1. Introduction

Genomics is a critical field of study that explores the structure, function, and evolution of genomes, providing comprehensive genetic information essential for understanding various biological processes. Recent advancements in genomic studies have highlighted their applicability in diverse domains, including agriculture, medicine, and environmental conservation. For example, Sudrajad et al. [1] demonstrated the utilization of genomic information to investigate the specific effects of dietary intake on livestock genetics. This research underscores the pivotal role of genomics in optimizing feed efficiency and improving livestock performance. Such findings reflect the growing significance of genomics in addressing complex biological challenges, particularly those requiring large-scale data analysis and computational resources. Protecting genome data is crucial due to its high sensitivity and importance in various life cycles. Therefore, it is essential to protect this information. The misuse of genomic data is possible through identity fraud, which occurs when the protection is not adequate. Online DNA testing services have made the risks even more significant in the technological age. Hackers could manipulate the information stored in these databases if they are not adequately protected. Genomic data can be utilized by hackers to create false genetic profiles, which can then be used for criminal purposes like identity theft or financial fraud. The potential for misuse is highlighted by cases such as the MyHeritage breach [15], which exposed over 92 million accounts, and unauthorised access to GEDmatch databases [16], underscoring the need for effective cryptographic safeguards.

Several studies regarding the development of genomic data using genomic technologies have been conducted [2][3][4]. These studies indicate that genomic data has experienced yearly growth. Large-scale data, such as genomic datasets, require significant storage capacity and computational resources, which result in high processing costs. Consequently, institutions tasked with storing and managing genomic information must consider flexible and cost-efficient service providers. Cloud computing emerges as a viable solution due to its ability to store and process data efficiently, providing scalability and flexibility that can reduce infrastructure costs for institutions utilizing these services [5]. However, using cloud services introduces challenges related to data security and privacy, as cloud services involve third-party providers. Threats may include system breaches leading to the leakage of sensitive information, data theft, or privacy violations by unauthorized parties, potentially harming individuals or institutions. Therefore, effective and efficient security measures are essential to protect genomic data stored and processed in the cloud.

Many studies have explored cryptographic solutions for genomic data security, such as RSA for high-throughput applications [8] and Paillier for privacy-preserving computations [9], but these studies often evaluate individual algorithms separately or focus on generalized data protection. As far as we are aware, RSA and Paillier have not been extensively tested for genomic workflows in cloud environments through systematic comparisons. However, By analyzing the algorithms' runtime, throughput, and memory usage, this study fills in the gap by providing a comprehensive assessment.

Enhancing genomic data security can be achieved through cryptographic approaches, as cryptographic processes inherently occur on data processed in the cloud. One such approach is Homomorphic Encryption, which enables computations on encrypted data without requiring decryption. Research has demonstrated

that Homomorphic Encryption serves as a robust foundation for cloud architectures and is suitable for securing the processing of data stored in the cloud [6]. With its high throughput and cryptographic features, RSA is a reliable option for secure data transmission and storage, while Paillier offers homomorphic properties that are useful for privacy-preserving computations.

This study aims to examine and evaluate the capability of Homomorphic Encryption in enhancing the security of genomic data stored and processed in the cloud. Specifically, the research compares the performance of RSA and Paillier algorithms, offering insights into their practical applicability in real-world genomic workflows.