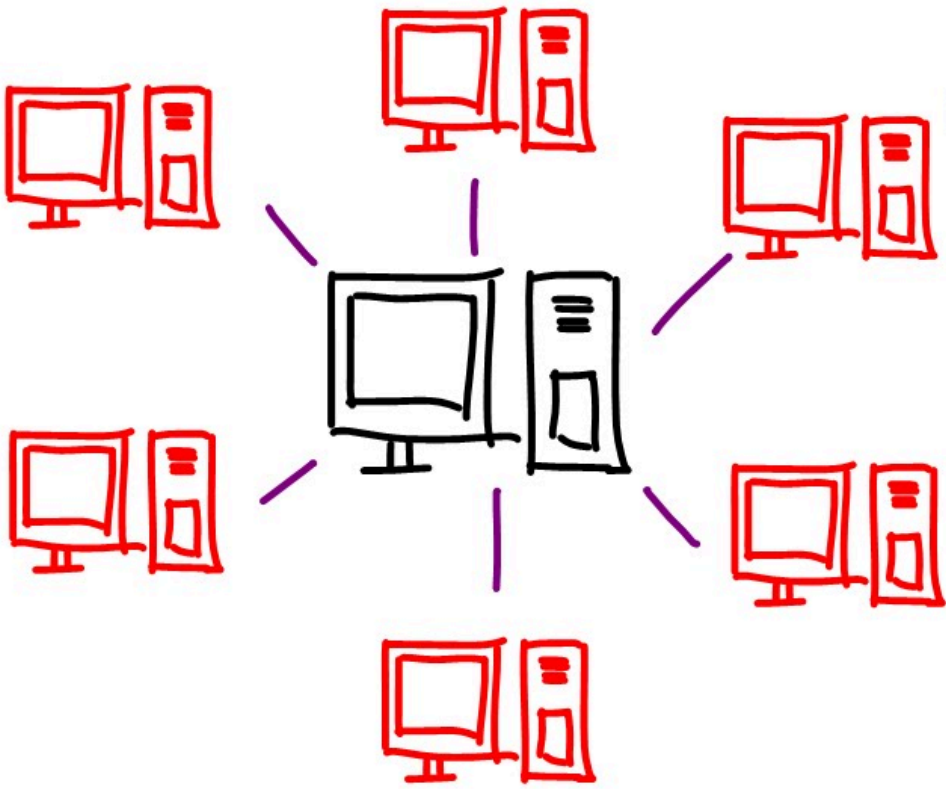
Distributed computing
Project Plan
Group C



Members

Evgeni Kurtev
Stefan-Nikola Stanev
Nikolay Gruychev
Vlad Bucur
Renis Hila
Naadir Twahir
Thomas Vasanth

Table of contents:

Members **1**
Table of contents: **2**
1. Problem Definition **3**
1.1. Problem to solve 3
1.2 Goals 3
1.3 Scope 3
1.4 Research Questions and Sub questions 3
1.5 Research Strategies to be used (Refer to The Research Framework, see below) 4
1.6 Deliverables 4
2. Team division of tasks **5**
3. Activities and Scheduling **5**
4. Test Environment **5**
5. Risks **5**

1. Problem Definition

1.1. Problem to solve

The problem we are trying to solve with our project is to make code uploading and distributing easier, more optimized, and overall better. We will try to automate the process of submitting and maintaining code most securely and practically.

1.2 Goals

The goal is to construct a secure environment that will distribute user-inputted code to multiple computing nodes while using security techniques such as digital signing to ensure the validity and security of information transmitted between the computing nodes and the master process.

1.3 Scope

We are going to create a way for people to deploy their code in a secure,scalable and managed environment. Our focus will be mainly on securing and making automation processes more private. However, we will still do all of the client's requirements and demands.

1.4 Research Questions and Sub questions

Our main research question will be:

What are the best practices for deploying, monitoring, and managing Kubernetes-based distributed systems to ensure security and performance?

And our sub questions are the following:

- How can we design an efficient deployment strategy for Kubernetes clusters that considers factors such as resource utilization, scalability, and fault tolerance?
- What are the recommended security configurations and controls for securing Kubernetes clusters, including access control, network policies, and container runtime security?
- What role does compliance management play in ensuring that Kubernetes-based distributed systems meet regulatory requirements and industry standards for security and data protection?
- what encryption mechanisms should be used in this project

1.5 Research Strategies to be used

- *Experimental Research*
    - *Design controlled experiments to compare the performance of different communication mechanisms within a Kubernetes cluster.*

- *Survey Research:*
    - *Collect feedback from practitioners and experts in the field to understand their experiences and preferences regarding communication strategies in Kubernetes.*

- *Case Study Research:*
    - *Investigate real-world implementations of Kubernetes clusters in organizations to examine how they handle information distribution and communication challenges.*

- *Action Research:*
    - *Collaborate with industry partners or open-source communities to implement and evaluate new communication protocols or tools in Kubernetes environments, iteratively refining the approaches based on feedback and observations.*

1.6 Deliverables

- K8s cluster with a container environment that runs the sent code.
- A way to automatically manage the amount of nodes and pods.
- Encrypted communication between the master node and the worker node
- HTTPS web server that hosts an application where the users can login and submit their code.
- CI/CD pipeline for code changes that updates the code in the specific pods.

2. Team division of tasks

We are going to split into smaller groups because we are 7 people and it is pretty hard to manage 7 individual tasks. Also we have a team leader that will track each sub group's progress and also he will assign and reassign tasks to the different members. The team leader of our group is Evgeni ,but later we can change the leader depending on the situation.

3. Activities and Scheduling

Date				
10/03/2024	*Create a draft of the project plan*	*Write down plans for the company pen test*	*Submit the Security Observation slides*	*Client Interview results*
29/03/2024	*Create A detailed project plan*	*The company to be pen-tested*	*Results from stakeholder's interviews*	*Interpretation of the indicated NIST and Additional Requirements*

4. Test Environment

We are going to use testing before every project change to ensure that the security and the solution we're going to provide would be at it's best. It is yet to be determined what kind of testing environment we'll use since we need to do a bit more researching before that. Refer to the design document for more technical details.

5. Risks

- Client not available
- Teammate(s) not available
- Netlab not available
- Project not matching the final requirements
- The team is running late with the submission
- Poor communication/misunderstandings occur within group / with client