Politechnika Wrocławska

# Aplikacje internetowe i rozproszone - Projekt

# Temat projektu

**Temat:** Sprawdzenie czy zadany zbiór zaszyfrowanych haseł może (i w jakim czasie) zostać złamany za pomocą komputera równoległego, jakim jest klaster stacji roboczych.

# Zakres projektu

W ramach projektu zrealizowany został system udostępniający usługę zlecenia zadania obliczeniowego (łamania hasła) za pomocą przeglądarki internetowej. W skład systemu wchodzą następujące komponenty:

- Aplikacja kliencka do zlecania zadań przez użytkowników
- Serwer aplikacji
- Aplikacja równoległa wykonująca obliczenia

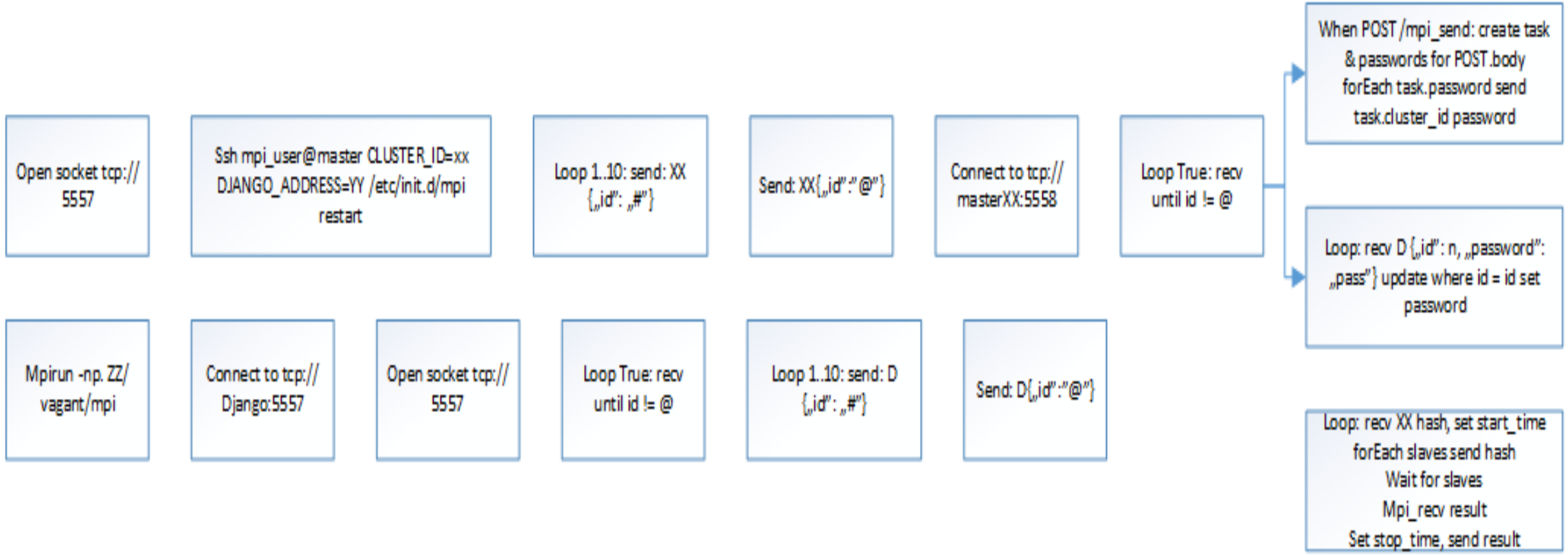
# Wykorzystane technologie - aplikacja kliencka

- Python 3.4 + python3-pika 0.9.14
- Django 1.7.2 + paramiko 1.15.2 + pyzmq 14.5.0
- HTML5
- jQuery 2.1.3
- jQGrid 4.7.1
- Bootstrap 3.3.4

# Wykorzystane technologie - aplikacja równoległa

- C++ 11
- ZeroMQ 4.1
- OpenMPI 1.8.5
- Vagrant 1.7.2

# Komunikacja między modułami



# Łamanie haseł

System potrafi łamać hasła szyfrowane przy użyciu dwóch metod szyfrowania:

- SHA1
- MD5

Do łamania haseł użytkownik może użyć trzech metod:

- Metoda słownikowa
- Metoda tablic tęczowych
- Metoda „Brute Force”

# Wydajność

Jak pokazały przeprowadzone testy wydajnościowe dzięki rozdzieleniu obliczeń pomiędzy różne maszyny udało się uzyskać około 300%-owy skok wydajności w porównaniu do pojedynczej maszyny.

Ziarnistość określa jak zadanie jest dzielone na podzadania (duża ziarnistość - duża liczba podzadań)