



Start ➡

# BASE PAPER PRESENTATION

## Team

Teresa Jency Bala  
ID:1938520113

Prema Das  
ID:1938520142

Supervisors,  
Swarna Roy  
Lecturer, CSE

Aparna Haldar  
Chairman  
Department of CSE



CSE4192: Thesis/Project (part-1)

Part - 4, Odd Semester, Department of CSE  
Imperial College of Engineering, Khulna Code:385  
(Affiliated with University of Rajshahi)

# Security Analysis of Cyber Attacks Using Machine Learning Algorithms in eGovernance Projects

Harmeet Malhotra<sup>1</sup>, Meenu Dave<sup>1</sup>, and Tripti Lamba <sup>2</sup>

1 Jagannath University, Jaipur, India

harmeet\_hello@yahoo.com, meenu.s.dave@gmail.com

2 Institute of Information Technology and Management, New Delhi, India

triptigautam@yahoo.co.in



# ABSTRACT

The abstract of the paper discusses the challenges and risks associated with the implementation of e-governance in India. The primary concern is the need for secure transactions while maintaining -

- high levels of privacy
  - transparency
  - accountability
  - integrity
  - confidentiality
- within government systems.

The paper highlights that one significant source of risks in e-governance is the poor security of *free WiFi networks* used to access e-services.

To address these challenges, the paper emphasizes on developing methods and tools capable of 1. autonomously detection & 2. defend against cyber attacks.

The paper's main focus is on analyzing different categories of cyber attacks using machine learning algorithms.



# INTRODUCTION

This Chapter of the Conference proceedings: “Futuristic Trends in Networks and Computing Technologies” discusses the security issues of e-governance in India.

They note that there has been little research on e-governance in India, and that the country is facing a number of challenges, including low computer literacy rates and a lack of trust in government services.


The authors also discuss the importance of security in e-governance systems, and they note that there are a number of threats to e-governance security, such as cyber attacks and privacy violations.

Finally, the authors introduce the topic, which is the use of machine learning algorithms to analyze cyber attacks on e-governance systems. The goal of the paper is to propose a strategic framework.



# BACKGROUND

This thesis is rooted in identification of a number of security challenges facing e-governance systems in India, including:

- Technical **vulnerabilities in TCP/IP network layers** and other resources, both technical and non-technical, and deployment of inadequate and **insufficient security laws and standards**.
  - **Lack of standard techniques** for detecting vulnerabilities, both known and unknown.
  - Variety of attacks, including watering hole attacks, replay attacks, zero-day attacks, etc.
  - **Lack of Specific security requirements** of e-governance systems, such as protecting legal information and other sensitive data, and maintaining confidentiality, integrity, and availability.
  - **Lack of trust in public systems**, which can make it difficult to implement e-governance solutions.
- 

# LITERATURE REVIEW

The literature review discusses the security challenges and solutions for e-government systems. The topics covered in the review include:

- **Security vulnerabilities** in e-government websites and there is a need for better security measures.
- E-government systems are **vulnerable to a variety of cyber attacks**, including denial-of-service attacks, unauthorized access, and data theft.
- E-government systems need to be **secure** in order to protect sensitive data and maintain public trust.
- Security **solutions** for e-government systems need to be created.





# PROBLEM



The Problem introduced is the lack of cyber security in many government departments. This can lead to a number of problems:

- data breaches
- identity theft
- financial fraud

It discusses the need for

- update security policies
- importance of promoting confidence in government departments to implement e-governance solutions.

# OBJECTIVE

**The paper aims to analyze the security of e-governance systems and the role of machine learning algorithms in detecting and preventing cyber attacks**



# METHODOLOGY

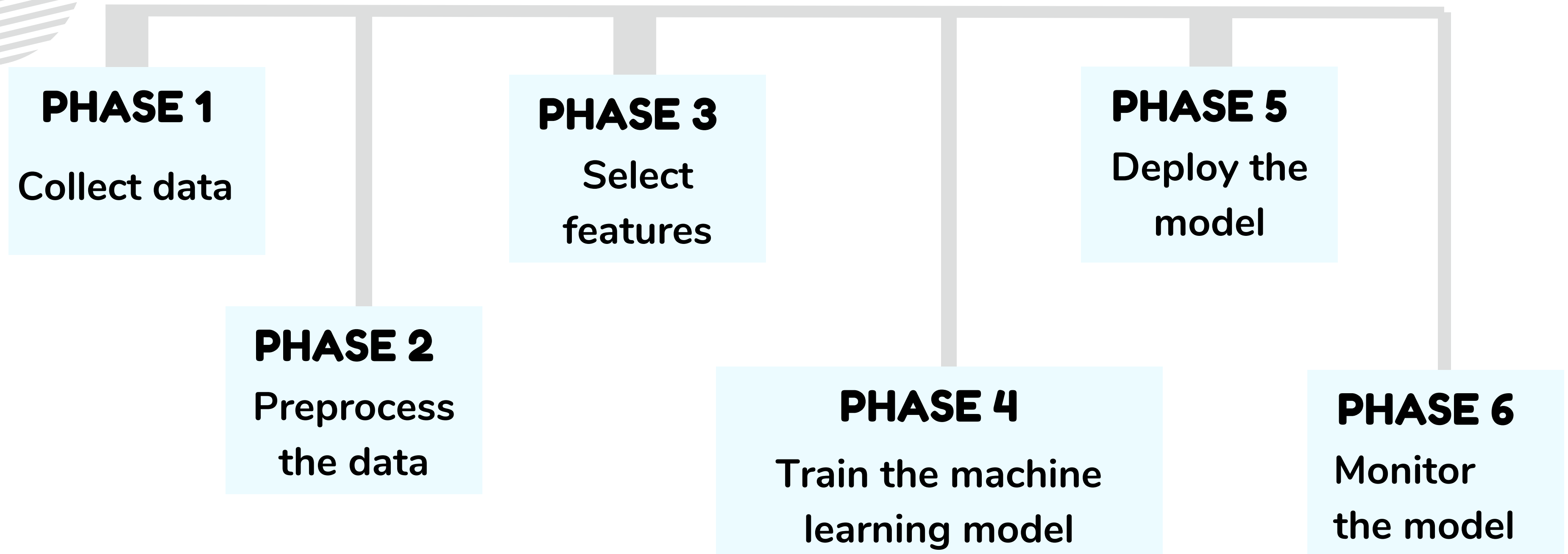
## QUANTITATIVE METHOD

Used to train and evaluate the machine learning algorithms

## QUALITATIVE METHOD

Used to identify the relevant features and to group the attacks into similar attacks

# IMPLEMENTATION



# RESULT

The framework has been trained on the *UNSW NB-15 dataset*, which is a public dataset of real-world network traffic data.

The framework was able to achieve an accuracy of 99% on the test set using the Neural Network algorithm, which suggests that it is effective at predicting cyber attacks.

**Table 2.** Comparison of results of machine learning algorithms

	SVM	Naive Bayes	Neural network
Accuracy	90.6	80.05	99.92
95% CI	(0.894, 0.917)	(0.7845, 0.8159)	(0.9972, 0.9999)
No information rate	0.35	0.35	0.36
Kappa	0.86	0.7196	0.9989


# CONCLUSION

The framework can be implemented in the firmware of the e-governance website server **to monitor the network**. Once an deviation of general purpose usage is seen, the framework will immediately notify the system and take measures to prevent the attack.

The framework is an improvement over existing methods because it is more accurate and can be implemented in real time. This makes it a valuable tool for protecting e-governance websites from cyber attacks.



# FUTURE WORK

- Explore new machine learning algorithms that could be developed that are specifically tailored to the needs of e-governance systems.
  - Existing algorithms could be evaluated on real-world e-governance data to see how well they perform in practice.
  - The framework could also include guidelines on how to evaluate the performance of machine learning algorithms and how to integrate them into existing e-governance systems.
  - Deploy the trained model to a web server. This can be done using a variety of technologies, such as Flask, Django, and TensorFlow Serving
- 

# REFERENCES

## 🔍 REFERENCE 1

Malhotra, Harmeet & Dave, Meenu & Lamba, Tripti. (2020). Security Analysis of Cyber Attacks Using Machine Learning Algorithms in eGovernance Projects. 10.1007/978-981-15-4451-4\_52.





# THANK YOU

