

# Decentralized Chat

Alan Wilms, Yunhua Zhao





# Overview

- Decentralized chat application using Python
- Libraries used:
  - curses - UI
  - rsa - encryption
  - etcd - messages & metadata distributed storage
  - cryptography - aes encryption

```
1 import subprocess
2 import os
3 import time
4 import errno
5 import rsa
6 from cryptography.fernet import Fernet
7
8
9 class EtcdChatLib:
10     def __init__(self, private_ip):
11         self.etcd_dir = os.path.expanduser("~/etcd/bin/")
12         self.chat_dir = os.path.expanduser("~/group-project-NOP/")
13         self.endpoints = [private_ip + ":2380"]
14         self.private_keys = {}
15         self.public_keys = {}
16
17     def add_endpoint(self, ip_addr):
18         self.endpoints.append(ip_addr + ":2380")
19
20     def get(self, key):
21         val = subprocess.check_output([self.etcd_dir + "etcdctl", "--endpoints=" +
22             if len(val.split("\n")) < 2:
23                 return None
24                 return val.split("\n")[1]
25
26     def put(self, key, val):
27         status = subprocess.check_output([self.etcd_dir + "etcdctl", "--endpoints=" +
28             if status.strip() != "OK":
29                 raise LookupError("Database seems to be down!")
30
31     def get_chatrooms(self):
32         '''Get list of chatrooms from etcd instance'''
33         val = self.get("meta/chatrooms")
34         if not val:
35             return []
36         return val.split("/")
37
38
39 import etcd
40 import sys
41 import time
42 import threading
43 import curses
44
45 from curses import textpad
46 from etcd_chat_lib import EtcdChatLib
47
48 class DecentralizedChat:
49     # defines several class variables
50     def __init__(self, screen):
51         self.db = EtcdChatLib("172.31.92.266")
52         self.db.add_endpoint("172.31.91.28")
53         self.db.add_endpoint("172.31.93.186")
54         self.db.add_endpoint("172.31.88.229")
55         self.db.add_endpoint("172.31.84.98")
56         self.username = None
57         self.chatroom = None
58         self.screen = screen
59         self.window_width = curses.COLS
60         self.window_height = curses.LINES
61         self.box = None
62         self.view = None
63
64     # sets up the initial username and chat selection
65     def setup(self):
66         self.screen.immedok(True)
67         curses.init_pair(1, curses.COLOR_BLACK, curses.COLOR_WHITE)
68         self.screen.addstr(" WELCOME TO DECENTRALIZED CHAT! \n\n", curses.color_pair(1))
69
70         self.print_status("Please type your username and then press ENTER.\n", False)
71         self.clear_box()
72         self.box.edit()
73         self.username = (self.box.gather()).strip()
```



# Features

- Group and two-person chats
- Room joining permission system via encryption
- Fully stored chat history
- Highly resilient
- Modular, extensible code

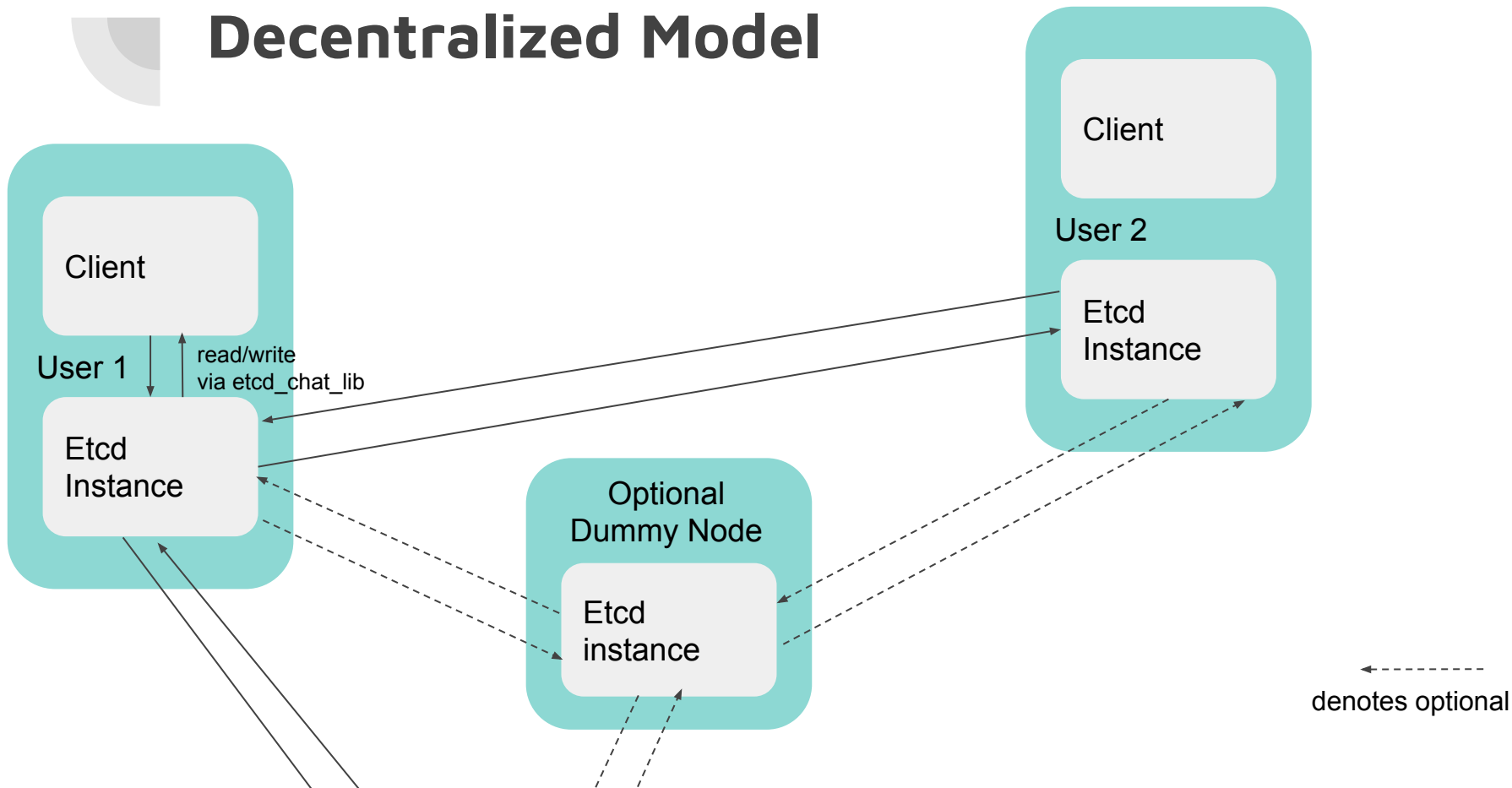
```
AlanWilms — ubuntu@ip-172-31-80-225: ~/group-project-NOP/src — ssh -i rdc_key_pair.pem ubuntu@ec2-100-26-188-167...
...pair.pem ubuntu@ec2-107-23-52-16.compute-1.amazonaws.com ... ..em ubuntu@ec2-100-26-188-167.compute-1.amazonaws.com
ROOM: Test

<admin> User Alan would like to join! Please type "!Alan" to accept
<admin> User Alan accepted by Yunhua.
<admin> User Sally would like to join! Please type "!Sally" to accept
<admin> User Sally would like to join! Please type "!Sally" to accept
<admin> User Sally accepted by Alan.
<Sally> Hi!
<Sally> Hello there!
<admin> User Alanman would like to join! Please type "!Alanman" to accept
<admin> User Alanman would like to join! Please type "!Alanman" to accept
<admin> User Alanman would like to join! Please type "!Alanman" to accept
<admin> User Alanman accepted by Alan.
<Alan> who are you
<Alanman> you
<Yunhua> and why is your name Alanman
<Yunhua> excuuuuuse me
<Alanman> bye
<Alan> uh huh
<Alan> that's
<Sally> funny?

Type and press ENTER to send a message.
```



# Decentralized Model





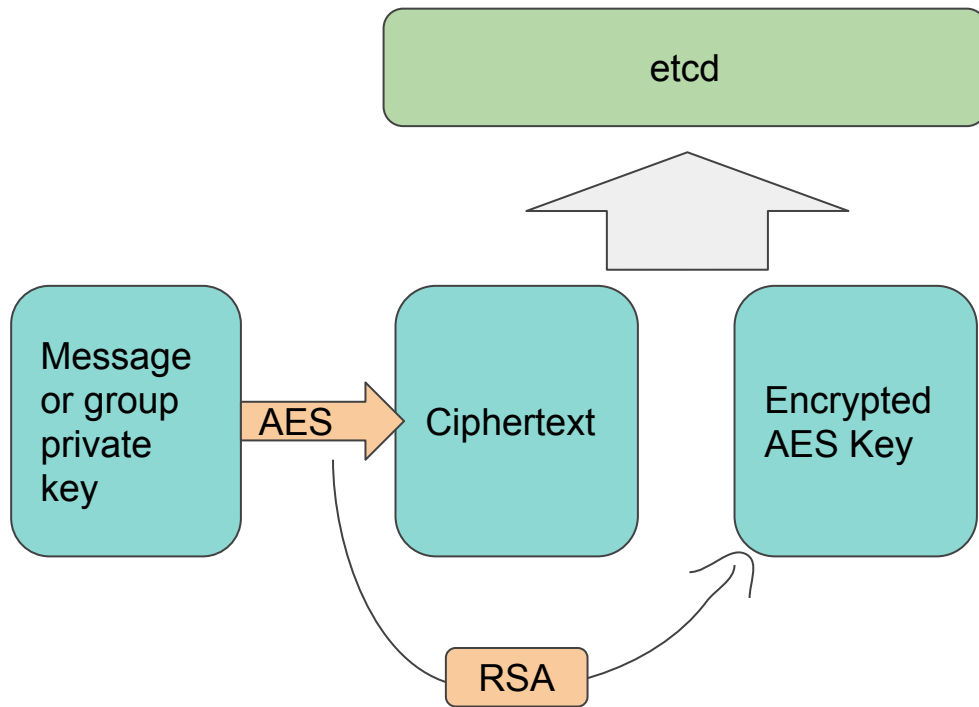
**Demo!**



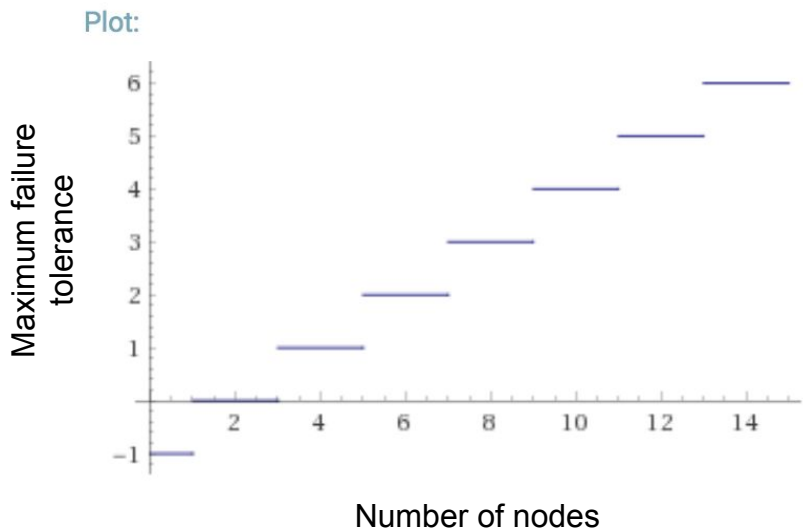
# Encryption

ROOM: Demo

```
<admin> User Demo3 would like to join! Please type "!Demo3" to accept
<admin> User Demo2 would like to join! Please type "!Demo2" to accept
<admin> User Demo4 would like to join! Please type "!Demo4" to accept
<admin> User Alan would like to join! Please type "!Alan" to accept
<admin> User Alan accepted by Yunhua.
<admin> User Demo2 accepted by Yunhua.
<Alan> Hello!
<admin> User Demo3 accepted by Yunhua.
<Alan> How is everyone doing?
<admin> User Demo4 accepted by Alan.
```



# Resiliency



```
RDC — ubuntu@ip-172-31-84-98: ~/group-project-NOP — ssh -i rdc_key_pair.pem ubuntu@ec2-18-234-20...
ream Message writer)
2018-12-14 09:48:52.117287 I | rafthttp: stopped streaming with peer b95006fe15a73ee (writer)
2018-12-14 09:48:52.117398 I | rafthttp: stopped HTTP pipelining with peer b95006fe15a73ee
2018-12-14 09:48:52.117495 W | rafthttp: lost the TCP streaming connection with peer b95006fe15a73ee (stream Message v2 reader)
2018-12-14 09:48:52.117543 E | rafthttp: failed to read b95006fe15a73ee on stream MsgApp v2 (context canceled)
2018-12-14 09:48:52.117581 I | rafthttp: peer b95006fe15a73ee became inactive (message send to peer failed)
2018-12-14 09:48:52.117642 I | rafthttp: stopped streaming with peer b95006fe15a73ee (stream MsgApp v2 reader)
2018-12-14 09:48:52.117725 W | rafthttp: lost the TCP streaming connection with peer b95006fe15a73ee (stream Message reader)
2018-12-14 09:48:52.117801 I | rafthttp: stopped streaming with peer b95006fe15a73ee (stream Message reader)
2018-12-14 09:48:52.117858 I | rafthttp: stopped peer b95006fe15a73ee
2018-12-14 09:48:52.118738 E | rafthttp: failed to find member c0a0a03515123294 in cluster 7cb149031198992b
2018-12-14 09:48:52.119041 E | rafthttp: failed to find member 851474a6ca7a0cc8 in cluster 7cb149031198992b
2018-12-14 09:48:52.119249 E | rafthttp: failed to find member 851474a6ca7a0cc8 in cluster 7cb149031198992b
2018-12-14 09:48:52.119471 E | rafthttp: failed to find member c0a0a03515123294 in cluster 7cb149031198992b
2018-12-14 09:48:52.119707 E | rafthttp: failed to find member b95006fe15a73ee in cluster 7cb149031198992b
2018-12-14 09:48:52.119908 E | rafthttp: failed to find member b95006fe15a73ee in cluster 7cb149031198992b

ubuntu@ip-172-31-84-98: ~/group-project-NOP$

ROOM: Demo

<Alan> 5
<Alan> 4
<Alan> 3
<Alan> 2
<Alan> 1
<Alan> 1
<admin> User Demo1 accepted by Yunhua.
<Alan> 1
<Alan> 2
<Demo1> Scroll
<Demo1> **Scroll
<Demo4> Scroll
<Demo1> Before killing local ETCD instance
<Demo1> After killing local ETCD instance
<Demo4> Killed a second ETCD instance, so only 3 out of 5 members of the cluster are still running

Type and press ENTER to send a message.

The local instance on this machine was the one killed
```



# Future Improvements

- More robust login system
  - with password to avoid spoofing
- Improved features
  - UI: escape, back commands
  - Functionality: ability to kick someone form a chat
- Better discovery capabilities