DAYANANDA SAGAR COLLEGE OF ENGINEERING
(An Autonomous Institute affiliated to VTU, Belagavi, Approved by AICTE & ISO 9001:2008 Certified)
Accredited by National Assessment & Accreditation Council (NAAC) with 'A' grade,
Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru-560078.

MINI-PROJECT

On

"Fingerprint based fraud detection Voting system"

BACHELOR OF ENGINEERING
IN
INFORMATION SCIENCE AND ENGINEERING

Submitted by

NISARGA K (1DS20IS065)

NITHYA M (1DS20IS067)

SAIJYOTI G M (1DS20IS085)

SANJANA GOUD (1DS20IS092)

Under the guidance of

Dr Chandrakala B M
Associate Professor

Department Of Information Science and Engineering
DAYANANDA SAGAR COLLEGE OF ENGINEERING
S M Hills, Kumara Swamy Layout, Bengaluru-560078

2022-23

CONTENTS

Abstract

The fingerprint-based fraud detection voting system is a project that aims to address the inefficiencies and vulnerabilities in the current voting system by introducing an innovative approach to voting authentication and fraud prevention. Traditional voting systems often rely on identification cards, which can be susceptible to duplication and misuse. In this project, we propose a solution that utilizes biometric fingerprint recognition technology to authenticate voters, ensuring secure and reliable voting processes. The system involves the development of an online voting machine equipped with a fingerprint reader. During the registration process, voters' fingerprints are stored as unique identifiers. On the day of voting, the fingerprint reader acquires the voter's fingerprint and compares it with the pre-stored data to verify their identity. This eliminates the need for physical identification cards and reduces the risk of fraudulent activities. To maintain voter anonymity, the system assigns each user a unique and random ID, ensuring no connection to their personal details. The interface of the voting machine is designed to be user-friendly and intuitive, prioritizing clear visual representation of data and basic functionalities. This enables voters to cast their votes easily and confidently, enhancing the overall voting experience. The fingerprint-based fraud detection voting system offers several advantages over traditional methods. It significantly reduces the risk of voter fraud by relying on the uniqueness of fingerprints, which are difficult to forge or manipulate. Moreover, it eliminates the need for voters to carry identification cards, streamlining the voting process and reducing the chances of lost or stolen cards. Through this project, we aim to contribute to the improvement of voting systems, ensuring fairness, accuracy, and transparency in the electoral process. By leveraging the power of biometric fingerprint technology, we can enhance the security and integrity of voting, fostering trust among voters and promoting

Chapter 1

Methodology

Proposed Technique

- Requirements Analysis: Identify the key requirements and objectives of the voting system. Define the necessary features, such as fingerprint authentication, fraud detection, and real-time result generation.Consider the constraints, such as budget, time, and available resources.

- System Design:Design the overall architecture of the voting system, including hardware and software components.Specify the roles and responsibilities of each component, such as the fingerprint sensor, microcontroller, LCD display, and database.Determine the communication protocols and interfaces between different components.

- Hardware Implementation:Select the appropriate hardware components, such as Arduino or similar microcontrollers, fingerprint sensors, LCD displays, and power supply.Connect and integrate the hardware components according to the system design.Test the hardware setup for functionality and reliability.

- Software Development:Develop the software code for the microcontroller to handle fingerprint authentication, fraud detection algorithms, and data processing.Implement a user-friendly interface on the LCD display to guide voters and display relevant information.Integrate the software with the hardware components for seamless operation.

- Fingerprint Enrollment:Develop a mechanism for enrolling eligible voters' fingerprints into the system's database.Assign a unique identifier or ID to each voter to ensure anonymity.Store the enrolled fingerprints securely to prevent unauthorized access.

- Authentication and Voting Process:Capture the fingerprint of a voter using the fingerprint sensor during the voting process.Compare the captured fingerprint with the enrolled fingerprints in the database for authentication.If the fingerprint matches, allow the voter to cast their vote using push buttons or similar input methods.Implement measures to prevent duplicate voting, such as tracking the already cast votes.

- Fraud Detection:Implement fraud detection algorithms to identify any suspicious activities or attempts at tampering with the voting process.Monitor for anomalies, such as multiple attempts by the same voter or unusual patterns in voting behavior.Raise alerts or take appropriate actions if fraudulent activities are detected.

- Result Generation and Reporting:Calculate the voting results based on the cast votes.Display the real-time voting statistics on the LCD display for transparency.Generate comprehensive reports of the voting process and results for auditing purposes.

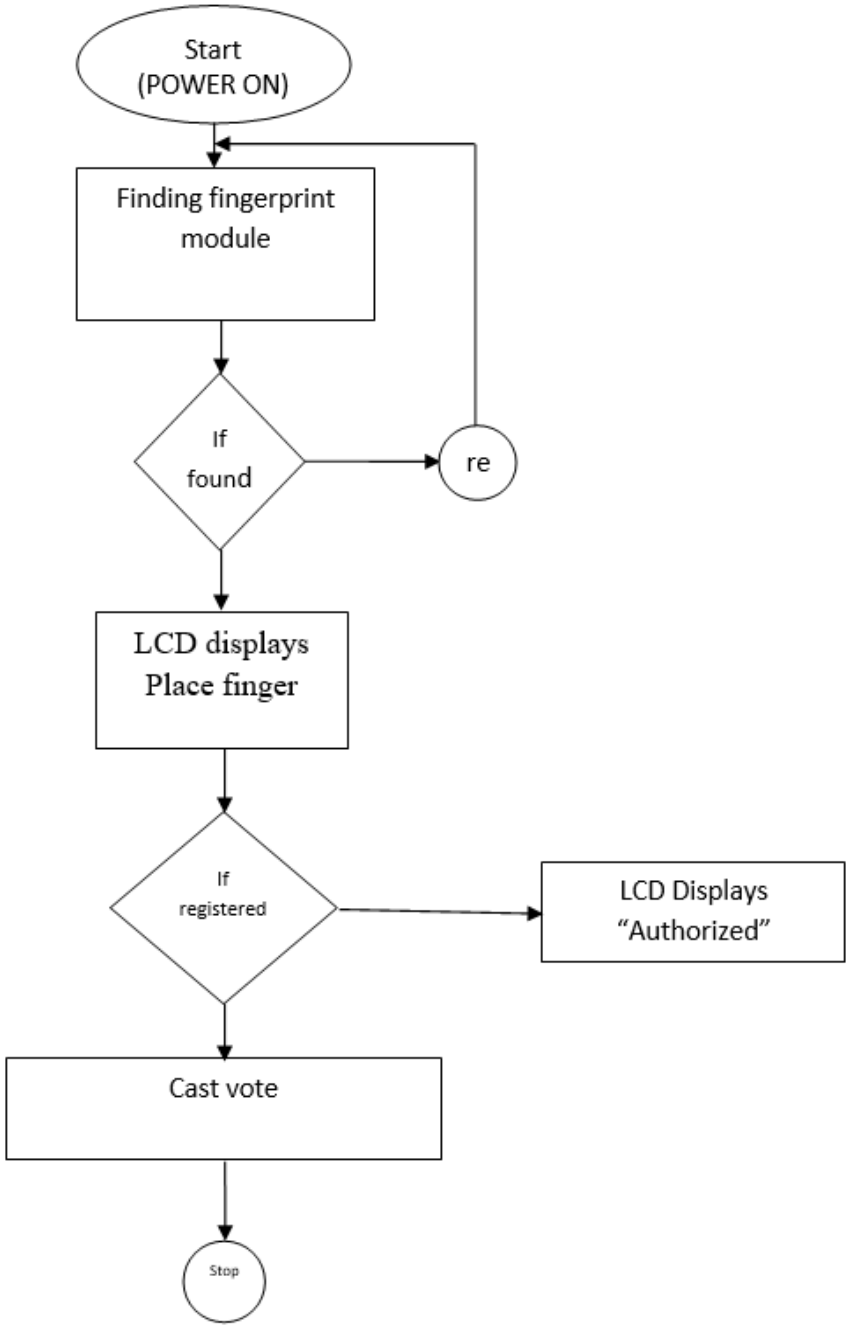
- Testing and Evaluation:Conduct thorough testing of the entire system to ensure its functionality, accuracy, and reliability.Perform usability testing to assess the user experience and identify areas for improvement.Collect feedback from users and stakeholders to refine the system.

- Deployment and Maintenance:Deploy the fingerprint-based voting system in the targeted environment, such as polling stations or institutions.Provide necessary training and support to users and administrators.Establish a maintenance plan to address any issues, update the system as needed, and ensure its continued operation.Throughout the project, it is crucial to follow ethical guidelines, adhere to legal requirements, and prioritize data security and privacy to maintain the integrity of the voting system.

Project flow:

- Initially the voters should register their fingerprint with the voting system by placing their finger on the fingerprint reader.
- After registering the fingerprints of different voters, the voting process is conducted further.
- The voter enters the ballot room, places his fingerprint on the fingerprint module to identify his details and if it matches with the details given during registration, he is further allowed to cast his vote
- If the fingerprint matches with the already registered fingerprint, the LCD will display that the voter is authorized.
- Candidate options are given to the voter, and he is allowed to vote for the candidate whom he decides to cast his vote for.
- If a voter is voting for the first time, they can vote without any interruption. However, if the voter attempts to vote for the second time, the buzzer will signal an alert.
- At the end, the admin can view the results of the voting process.

1.2 Flowchart



Chapter 2
System Design

2.1 Existing System:

The existing system for fingerprint-based fraud detection in a voting system might involve traditional paper-based voting methods where individuals cast their votes by marking their preferences on paper ballots. This system typically relies on manual verification processes, such as signature verification or ID checks, to detect fraudulent activities. However, these methods are susceptible to human errors and can be easily manipulated, leading to potential voting fraud.with greater independence and confidence.

2.2 Proposed System:

The proposed system aims to address the limitations of the existing system by developing a smart wearable device specifically designed for visually impaired individuals. One key feature of the proposed system is the integration of a navigation mode that utilizes object detection and probability calculation to determine potential obstacles that could lead to collisions or accidents. This mode will provide immediate feedback to the user, ensuring they are aware of objects with a higher probability of crashing with them.

2.3 System Architecture:

The system architecture of a Fingerprint-based Fraud Detection Voting System can be structured as follows:

1. Fingerprint Sensor:
    - The Fingerprint Sensor is responsible for capturing the fingerprint of a voter during the authentication process.
    - It communicates with the Arduino Uno to transfer the captured fingerprint data.
2. Arduino Uno:
    - The Arduino Uno acts as the main controller of the system.
    - It receives the fingerprint data from the sensor and performs the necessary processing and authentication.
    - It controls the interaction with other components and manages the overall system operation.
3. LCD Display:
    - The LCD Display provides a user-friendly interface to guide voters and display relevant information.
    - It shows instructions, voting options, and real-time feedback to the users.
    - The Arduino Uno communicates with the LCD Display to update and display the required information.
4. Push Buttons:
    - Push Buttons are used as input devices for voters to cast their votes.
    - The Arduino Uno detects the button presses and processes them accordingly.
    - It ensures that each voter can cast only one vote and prevents duplicate voting.

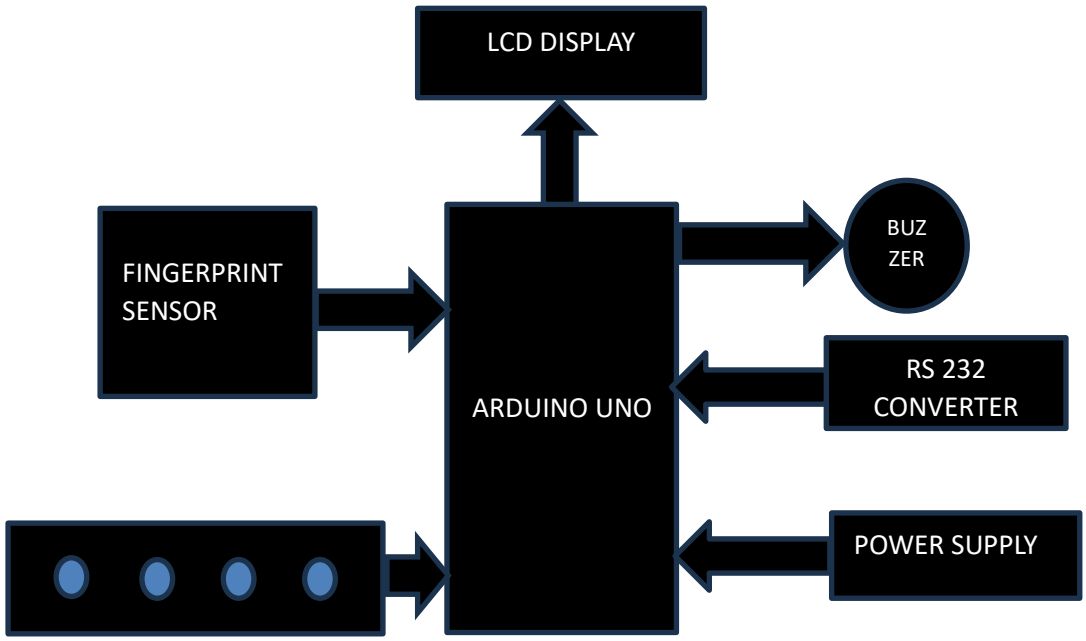
5. Fraud Detection Module:
    - The Fraud Detection Module contains algorithms and logic to detect any fraudulent activities during the voting process.
    - It monitors for anomalies, such as multiple attempts by the same voter or unusual patterns in voting behavior.
    - It raises alerts or takes appropriate actions if any fraudulent activities are detected.
6. Power Supply:
    - The Power Supply provides the necessary 12V DC power to the entire system.
    - It ensures stable and reliable power delivery to all components.
7. Serial Communication:
    - The Arduino Uno may utilize serial communication, such as UART or SPI, to interact with other modules or devices.
    - For example, it may communicate with a computer or external storage device to store and retrieve voting data.
8. Data Storage:
    - The system may include a storage mechanism, such as EEPROM or external memory, to store enrolled fingerprints, voting records, and other relevant data.
    - The Arduino Uno manages the storage and retrieval of data as needed during the voting process.
9. External Interface:
    - The system may provide an external interface, such as a USB port or RS-232 converter, for connecting with external devices or systems.
    - This interface can be used for data transfer, result reporting, or system configuration.

The overall system architecture revolves around the Arduino Uno, which acts as the central control unit. It interfaces with the Fingerprint Sensor, LCD Display, Push Buttons, Fraud Detection Module, Power Supply, and other components to ensure secure and reliable fingerprint-based voting with fraud detection capabilities.

Implementation

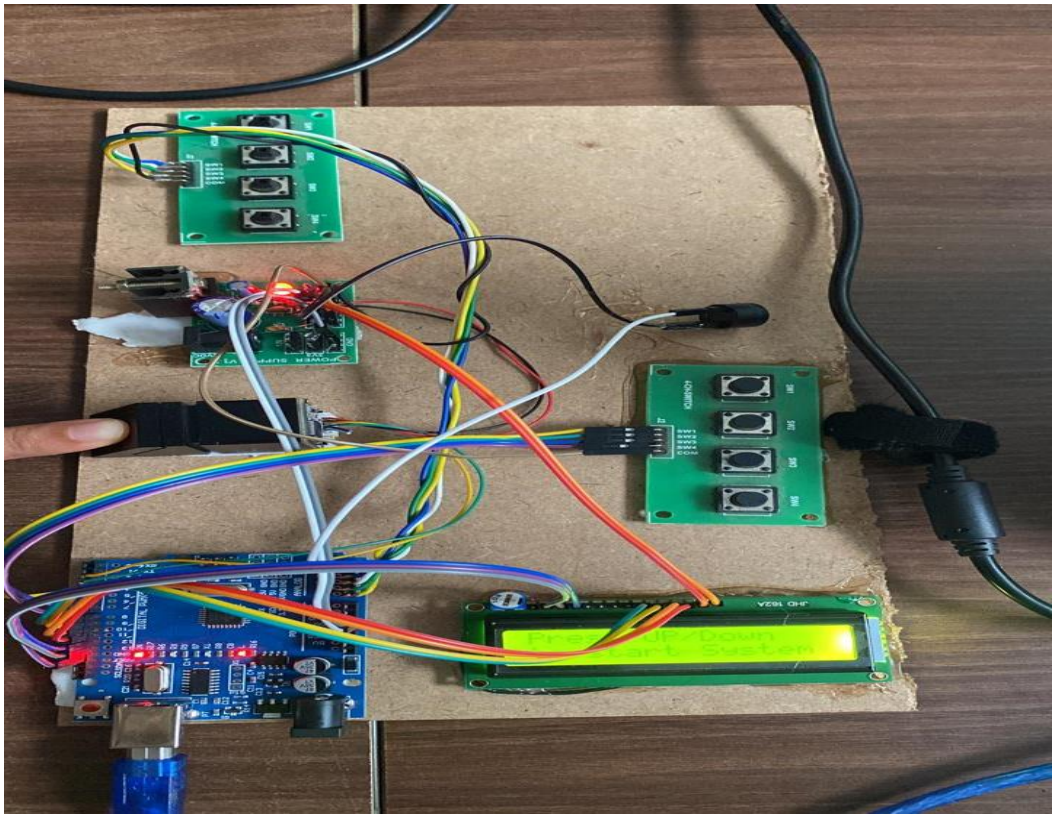
```
void Enroll()
{
int count=0;
lcd.clear();
lcd.print("Enter Finger ID:");
while(1) {
lcd.setCursor(0,1);
lcd.print(count);
if(digitalRead(up) == 0) {
     count++;
if(count>25)
 count=0;
delay(500);
}

else if(digitalRead(down) == 0) {
count--;
 if(count<0)
count=25;
delay(500);
}
else if(digitalRead(del) == 0) {
id=count;
getFingerprintEnroll();
for(int i=0;i<records;i++){
 if(EEPROM.read(i+10) == 0xff){
   EEPROM.write(i+10, id);
          break;
}
}
return;
else if(digitalRead(enroll) == 0)
            return;
```

Block Diagram

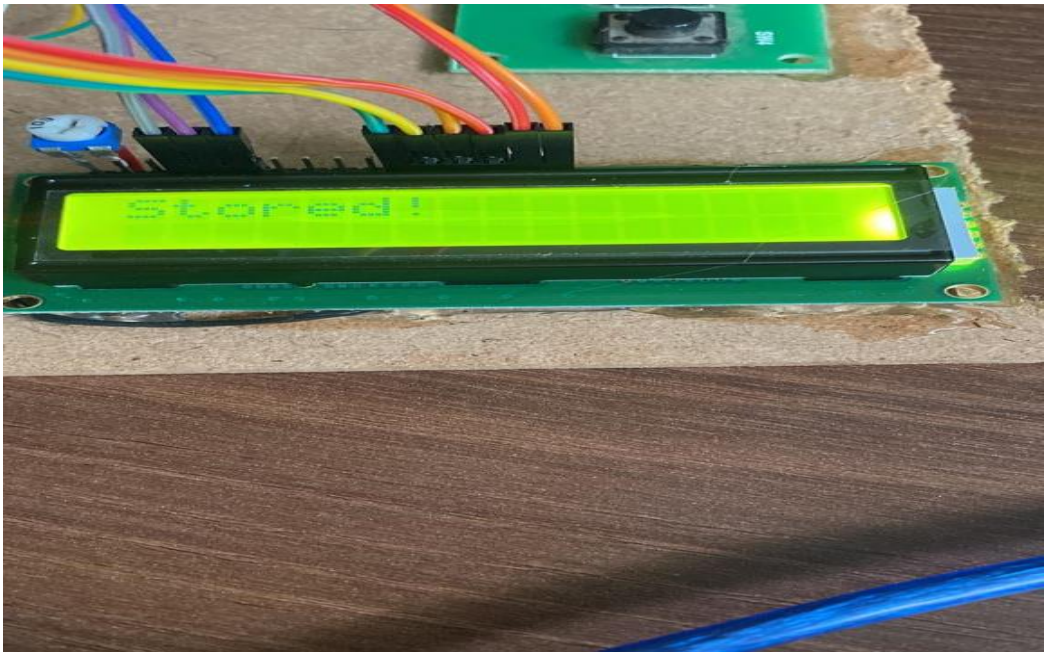


Results

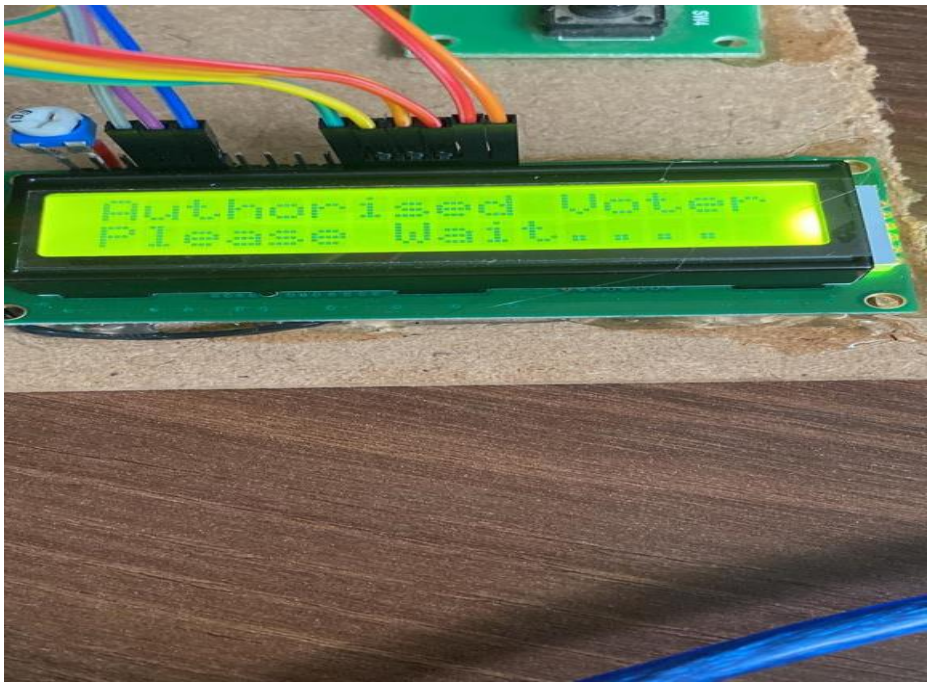
Overall system:



Enrollment:



Real-time Fingerprint Matching:



Voting interface:

Conclusion

In conclusion, the implementation of a fingerprint-based fraud detection voting system offers significant advancements in the security and integrity of the voting process. By leveraging the unique biometric characteristics of fingerprints, this system ensures accurate identification of voters and effectively detects fraudulent activities. Through the development and integration of fingerprint enrolment, real-time matching, fraud detection mechanisms, and a user-friendly interface, the voting system provides a robust solution. It enables authorized voters to cast their vote seamlessly while preventing unauthorized individuals from participating multiple times. The system's ability to integrate with existing voter registration databases further enhances its effectiveness and reliability. The administrator's access to comprehensive result analysis and reporting facilitates informed decision-making and ensures transparency in the electoral process. Through rigorous testing and evaluation, the system's functionality, accuracy, and security are validated, instilling confidence in its performance. Once deployed, ongoing maintenance and support are essential to ensure the system's continuous operation and adaptability to evolving needs. Overall, the fingerprint-based fraud detection voting system addresses the critical challenges of voter authentication and fraud prevention. Its successful implementation significantly contributes to fair and trustworthy elections, safeguarding the democratic principles of transparency, accuracy, and inclusivity.

References

[1] Signals, Systems and Computers, 2004 Conference Record of the Thirty-Eighth Asilomar Conference on Publication 7-Nov-2004 Volume: 1, on page(s): 577-581 Vol.1.

[2] International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, October 2012.

[3] International Journals of Biometric and Bioinformatics, Volume (3): Issue (1).

[4] Mukesh Kumar Thakur, Ravi Shankar Kumar, Mohit Kumar, Raju Kumar "Wireless Fingerprint Based Security System using Zigbee" , International Journal of Inventive Engineering and Sciences (IJIES) ISSN: 2319–9598, Volume-1, Issue-5, April 2013.

[5] Mary Lourde R and Dushyant Khosla, "Fingerprint Identification in Biometric Security Systems", International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010.

[6] "Fingerprint Matching" by Anil K. Jain, Jianjiang Feng and Karthik Nandakumar, Department of Computer Science and Enginnering, Michign State University. About Authors:A.Aditya Shankaris a final year undergraduate student, Dept. Of Electronics and Communication Engineering from Dadi Institute of Engineering and Technology, Visakhapatnam,Andhra Pradesh. His main areas of interest are Sensor Technology, Analog and Digital Circuits, Embedded Systems andWireless Communication &Networking.