COSC2539 Assignment 3 Instruction Document

Overview

Assignment 3 in COSC2539 focuses on group research and presentation in the field of security and privacy. It is divided into two main parts: a research paper and a presentation, each with distinct requirements and objectives.

Tasks and Questions

Q1: Research Security Research Paper IEEE Format (70 Marks)

1. **Task Description**: Conduct group research in a security and privacy-related area. Propose a topic for approval and then write a research paper.
2. **Part 1 - Topic Proposal (10 Marks)**:
    - **Content**: Write a one-page proposal including the chosen topic, plan for completion, and a change log for any significant adjustments.
    - **Due Date for Rough Draft**: December 21st, 2022.
    - **Appendix Requirement**: Attach the proposal and changes to the Appendix of your paper.
3. **Part 2 - Research Report (60 Marks)**:
    - **Report Structure**: Should include Introduction, Literature Review, System Specifications (if necessary), Methodology for Analysis, Results and Discussion, Conclusion, References, and Appendix.
    - **Length and Format**: 6 pages using the IEEE template, with at least 15 references (10 from academic journals).
    - **Sources**: Use Google Scholar, IEEEXplore, or RMIT Vietnam Library for research.

Q2: Presentation (30 Marks)

1. **Task Description**: Prepare and deliver a presentation based on the research paper.
2. **Presentation Details**:
    - **Duration**: Each group member must present for 3 minutes. For example, a team of 5 should present for 15 minutes in total.
3. **Team Contribution Declaration**:
    - **Requirement**: Submit a contribution declaration form signed by all members, indicating each member's involvement in the project.
    - **Grading**: Individual contributions and grades will be adjusted based on this form.

Guide for Q1: Research Security Research Paper IEEE Format

Outline

Part 1: Topic Proposal (One Page)

Title

"Enhancing Electoral Security and Privacy: A Comprehensive Approach"

Introduction

- Briefly introduce the importance of security and privacy in elections.
- State the objective of the research.

Rationale for Topic Selection

- Explain the significance of the topic in the current global context.
- Discuss the impact of digital technologies on electoral processes.

Plan for Completion

- Team Members and Roles:
  - List each team member and their specific responsibilities.
- Milestones:
  - Provide a timeline of key milestones leading up to the submission of the final paper.
- Change Management:
  - Explain the procedure for documenting any significant changes to the proposal.

Expected Outcomes

- Briefly describe what the research aims to achieve or propose.

Appendix Mention

- Note that the final proposal and change log will be included in the Appendix of the final paper.

Sample for Topic Proposal

Project Proposal for Security Research Paper

Title:

"Enhancing Electoral Security and Privacy in Digital Voting Systems"

Introduction:

In the age of digital transformation, the integrity and confidentiality of electoral processes have become increasingly vulnerable to cyber threats. This proposal outlines our plan to research and develop a comprehensive security and privacy framework for digital voting systems, aiming to bolster electoral integrity and voter confidence.

Rationale for Topic Selection:

Our choice of this topic is driven by the growing concerns over electoral interference and data breaches in digital voting systems worldwide. The democratic process hinges on the security and trustworthiness of voting systems. Addressing these concerns is not only timely but critical to preserving the foundation of democratic societies.

Objectives:

- To analyze the current landscape of digital voting systems' security and privacy.
- To identify and assess prevalent vulnerabilities and attack vectors.
- To propose a comprehensive security and privacy framework tailored for digital voting systems.

Plan for Completion:

- **Team Composition and Responsibilities**:
    - **Alice Nguyen (Project Coordinator)**: Oversee project progress and ensure milestones are met.
    - **John Smith (Research Lead)**: Conduct a comprehensive literature review and data analysis.
    - **Maria Garcia (Technical Analyst)**: Focus on current technologies in digital voting and potential security enhancements.
    - **Ahmed Khan (Security Expert)**: Analyze security threats and propose mitigation strategies.
    - **Rachel Green (Documentation and Compliance)**: Ensure the project adheres to the IEEE format and manage report compilation.
- **Milestones**:
    - **Topic and Initial Research (November 15th, 2022)**: Finalize the topic and complete initial research.
    - **Literature Review Completion (November 30th, 2022)**: Finalize the literature review section.
    - **Framework Development (December 15th, 2022)**: Develop the initial draft of the proposed security framework.
    - **First Draft of Report (December 21st, 2022)**: Complete the first full draft of the report.

    - **Final Review and Edits (January 5th, 2023)**: Finalize the report and make necessary revisions.
    - **Submission of Final Report (January 10th, 2023)**: Submit the completed research paper.
- **Change Log**:
    - *To be updated with significant changes throughout the project duration.*

Expected Outcomes:

The research aims to yield a detailed analysis of current vulnerabilities in digital voting systems and provide a robust framework that enhances both security and privacy. This framework is expected to serve as a guideline for future electoral system developments and reforms.

Appendices:

- The final paper will include an Appendix with the detailed project proposal, change log, and supplementary research materials.

Note: This project proposal is a hypothetical example created for the purpose of illustrating the structure and content for Assignment 3 in COSC2539.

Part 2: Research Report (Six Pages)

Approach to Writing the Research Report

1. **Introduction (Sample Excerpt)**
    - **Topic Introduction**: Start with an overview of the critical nature of security and privacy in digital voting systems.
    - **Relevance**: Highlight recent concerns and incidents that have brought this topic into focus.
    - **Objective**: State the purpose of your research.
2. **Literature Review**
    - **Existing Research**: Summarize key findings from the academic journals and other reputable sources.
    - **Relevant Theories and Models**: Discuss any theoretical frameworks or models that are pertinent to digital voting security.
    - **Gaps in Research**: Identify any gaps in the existing literature that your research aims to fill.
3. **System Specifications**
    - **Proposed Design/Tools**: Detail any specific system designs or tools that are central to your research.

- **Feasibility and Practicality**: Discuss the practical aspects of implementing these designs or tools in real-world scenarios.

4. **Methodology for Analysis**
    - **Research Methods**: Describe the methods used, whether qualitative, quantitative, or a mix.
    - **Data Collection**: Explain how data was collected, including any simulations, surveys, or case studies.
5. **Results and Discussion**
    - **Findings**: Present the main findings of your research.
    - **Analysis**: Analyze these findings, discussing their implications and how they relate to the existing literature.
    - **Challenges and Limitations**: Discuss any challenges encountered during your research and the limitations of your findings.
6. **Conclusion**
    - **Summary of Findings**: Briefly summarize the key points of your research.
    - **Implications**: Highlight the practical implications of your findings for the election industry.
    - **Future Research**: Suggest areas for future research.
7. **References**
    - **Citing Sources**: List all sources used in your research, following the IEEE format.
8. **Appendix**
    - **Supplementary Materials**: Include additional materials, the original proposal, and the change log.
9. **Visual Aids**
    - **Tables and Figures**: Incorporate tables, figures, or diagrams where necessary to support your findings.

Sample Excerpt from Introduction

Introduction

In recent years, the security and privacy of digital voting systems have become a paramount concern in the electoral process. The advent of digital technologies in elections has introduced new dimensions of vulnerabilities, making the integrity of electoral outcomes susceptible to cyber threats and privacy breaches. This research aims to explore and develop a comprehensive framework to enhance the security and privacy of digital voting systems. The increasing prevalence of digital voting methods, coupled with high-profile incidents of electoral interference, underscores the urgency and relevance of this topic. Our research seeks to provide a critical analysis of current security measures and propose advanced solutions to fortify the electoral process against evolving digital threats.

Part 2: Sample Excerpt for Literature Review

Literature Review

The literature on digital voting security and privacy is extensive, reflecting the growing concern and interest in safeguarding electoral processes in the digital age. This review synthesizes key findings from academic journals and other reputable sources, discusses relevant theories and models, and identifies gaps in the existing research.

Existing Research

Recent studies have highlighted various vulnerabilities in digital voting systems. For instance, Thompson et al. (2020) point out the susceptibility of electronic voting machines to hacking, emphasizing the lack of robust encryption methods. In contrast, Baker and Greene (2021) focus on the privacy aspect, discussing how voter data can be compromised through digital platforms. Both sets of authors agree on the need for comprehensive security protocols but differ in their approach to addressing these issues.

On the technological front, innovations such as blockchain have been proposed as a solution to enhance security and transparency in digital voting. A study by Patel and Smith (2019) demonstrates how blockchain technology can create a verifiable and immutable voting ledger, thereby reducing the risk of vote tampering. However, they also caution about the scalability challenges and the need for user education in implementing such technology.

Relevant Theories and Models

Theoretical frameworks in cybersecurity provide valuable insights into the challenges faced by digital voting systems. The CIA Triad model, which focuses on Confidentiality, Integrity, and Availability, is particularly relevant. This model, as discussed by Johnson (2018), can serve as a foundational guide for developing secure digital voting systems by ensuring voter data confidentiality, maintaining vote integrity, and guaranteeing system availability during elections.

Another pertinent model is the NIST Cybersecurity Framework, which offers a structured approach to identifying, protecting, detecting, responding, and recovering from cyber incidents. As outlined by Lee and Choi (2020), applying this framework to digital voting systems can significantly enhance their resilience against cyber threats.

Gaps in Research

While existing literature provides a comprehensive view of the technical vulnerabilities and potential solutions for digital voting systems, there is a noticeable gap in the empirical analysis of these systems under real-world electoral conditions. Few studies offer a detailed analysis of how proposed security models perform in actual electoral environments, especially under diverse socio-political contexts. Additionally, there is a lack of interdisciplinary research combining cybersecurity principles with political science perspectives, which is crucial for understanding and addressing the broader implications of digital voting security on democratic processes.

Furthermore, another gap is the limited exploration of voter behavior and perception in the context of digital voting security. Understanding how voters perceive and trust these systems is vital for their successful implementation and widespread adoption.

References:

1. Thompson, R., et al. "Vulnerabilities in Electronic Voting Machines." *Journal of Cybersecurity*, vol. 35, no. 2, 2020, pp. 110-125.
2. Baker, S., and Greene, A. "Privacy Concerns in Digital Voting." *Data Protection Journal*, vol. 12, no. 3, 2021, pp. 78-89.
3. Patel, A., and Smith, J. "Blockchain in Voting: A Secure Approach to Digital Democracy." *Journal of Technological Innovations*, vol. 14, no. 4, 2019, pp. 45-60.
4. Johnson, D. "Applying the CIA Triad to Digital Voting Systems." *Cybersecurity Review*, vol. 22, no. 1, 2018, pp. 33-47.
5. Lee, M., and Choi, B. "Enhancing Electoral Systems Security: A NIST Framework Approach." *International Journal of Cybersecurity Applications*, vol. 16, no. 2, 2020, pp. 200-216.

Note: The references and studies mentioned are hypothetical and created for illustrative purposes.

Part 3: Sample Excerpt for System Specifications

System Specifications

To address the identified vulnerabilities in digital voting systems and fill the gaps highlighted in the literature review, our proposed system specification focuses on integrating advanced cybersecurity technologies and methodologies. The primary components of this system include:

1. Blockchain-Based Voting Ledger

- **Implementation**: Utilizing blockchain technology as the backbone of the digital voting system. This decentralized ledger offers a transparent and immutable record of votes, ensuring the integrity of each vote cast.
- **Security Advantage**: With blockchain, vote tampering becomes exceedingly difficult due to the cryptographic linkage of blocks and the distributed nature of the ledger.
- **Privacy Protection**: While ensuring vote integrity, the system also anonymizes voter data, separating voter identity from the vote cast to maintain voter confidentiality.

2. Multi-Factor Authentication (MFA)

- **Purpose**: To bolster voter authentication and minimize unauthorized access, MFA will be implemented. This ensures that the individual casting the vote is indeed the legitimate voter.

- **Method**: The MFA system combines something the voter knows (a password or PIN), something the voter has (a mobile device or smart card), and something the voter is (biometric verification like fingerprint or facial recognition).

3. End-to-End Encryption (E2EE)

- **Application**: From the point of voting to the tallying of votes, E2EE ensures that votes are encrypted, making them inaccessible to unauthorized entities during transmission and storage.
- **Benefit**: This maintains the confidentiality and integrity of the vote throughout the voting process.

4. Real-Time Intrusion Detection and Response System

- **Integration**: Implementing a system that continuously monitors network traffic for signs of unusual or malicious activity.
- **Response Mechanism**: The system is designed to respond immediately to detected threats, minimizing potential damage and preventing breach attempts.

5. Regular Security Audits and Compliance Checks

- **Procedure**: Conducting periodic audits of the voting system to identify and rectify any security weaknesses.
- **Compliance**: Ensuring the system adheres to international cybersecurity standards and electoral regulations.

6. Voter Education and Interface Design

- **Educational Programs**: Implementing voter education initiatives to inform voters about the security measures in place and how to securely cast their votes.
- **User-Friendly Interface**: Designing an intuitive voting interface that maintains security without compromising the ease of use for voters.

Note: This system specification is hypothetical and serves as a sample excerpt for part of a research paper on digital voting security and privacy.

› Part 4, 5,...

↳ 1 cell hidden