UNIMY
UNIVERSITY MALAYSIA OF COMPUTER SCIENCE & ENGINEERING

FINAL YEAR PROJECT PROPOSAL SUBMISSION FORM

Instructions

Students	**: Please complete section A, D and F**
Supervisor	**: Please complete section B**
Co-Supervisor	**: Please complete section C**
Evaluator	**: Please complete section E**

SECTION A : STUDENT INFORMATION

NAME **: Abdurrahman Noor-Ul-Haqq Gurib**
:

PROGRAM **Diploma in IT Cyber Security STUDENT ID: 001401**

SEMESTER **: Year 3 Semester 1**

PROJECT TITLE **: Secure Access Control (Enhancing Modern Voting through Cybersecurity Monitoring)**

SECTION B : SUPERVISOR CONSENT

I …… **agree/disagree*** to be the supervisor of the above mentioned name student in his/her Final Year Project course.

DATE : …… **SIGNATURE** **:** ……

OFFICIAL STAMP :

SECTION C : CO-SUPERVISOR CONSENT (*if applicable*)

I …… **agree/disagree*** to be the co-supervisor of the above mentioned name student in his/her Final Year Project course.

DATE : …… **SIGNATURE** **:** ……

OFFICIAL STAMP :

SECTION D : STUDENT DECLARATION

I hereby declare that this project is :

[✓] My own idea
[X] My supervisor's idea / topic

DATE : 29th of August 2023 **SIGNATURE** **:** ……

SECTION E : EVALUATION PANEL

OUTCOME [ ] Full Approval
[ ] Conditional Approval (Minor)
[ ] Conditional Approval (Major)
[ ] Fail / Rejected

NOTE (Please state reasons for conditional / fail approval)

……..

……..

DATE : …….. PANEL SIGNATURE : ……

SECTION F : PROJECT DETAILS

Project Type **[✓] Development Track**
[✓] Research Track

Area **: Enhancing Modern Voting through Cybersecurity Monitoring**

Problem Background and Proposed Solution :

Problem Background:

- In recent years, the landscape of voting systems has been undergoing a significant transformation with the adoption of digital platforms. While this evolution brings convenience and accessibility to voters, it also introduces a host of challenges related to security and transparency. Traditional paper-based voting methods, although time-consuming, have enjoyed a level of inherent security that digital voting systems often struggle to replicate.

- The digitalization of voting introduces vulnerabilities such as unauthorized access, tampering, and data breaches. Malicious actors can exploit these vulnerabilities to manipulate voting outcomes, eroding the very foundation of democratic processes. Additionally, concerns arise about voter data privacy and the need to guarantee the authenticity and integrity of each vote cast.

Proposed Solution:

- To address these challenges, my project proposes a comprehensive solution that amalgamates modern voting processes with state-of-the-art cybersecurity practices. My goal is to create a secure and transparent digital voting ecosystem that instills confidence in both voters and the integrity of the electoral process.

My proposed solution involves the implementation of multi-faceted security measures:

1. Encryption: All voter data and ballots are encrypted, ensuring that even if intercepted, the information remains indecipherable to unauthorized parties.

2. Authentication: Rigorous user authentication mechanisms guarantee that only eligible voters can participate, minimizing the risk of fraudulent entries.

3. Real-time Monitoring: The introduction of real-time monitoring tools enables the identification of anomalous activities and potential threats as they occur, allowing immediate response and intervention.

4. Auditing and Traceability: The entire voting process is meticulously logged, creating an audit trail that tracks every action, from voter registration to ballot submission and result declaration.

5. Data Integrity Measures: Measures to maintain the integrity of voter data and voting results, such as digital signatures and checksums, are employed to ensure that no tampering has occurred.

6. Transparency: By providing stakeholders access to the auditing logs and results, transparency is enhanced, and trust is fostered among voters, electoral authorities, and observers.

Objectives :

The objectives of the project my project are as follows:

1. Enhance Security: Develop and implement a robust cybersecurity framework to safeguard the integrity, authenticity, and confidentiality of the digital voting process.
2. Prevent Manipulation: Implement encryption and authentication measures to prevent unauthorized access, tampering, and manipulation of votes and voter data.
3. Real-time Monitoring: Integrate real-time monitoring tools to detect and respond to anomalies, ensuring the immediate identification of potential cybersecurity threats.
4. Transparent Audit Trail: Create an audit trail that records every step of the voting process, from voter registration to result declaration, ensuring transparency and accountability.
5. User Confidence: Build a secure and user-friendly digital voting platform that instills confidence in voters, encouraging their participation in the electoral process.
6. Data Privacy: Ensure the protection of voter data privacy by implementing robust data protection measures and adhering to relevant privacy regulations.
7. Usability: Develop an intuitive user interface that allows voters to cast their ballots easily and effectively, without compromising security.
8. Collaboration: Foster collaboration between cybersecurity experts, software developers, and electoral authorities to ensure a holistic approach to secure digital voting.
9. Scalability: Design the system to be scalable, accommodating larger voter populations without compromising security and performance.
10. Knowledge Sharing: Document the cybersecurity measures, processes, and lessons learned to contribute to the broader understanding of secure digital voting systems.
11. Future Adaptability: Design the system with flexibility in mind, allowing for the incorporation of new security techniques as the cybersecurity landscape evolves.
12. Alignment with Regulations: Ensure that the project adheres to relevant legal and regulatory frameworks related to digital voting, cybersecurity, and data privacy.

Scopes :

In-Scope:

1. Security Enhancement: Develop and implement a comprehensive cybersecurity framework to enhance the security of the digital voting system.
2. Encryption and Authentication: Integrate encryption and authentication mechanisms to protect voter data, ballots, and the overall voting process.
3. Real-Time Monitoring: Incorporate real-time monitoring tools to detect and respond to cybersecurity threats and anomalies in the voting process.
4. User Interface Design: Design an intuitive and user-friendly interface for voters to cast their ballots securely.
5. Audit Trail: Create a detailed audit trail that logs every step of the voting process, ensuring transparency and accountability.
6. Data Privacy: Implement measures to ensure the privacy and confidentiality of voter data in compliance with relevant regulations.

7. Documentation: Thoroughly document the cybersecurity measures, processes, and design decisions for future reference and knowledge sharing.

8. Usability Testing: Conduct usability testing to ensure that the digital voting platform is accessible and usable for all voters.

Out of Scope:

1. Physical Voting Infrastructure: The project does not involve the physical setup of voting machines or polling stations.

2. Legislative Changes: The project does not encompass changes to existing voting laws or regulations.

3. External Threats: While the project addresses cybersecurity threats, it does not aim to eliminate broader external threats such as voter coercion or misinformation.

4. Voter Registration: The project does not cover the entire voter registration process but focuses on securing the voting process after registration.

Project Requirements :

Software :

Secure Access:
Users must log in securely using strong passwords or other methods.
Only authorized users should access the system.

Voting Functionality:
Users should be able to choose candidates and submit votes.
The system must accurately record and store votes.

Real-Time Monitoring:
The system should watch for any unusual activities during voting.
If something suspicious happens, it should alert administrators.

Data Protection:
Voter data and votes must be encrypted to prevent unauthorized access.
Only authorized personnel should have access to the data.

Audit Trail:
The system should keep a detailed record of every action taken during voting.
This helps track and verify the voting process.

User-Friendly Interface:
The user interface should be easy to understand and navigate.
Voters should be able to cast their votes without confusion.

Compatibility:
The system should work well on various devices and browsers.

Integration:
Different parts of the system should work smoothly together.
Frontend and backend components must communicate seamlessly.

Clear Documentation:
Provide user manuals for voters and technical documentation for developers.
This ensures that everyone understands how to use and maintain the system.

Privacy Compliance:
The system must adhere to data privacy regulations and protect voter information.

Hardware :

Servers:
Powerful computers to host the digital voting platform.
Should have enough storage and processing power to handle voter data and transactions.

Networking Equipment:
Routers, switches, and cables to connect the servers and users.
Stable and secure network connections are essential for smooth operation.

Firewalls and Security Devices:
Tools to protect the servers and data from cyber threats.
Firewalls block unauthorized access, and security devices monitor for suspicious activities.

Backup Systems:
Backup servers or cloud storage to ensure data is safe in case of hardware failures.

User Devices:
Devices such as laptops, tablets, or smartphones that voters will use to access the digital voting platform.

Printing Devices:
Printers to produce hard copies of voting receipts or documents.

Physical Security Measures:
Secure facilities to house the servers and networking equipment.
Measures to prevent unauthorized physical access.

Power and Redundancy:
Reliable power sources and backup generators to ensure continuous operation.
Redundant hardware to minimize downtime in case of failures.

Cooling Systems:
Cooling equipment to prevent servers from overheating.

*To attach Gantt chart and task distribution

Task	Duration	Start Date
Project Kickoff	1 week	June 1
Requirements Gathering	2 weeks	June 7
Analysis	2 weeks	June 14
Design	3 weeks	June 28
Development	6 weeks	July 12
Security Integration	3 weeks	August 2
Testing	4 weeks	August 16
User Acceptance Testing	2 weeks	August 16
Documentation	1 week	August 20
Final Review	1 week	August 27
Project Completion	-	August 30