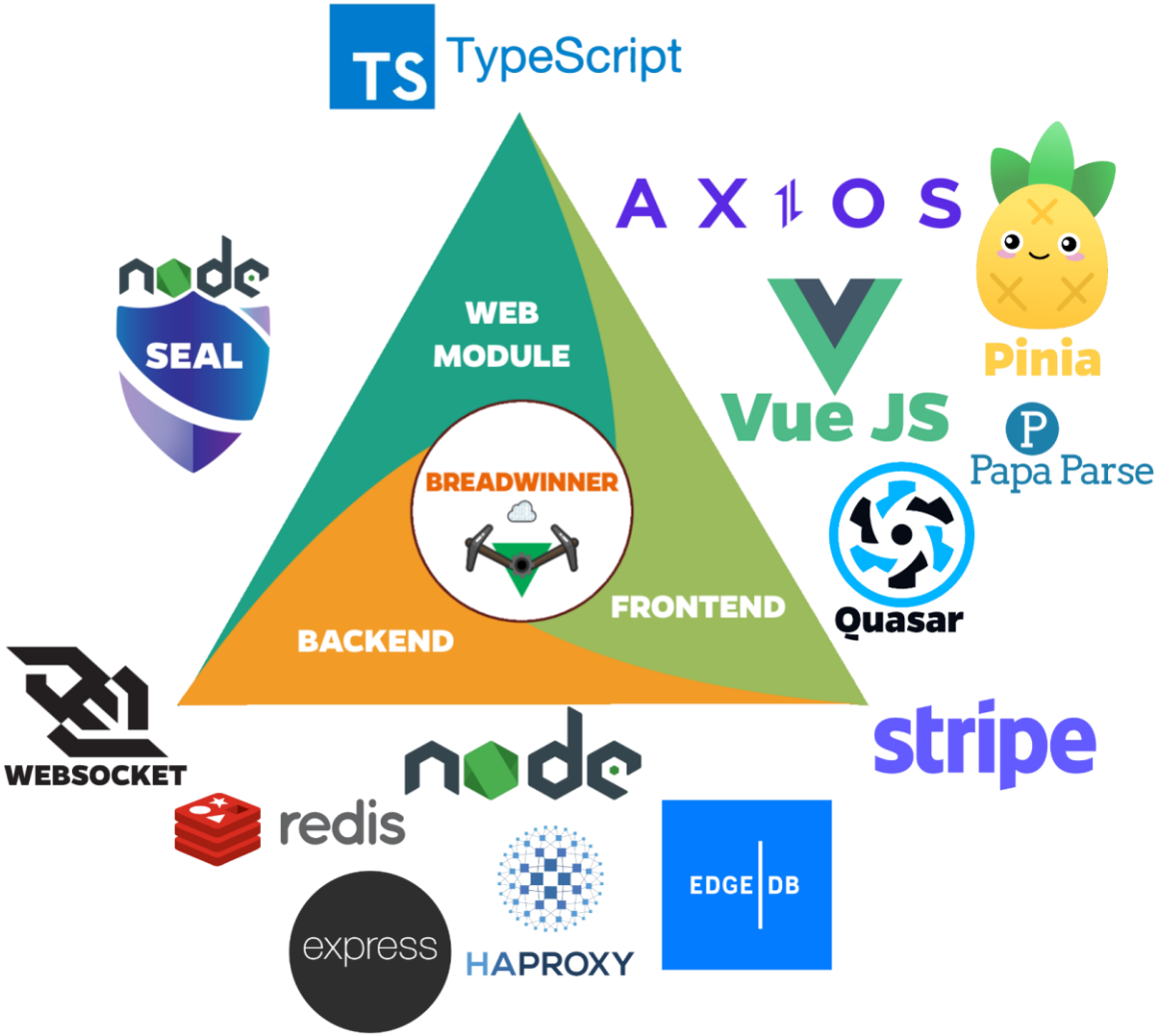
Actors

- Data suppliers – desire cloud storage & processing
- Data processors – looking for an alternative monetization scheme for their website
- Website visitors – offer devices as infrastructure


Website
Breadwinner Worker
Website visitors
Websocket Communication
API Key Authentication
External payment processor
Signed webhook
External Redis session cache
WebSocket Server
Server
Server
Server
Server
REST API
EdgeDB Database
Session
Breadwinner Worker
Frontend
SPA
HTTP Client
HTTPS (HSTS)
Backend
Data Supplier
Data Processor
BREADWINNER

3. Solution implementation




TypeScript
AXIOS
Pinia
node
SEAL
WEB
MODULE
Vue JS
Papa Parse
BREADWINNER
Quasar
FRONTEND
BACKEND
WEBSOCKET
stripe
node
redis
EDGE DB
express
HAPROXY

Security considerations

- Confidentiality – FHE, TLS, Access Control (Sessions), Argon2
- Integrity – TLS, FE & BE validations, tokens when sending data chunks to web modules
- Availability – Load balancing, Internet devices as infrastructure

Conclusions

- Technical viability of secure outsourced processing has been proven
- Limitation – verifiable computation (ongoing research)
- Economic viability of the platform – left as future work
- Fully Homomorphic Encryption – evolving and preparing for the future (Hardware acceleration, quantum)

Thank you!

Questions?