ZKP and Security for Voting Systems

Project ID: 24 - 25J - 236

Project Proposal Report

Perera U.L.S.A – IT21278976

B.Sc. (Hons) in Information Technology Specializing in

Cyber Security

Department of Computer Systems Engineering

Sri Lanka Institute of Information Technology

Sri Lanka

August 2024

ZKP and Security for Voting Systems

Project ID: 24 - 25J - 236

Project Proposal Report

Perera U.L.S.A – IT21278976

Supervised by – Mr. Kavinga Yapa Abeywaradana

B.Sc. (Hons) Degree in Information Technology

Department of Computer Systems Engineering

Sri Lanka Institute of Information Technology

Sri Lanka

August 2024

Declaration

We declare that this is our own work, and this proposal does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other university or Institute of higher learning and to the best of our knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Name	Student ID	Signature
Perera U.L.S.A	IT21278976	

The supervisor/s should certify the proposal report with the following declaration.

The above candidate is/are carrying out research for undergraduate dissertation under my supervision.

Supervisor	Date	Signature
K.Y. Abeywardena	22nd of August 2024	

Abstract

Homomorphic encryption (HE) has taken a new paradigm shift in performing computations on encrypted data and still aims at providing privacy and security at the same time. This work looks at the areas of concern that HE could be applied in electronic voting systems to overcome the major challenges such as voter anonymity, accuracy and election transparency. The proposed solution combines HE with ZKP to encode the votes in such a way that they are both anonymous, yet the result can be tallied, and correctness can be verified. As for the scope of the research, the proposed e-voting protocol is intended to be a scalable, secure and friendly for usage solution to the shortcomings of the presently available e-voting systems. The project will therefore entail designing new encryption schemes and fine tuning its performance as well as conducting simulations and real life tests to prove its worth. Being based on sophisticated cryptographic methods, this work is expected to add to improvement of transparent and trustworthy elections.

Keywords: *Homomorphic Encryption, Zero-Knowledge Proofs (ZKPs), E-Voting Systems, Data Privacy, Election Security, Cryptographic Protocols, Secure, Computation, Vote Confidentiality, Verifiable Voting, Scalable Encryption*

Table of Contents

1. INTRODUCTION

1.1. Background study

As a result of technological advancement in the world today, e-voting systems play a vital role in today's worldly Elections. Nonetheless, there are very many issues of concern when it comes to e-voting systems such as security, voters' privacy, transparency and trust. Problems like ease of hacking, manipulation of the vote or a compromise on the voter's identity and the choice made, are some of the problems that traditional e-voting systems present. These problems have raised the demands on secure cryptographic techniques to protect the identity of voters while at the same time making the elections' results accurate and verifiable. [1]

It is Homomorphic encryption (HE) which rises out as suitable solution to these challenges. In contrast to the conventional methods of encrypting data, homomorphic encryption avails the chance of computations to run on the encrypted data without the evaluations having to be decrypted firstly. This feature is especially useful in electronic voting, where it becomes very important to count all the votes and at the same time protect the vote choices of the individual voters. Here, by applying homomorphic encryption votes cast during the election are encrypted and then tallied without exposure of any result at any stage of the process so that the votes or the identity of the voters is not revealed.

The use of the blockchain doesn't stop with improved security, to bring even more checks to the system, integrating Zero-Knowledge Proofs (ZKPs) gives another layer of the shield. ZKPs allow one to prove computations or statements and be certain that no other data is exposed. The use of ZKPs in e-voting can therefore be as a means of proving that the votes have been counted correctly without necessarily revealing the local votes or violating the voter's anonymity.

Incorporation of homomorphic encryption and ZKPs solves most of the problems faced with in the current systems of e-voting. Nevertheless, there are still issues, which are to be solved, like, for instance, improving the computational compacity and the applicability of these techniques at large scale elections, making the voting process easy and convenient for the voter, and integrating the proposed solutions with the existing frameworks. This background work paves way for the analysis of a security, usability, and verifiability of e-voting incorporating homomorphic encryption as well as ZKPs.

1.2. Literature Survey

Homomorphic encryption (HE) is a class of encryption techniques that allow computations on ciphertexts, producing an encrypted result that, when decrypted, matches the result of operations performed on the plaintexts. Introduced by Rivest, Adleman, and Dertouzos in 1978, this concept remained theoretical until the breakthrough of fully homomorphic encryption (FHE) by Gentry in 2009. Gentry's FHE scheme, although revolutionary, was initially impractical due to its high computational overhead. Since then, significant research has focused on developing more efficient HE schemes that can be applied in real-world scenarios.

There are three main types of homomorphic encryption: Partially Homomorphic Encryption (PHE), which supports either addition or multiplication, Somewhat Homomorphic Encryption (SHE), which supports a limited number of both operations, and Fully Homomorphic Encryption (FHE), which supports an arbitrary number of additions and multiplications. In the context of voting systems, SHE and FHE have gained attention due to their ability to perform complex vote aggregation securely.

To comprehend the concept of e-voting it has been widely studied to examine the efficiency, accessibility and transparency of the elections. Classical cryptographic methods have aimed to protect the content and confidentiality of the votes by means of encryption and well protected algorithm. In past voting systems, the Chaum-Pedersen mix-net and the Benaloh encryption system are some of the schemes that were employed to enable the tallying of the votes while at the same time protecting the voters' identities. However, these systems have a limitation of compromise in either scalability or transparency depending on the number of elections to be monitored.

New developments in cryptography and especially in homomorphic encryption have made the improve e-voting protocols, where encrypted votes are tallied without decryption. Protocols like PHE and homomorphic tallying are applied in the Helios voting system for small-scale elections and these create the basis for further studies on larger and efficient and secure electoral systems. This paper sees Helios as a proof of concept for homomorphic encryption, but at the same time learning that the voting system needs to be shielded adequately against coercion and eventual invasion of privacy.

Many papers have already discussed the sort of homomorphic encryption as the tool in voting systems. It has for example been proposed that additive homomorphic encryption can be used in e-voting where the votes are directly encrypted and summed in the encrypted space. A harm minimization concept such as the JCJ protocol and the Belenios voting system make use of homomorphic encryption techniques to tally the votes while maintaining the anonymity of the voter. The main benefit of these systems is that the vote counting is made without decryption and thus the security is increased.

However the question arise of how such protocols can be scaled for use in large scale elections within which computational gain becomes cumbersome. Previous work has dealt with development of lightweight homomorphic encrypted computations that are secure, efficient, and easily scalable. However, work is being done on enhancing the user interface and confidence given that the complex cryptography systems have low usage due to the perceived huge complexity.

1.3. Research Gap

This proves the fact that homomorphic encryption and its applicability to e-voting has not fully gotten passed its hurdles. One of the main problems can be viewed in the dilemma concerning the trade-off between security and performance. Most secure of the mentioned schemes is fully homomorphic encryption but may take more time and so may not be feasible for real-time large-scale election. So, there are current developments to work on potential improvements to these kinds of encryption schemes which add less latency and are more scalable.

However, extending the application of homomorphic encryption with ZKPs can also provide possibilities and difficulties. In this combination there are strong guarantees of privacy and verifiability though the protocol specification must be such that the system remains efficient and user-friendly. Furthermore, the goals of security include protecting against attacks on the voting system where voters manipulate votes, voters are coerced into voting in a particular manner, or via denial-of-service attacks during the election.

The following table is a comparison between existing project management tools and the proposed solution.

Table 1 Research Gap

Research Feature	Helios Voting System	JCJ Protocol	Belenios Voting System	Proposed Tool
Scalability	✗	✗	✗	✓
Privacy Protection	✗	✓	✗	✓
End-to-End Verifiability	✓	✓	✗	✓
Efficiency in Vote Tallying	✓	✗	✓	✓
Voter Trust and Transparency	✗	✓	✗	✓

1.4. Research Problem

Thus, the aspects such as the integrity and confidentiality of e-voting systems are regarded as significant issues as the number of the governments and other organizations trying to introduce secure digital voting grows rapidly. Current forms of e-voting systems present themselves with numerous challenges regarding scalability, anonymity and efficiency resulting to challenges such as vote rigging, voter intimidation and privacy invasion. Cryptographic solutions incorporated in such systems include however, they are inefficient, cannot scale, or offer the needed privacy.

With all these changes, it is evident that there is a great need for an elevated cryptographic method that protects the voters' identity all the while creating room for the credibility and the fairness of the tallied votes to be conductively audited. Homomorphic encryption (HE) can offer a solution as computations on the encrypted votes are possible without having to decrypt them and hence maintaining the confidentiality of the votes. Nevertheless, current realisations of HE-based systems are computationally costly and do not always include a practical approach to voter verifiability mechanisms.

These questions are a subject of this research which proposes to design a secure and scalable e-voting system based on homomorphic encryption and ZKPs. The system will permit the votes to be encrypted and counted under an electronic enshroud without compromising the individual sample votes. The idea is to work beyond the existing systems' downsides and come up with a safe and feasible solution for a massive election.

2. OBJECTIVE

The objective of this research component is to explore and implement homomorphic encryption methods, integrated with zero-knowledge proofs (ZKPs), to develop a secure, privacy-preserving, and verifiable voting system. The research will focus on addressing current limitations in e-voting systems by enhancing vote confidentiality, ensuring accurate and transparent tallying, and optimizing performance for scalability in real-world election scenarios.

2.1. Main Objective

To design and develop a secure, scalable, and privacy-preserving electronic voting system using homomorphic encryption and zero-knowledge proofs (ZKPs) that ensures voter confidentiality, accurate vote tallying, and end-to-end verifiability in large-scale elections.

2.2. Specific Objective

To achieve the main objective, the following specific objectives will be followed

- To implement homomorphic encryption techniques that allow secure vote tallying without compromising voter privacy.
- To integrate zero-knowledge proofs (ZKPs) into the system to provide verifiable voting processes without revealing sensitive information.
- To evaluate the performance and security of the proposed system under different election scenarios, ensuring it meets the requirements for real-world applications.

\

3. METHODOLOGY

The methodology of a secure voting system implementation comprises a series of structured steps that involve the use of homomorphic encryption (HE) and zero-knowledge proofs (ZKPs). To begin, an exhaustive requirement analysis is performed on the existing electronic voting system with special focus on privacy, scalability, verifiability and efficiency in order to find out what challenges they face. From there, a suitable homomorphic encryption scheme is chosen that will facilitate secure vote tallying while at the same time maintaining the anonymity of individual votes. The next step involves designing as well as integrating ZKPs into the system to enable both voters and third parties verify how correct the encrypted votes are compared to tallying with no risk of revealing sensitive information.

After this secure voting protocols are developed so as to cover every aspect of the voting process such as encrypting votes aggregating them tallying them up then verifying results. Afterwards these protocols are put into practice through a prototype system combining both homomorphic encryption and zero-knowledge proofs making them work hand in hand. On this juncture, examining security for possible attacks like vote tampering coercion or invading any privacy before carrying out performance tests aimed at gauging efficiency scalability or response times.

In order to determine how effective the system is, extensive testing has been conducted in both simulated and real-world environments. Afterward, results are evaluated in order to see where optimization can be done for improved performance. Finally, a comprehensive documentation of the design, protocols, results as well as future research suggestions helps to end that makes the developed system secure and usable on large-scale elections.

The following technologies will be applied during the implementation

Encryption and Cryptography	• Microsoft SEAL • HElib • PalisaDE
Software Development	• Python • C++ • JavaScript/TypeScript
Data Storage and Management	• PostgreSQL • MongoDB • Cloud Services:
Networking and Security	• TLS/SSL • VPNs **Security Tools:** • Nmap • Wireshark •

3.1. Component Overview Diagram

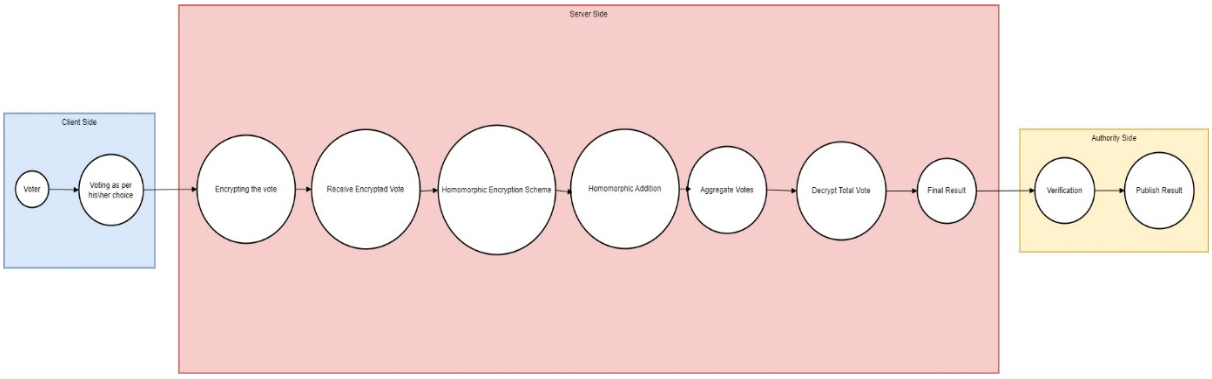
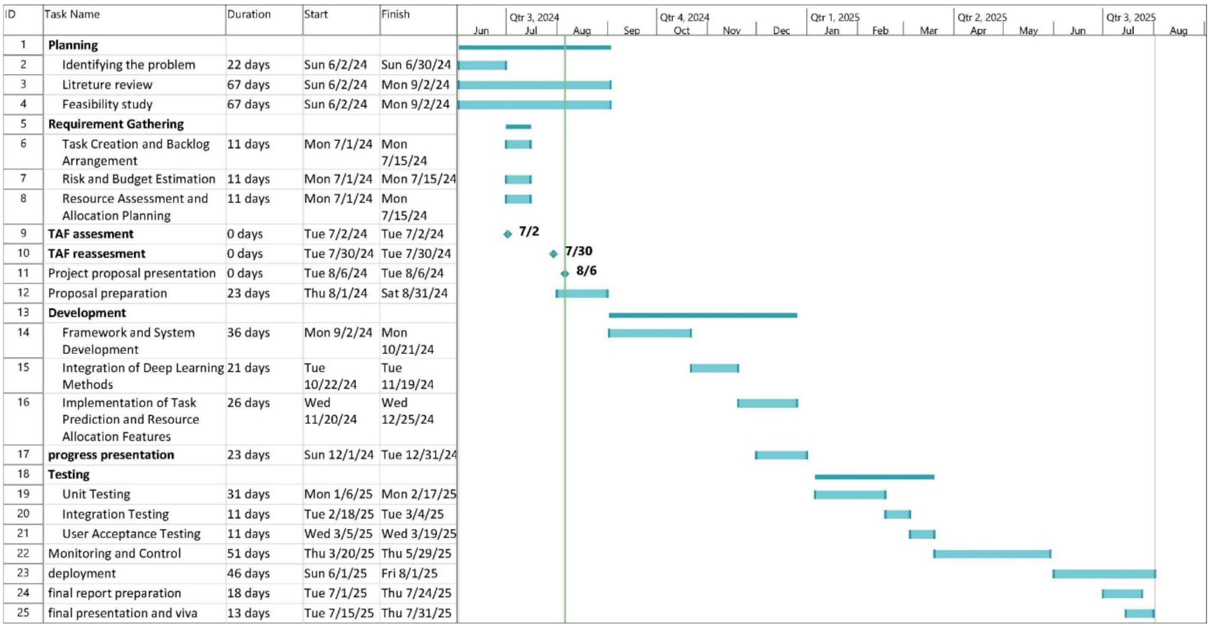


Figure 1 Component Overview Diagram

3.2. Gantt Chart



ID	Task Name	Duration	Start	Finish
1	**Planning**			
2	Identifying the problem	22 days	Sun 6/2/24	Sun 6/30/24
3	Litreture review	67 days	Sun 6/2/24	Mon 9/2/24
4	Feasibility study	67 days	Sun 6/2/24	Mon 9/2/24
5	**Requirement Gathering**			
6	Task Creation and Backlog Arrangement	11 days	Mon 7/1/24	Mon 7/15/24
7	Risk and Budget Estimation	11 days	Mon 7/1/24	Mon 7/15/24
8	Resource Assessment and Allocation Planning	11 days	Mon 7/1/24	Mon 7/15/24
9	**TAF assesment**	0 days	Tue 7/2/24	Tue 7/2/24
10	**TAF reassesment**	0 days	Tue 7/30/24	Tue 7/30/24
11	Project proposal presentation	0 days	Tue 8/6/24	Tue 8/6/24
12	Proposal preparation	23 days	Thu 8/1/24	Sat 8/31/24
13	**Development**			
14	Framework and System Development	36 days	Mon 9/2/24	Mon 10/21/24
15	Integration of Deep Learning Methods	21 days	Tue 10/22/24	Tue 11/19/24
16	Implementation of Task Prediction and Resource Allocation Features	26 days	Wed 11/20/24	Wed 12/25/24
17	**progress presentation**	23 days	Sun 12/1/24	Tue 12/31/24
18	**Testing**			
19	Unit Testing	31 days	Mon 1/6/25	Mon 2/17/25
20	Integration Testing	11 days	Tue 2/18/25	Tue 3/4/25
21	User Acceptance Testing	11 days	Wed 3/5/25	Wed 3/19/25
22	Monitoring and Control	51 days	Thu 3/20/25	Thu 5/29/25
23	deployment	46 days	Sun 6/1/25	Fri 8/1/25
24	final report preparation	18 days	Tue 7/1/25	Thu 7/24/25
25	final presentation and viva	13 days	Tue 7/15/25	Thu 7/31/25

Figure 2 Gantt chart

3.3. Work Breakdown Structure

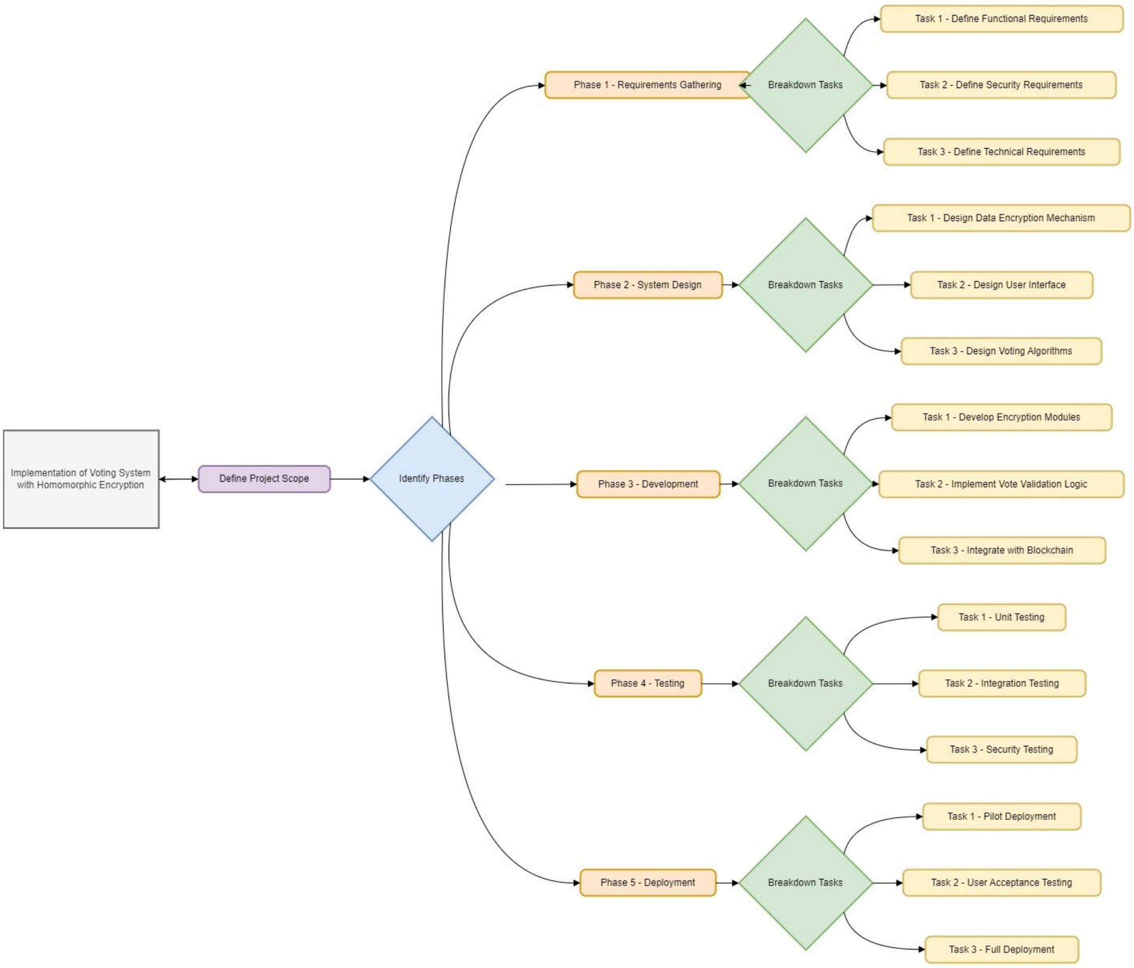

Implementation of Voting System with Homomorphic Encryption
Define Project Scope
Identify Phases
Phase 1 - Requirements Gathering
Breakdown Tasks
Task 1 - Define Functional Requirements
Task 2 - Define Security Requirements
Task 3 - Define Technical Requirements
Phase 2 - System Design
Breakdown Tasks
Task 1 - Design Data Encryption Mechanism
Task 2 - Design User Interface
Task 3 - Design Voting Algorithms
Phase 3 - Development
Breakdown Tasks
Task 1 - Develop Encryption Modules
Task 2 - Implement Vote Validation Logic
Task 3 - Integrate with Blockchain
Phase 4 - Testing
Breakdown Tasks
Task 1 - Unit Testing
Task 2 - Integration Testing
Task 3 - Security Testing
Phase 5 - Deployment
Breakdown Tasks
Task 1 - Pilot Deployment
Task 2 - User Acceptance Testing
Task 3 - Full Deployment

Figure 3 Work breakdown structure

4. PROJECT REQUIREMENTS

The following functional, nonfunctional, and system requirements will be only focusing on the component Prediction and Allocation of Infrastructure Resources.

4.1. Functional Requirements

- The system must encrypt each vote using homomorphic encryption to ensure data privacy before transmission.
- The module must allow addition operations on encrypted data without requiring decryption, enabling the aggregation of votes.
- The encryption and decryption processes should be optimized for performance to handle a large number of votes efficiently.

4.2. Non-Functional Requirements

- Performance
- Scalability
- Security
- Usability
- Maintainability

4.3. System Requirements

- RAM - 16 GB or higher.
- Storage - SSD with at least 500 GB capacity
- High-speed internet connection
- Operating System - Windows 10/11, macOS, or Linux.

5. DESCRIPTION OF PERSONNEL AND FACILITIES

Registration Number	Name	Task Description
IT21278976	Perera U.L.S.A	• The research on homomorphic encryption (HE) will focus on selecting and implementing a suitable HE schemes that enables secure and efficient vote tallying while preserving voter privacy. The study will involve simulations to evaluate the performance of different HE algorithms and optimize their integration into the voting system. • The research will be carried out using high-performance computing systems capable of handling the intensive computations required by homomorphic encryption. The facility provides advanced workstations and secure environments necessary for testing and refining the encryption processes.

6. COMMERCIALIZATION

The proposed research aims to develop a secure, scalable, and privacy-preserving electronic voting system that integrates homomorphic encryption and zero-knowledge proofs (ZKPs). The solution addresses key challenges in current e-voting systems, including voter privacy, verifiability, and trustworthiness. The commercialization potential lies in several areas:

1. **Government and Public Sector**: Governments and public institutions could adopt the developed system for secure national and local elections, ensuring voter privacy while maintaining trust and transparency.
2. **Private Sector and Organizations**: Corporations and large organizations that require secure voting systems for internal elections (e.g., board elections, shareholder voting) can benefit from this technology to ensure fair and confidential voting processes
3. **Licensing and SaaS Model**: The system could be offered as a software-as-a-service (SaaS) product or licensed to other developers and institutions looking to implement secure voting mechanisms.
4. **Customization and Consulting Services**: The system could be customized for different industries or election types, with additional consulting services offered to tailor the solution to specific organizational needs.
5. **Integration with Existing Voting Platforms**: The homomorphic encryption and ZKP technology could be integrated with existing e-voting platforms to enhance their security and privacy features.

7. BUDGET AND BUDGET JUSTIFICATION

Description	Amount (LKR)
Development cost	120,000
Server cost	70,000
Software license	15,000
Transportation cost	10,000
Paper cost	3000
Telecommunication cost	20,000
Maintenance cost	25000
Testing Q/A	25,000
Marketing/ promotions	10,000
Commercialization	20000
Other costs	10,000
Total	**328,000**

REFERENCES

[1] Smart Contract-Based E-Voting System Using Homomorphic Encryption and Zero-Knowledge Proof *Wu, Y., & Kasahara, S. (2023)*

[2] E-voting System Using Homomorphic Encryption and Blockchain Technology. *Hyunyeon Kim, Kyung Eun Kim, Soohan Park, and Jongsoo Sohn*

[3] Privacy-Preserving and Format-Checkable E-Voting Scheme *(https://link.springer.com/chapter/10.1007/978-3-031-41181-6_4)*

[4] KDHS-Voting: A Distributed Homomorphic Signcryption E-Voting

[5] Improvements in Everlasting Privacy: Efficient and Secure Zero Knowledge Proofs

[6] A Privacy-Preserving E-Voting System Based on Blockchain and Homomorphic Encryption

[7] Verifiable E-Voting Using Homomorphic Encryption and Blockchain

[8] Secure E-Voting System Using Homomorphic Encryption and Blockchain.