PROJECT SYNOPSIS

PART A: Synopsis Registration

1. Student Details

Name: Praneet
Roll No: 2302570049
Name of Program: MBA
Session: 2023-2025
Semester: Semester 1
Subject: Cyber Law & Governance

2. Project Synopsis Details

Title: Enhancing Security through Homomorphic Encryption

ABSTRACT:

In an era increasingly reliant on data, the imperatives of robust data security and privacy preservation have grown more paramount than ever. The research endeavour, titled **"Enhancing Security through Homomorphic Encryption**," immerses itself in the realm of advanced cryptography to confront these challenges. Our central objective is the development of innovative methodologies within the domain of Homomorphic Encryption, designed to facilitate secure data processing while preserving the confidentiality of information. This research project holds substantial significance for the technology sector as it can fortify data protection in pivotal applications such as cloud computing, financial transactions, and the management of sensitive healthcare data.

INTRODUCTION:

The explosive proliferation of digital data and the ascendancy of cloud computing have thrust the matter of data privacy to the forefront of contemporary discourse. Conventional encryption techniques fall short when data processing is delegated to third-party entities, such as cloud service providers. Homomorphic Encryption, which enables computations on encrypted data, has emerged as a promising remedy to this conundrum. Our undertaking seeks to propel this technique into a more efficient, secure, and pragmatic sphere. Such an advancement is indispensable for cybersecurity in the age of big data.

LITERATURE REVIEW:

Our comprehensive survey of the existing body of literature underscores the commendable progress made by researchers in comprehending the theoretical underpinnings of Homomorphic Encryption. However, the realm of practical implementations and real-world use cases remains underexplored. Prior research efforts have predominantly centered on algebraic facets, such as fully homomorphic or somewhat homomorphic schemes, with limited forays into practical applications. While case

studies elucidate the potential of secure data outsourcing, there remains an imperative to further explore real-world implementations.

DISTINGUISHING CONTRIBUTION:

Our research project stands out by addressing the gap between theoretical foundations and practical application within Homomorphic Encryption. We are engendering novel algorithms designed to elevate both the performance and security of this encryption methodology. Our approach endeavours to harmonize theoretical rigor with pragmatic utility, while simultaneously offering a roadmap for implementation, with the aim of rendering Homomorphic Encryption more accessible and user-friendly.

OBJECTIVES:

Innovate novel Homomorphic Encryption algorithms optimized for efficiency and security.

Strike an equilibrium between computational speed and data protection.

Implement and subject these algorithms to rigorous assessment within real-world scenarios, including secure cloud-based data processing and privacy-preserving machine learning.

Evaluate performance metrics, scalability, and resistance to security threats.

Furnish practical recommendations and guidelines for the deployment of Homomorphic Encryption in diverse applications.

Offer insights into seamless integration, effective key management, and performance optimization.

Hypothesis:

We posit that our research will yield Homomorphic Encryption algorithms that are not only more efficient but also more secure, rendering them suitable for real-world applications. These algorithms are anticipated to markedly reduce the computational overhead traditionally associated with Homomorphic Encryption, all the while maintaining a robust security posture. Our findings are projected to exert a direct, positive influence on data security within contexts such as cloud computing and various data processing applications.

METHODOLOGY:

Our methodological approach comprises two primary components. Initially, we shall conceive and refine Homomorphic Encryption algorithms, leveraging principles of mathematics and cryptographic methodologies. Subsequently, we will implement these algorithms within practical contexts, including cloud-based data processing and privacy-preserving machine learning. Data collection will encompass extensive testing and benchmarking, employing an array of datasets and performance metrics. The research design emphasizes the generalizability of our findings.

CONCLUSION:

The efficacious execution of our research project holds the potential to revolutionize data security and privacy measures within the technology industry. By offering Homomorphic Encryption solutions that are not only more efficient but also more secure, we enable organizations to confidently outsource data processing while maintaining the utmost levels of privacy and security. This transformative accomplishment is poised to foster trust, ignite innovation, and fuel growth within the domain of data-driven technologies.