CHAPTER 1. INTRODUCTIONS

1.1 Project Background

A secure and reliable election system is the foundation of a healthy and credible democratization process. In the era of advancing information technology, electronic voting has become one of the methods adopted by many countries to enhance efficiency and accessibility in the voting process. However, with technological advantages come new challenges, especially related to the security of electronic voting systems (Cop and Purnama, 2015).

One of the main threats to the integrity and confidentiality of electronic voting is phishing attacks. Phishing attacks are manipulation methods where attackers attempt to obtain sensitive information such as passwords, identity card numbers, or other personal information by impersonating a trusted entity (Alotaibi *et al.*, 2022). In the context of elections, phishing attacks can affect the integrity of votes by stealing voter identities or influencing the election results.

The dynamic nature of phishing attacks, indicating that they have evolved and become sophisticated enough to trick not only regular voters but even well-trained election officials. This suggests that the traditional methods of defense may no longer be sufficient, necessitating the development of more advanced and robust solutions. These solutions should have the capability to effectively detect and thwart phishing attempts. Ultimately, the overarching goal is to fortify the security of electronic voting systems, ensuring that they remain resilient in the face of evolving cyber threats.

Visual cryptography is one promising cryptographic technique to protect sensitive information in this context (Tingare *et al.*, 2021). Visual cryptography can split information into seemingly random parts that do not provide clues about the original information, except when these parts are combined (Poriye and Tyagi, 2009). This allows for secure information sharing without sacrificing confidentiality.

By leveraging visual cryptography in electronic voting systems, the author aims to create a secure and reliable solution to protect the integrity of elections from phishing attacks (Yuniati and Munir, 2018). This solution will empower voters to cast their votes confidently, knowing that their identities and votes are safe from phishing attempts.

By the incorporation of visual cryptography into electronic voting systems as a means to enhance the integrity and security of the democratic process. The author expresses a hope that this research endeavor will yield a positive impact on the advancement of secure and dependable electronic voting technology. This suggests that the integration of visual cryptography is seen as a significant step toward fortifying the trustworthiness of electronic voting systems, ultimately contributing to the progress of democratic practices.

1.2 Problem Statement

Here are the problem statements in "Preventing Phishing Attack on Voting System Using Visual Cryptography":

1. Vulnerability to Phishing Attacks in Electronic Voting System: The electronic voting system allows voters to cast their votes online, but it is susceptible to phishing attacks. These attacks can be attempts to deceive and obtain sensitive information or gain unauthorized access to the system. As a result, the integrity and security of the voting process may be compromised.
2. Insecurity of Voter's Personal Information: Voter's personal information, including names, addresses, and voting preferences, is sensitive data that requires protection. Phishing attacks can pose a risk of leakage or misuse of this information by unauthorized parties, threatening the privacy and security of voters.
3. Fraud and Manipulation of Election Results: Phishing attacks can pave the way for fraud in election results. Attempts to manipulate votes or voter information can disrupt the integrity of the democratic representation of the

people's will. This undermines public trust in the election process and the validity of its outcomes.

1.3 Project Objective

The objectives of the project “Preventing Phishing Attack on Voting System Using Visual Cryptography” are as follows:

1. To build and implement a visual cryptography (VC)-based voting system to ensure the security and confidentiality of vital internal decisions within the company. Visual cryptography is a method that involves encoding information in such a way that decryption requires a visual aid, making it a powerful tool for secure communication (Mahmoud, 2017). The implementation of this system will facilitate secure voting procedures for sensitive company matters, ensuring the confidentiality of the decisions made.
2. To counter phishing attacks that could threaten the security and integrity of the voting process. With a high level of security, voters can cast their votes online without the risk of being targeted by phishing attacks or attempts to manipulate data. Furthermore, the system facilitates voters in doing so from remote locations, thereby enhancing flexibility and accessibility in the voting process (Nisha and Madheswari, 2016).
3. To integrating a phishing attack detection system that can identify and block attempts to attack the voting system. This system would be capable of recognizing and preventing any efforts to compromise the voting system. As a result, the implementation of this system would lead to a decrease in the likelihood of sabotage or theft of both the voters' voices and their personal data.
4. To enhance awareness among voters regarding phishing attempts, they propose achieving this by directing them to the legitimate website and providing crucial security information while they cast their votes. Essentially, the goal is to empower voters with knowledge on how to recognize and

protect themselves from phishing scams during the voting process. This measure is crucial in maintaining the integrity and security of the electoral system.

By achieving these objectives, the project aims to develop a voting system that is both secure and dependable. This system should also encourage active participation from voters without compromising the trustworthiness of their votes. In summary, the project endeavors to establish a voting process that is safe, trustworthy, and engaging for all participants.

1.4 Scope

1.4.1 Project Scope

1. System Design and Development: Designing and developing a visual cryptography (VC) based voting system to ensure the security and confidentiality of internal corporate decisions (Raj *et al.*, 2016).
2. Phishing Attack Detection Implementation: Addressing phishing attacks that attempt to target or disrupt the voting system. By implementing phishing attack detection, the system can identify and prevent such attack attempts, ensuring the security and integrity of the voting process.
3. Integration with Infrastructure: Integration with the existing technological infrastructure within the company to ensure compatibility and interoperability.

1.4.2 System Scope

1. High Security with Visual Cryptography: This functionality utilizes visual cryptography as the primary foundation to ensure a high level of security within the voting system. With this approach, voter data and information are safeguarded from phishing attacks and manipulation attempts that could threaten the integrity of the election.
2. Phishing Attack Detection and Prevention: The system is equipped with sophisticated detection mechanisms designed to identify and prevent phishing attack. With this capability, the system can thwart attackers from

compromising the integrity of the election process, thereby reinforcing the security of every cast vote (Juan and Chuanxiong, 2007).

3. Secure and Convenient Online Voting: This functionality provides voters with the option to securely cast their votes online. Additionally, it enhances accessibility and convenience for voters, enabling them to participate in the election process seamlessly. Therefore, this system not only guarantees security but also prioritizes ease of use for voters (Kaliyamurthie *et al.*, 2013).

1.5 Significane

In the project "Preventing Phishing Attack on Voting System Using Visual Cryptography," various significant benefits are brought to the voting process. The use of visual cryptography in this system provides an additional layer of security, reducing the potential risk of phishing attacks that could threaten the integrity and outcome of the election. The mechanism for detecting phishing attacks also ensures that every vote cast is authentic and not influenced by manipulation or fraud attempts. This not only enhances voter trust, especially in the context of online voting, but also enables participation from remote locations, expanding access for those who may find it difficult to be physically present at a polling place. Additionally, the system ensures accurate and fair election results by preventing fraudulent or manipulative efforts. Finally, through protection from phishing attacks, voters' personal information is also safeguarded from potential unauthorized or malicious access. Thus, this project aims to enhance the integrity and security of the voting process, giving voters confidence that their votes will be counted accurately and unaffected by fraudulent or phishing attempts.

1.6 Project Summary

The summary of the project "Preventing Phishing Attack on Voting System Using Visual Cryptography" aims to enhance the security and integrity of the voting process by leveraging visual cryptography. This innovative approach

ensures that the voting system is resilient to phishing attacks, safeguarding the authenticity of votes and preserving sensitive voter information. The system not only enables secure online voting but also provides flexibility for voters to participate from remote locations. Through sophisticated phishing detection mechanisms, potential threats to the integrity of the voting system are identified and thwarted. Ultimately, this project instills confidence in voters, guaranteeing that their votes will be accurately counted, free from manipulation or fraud attempts. The implementation of this system strengthens the democratic process, upholds transparency, and ensures the representation of the will of the people.