REVIEW OF RESEARCH
ISSN: 2249-894X
IMPACT FACTOR : 5.7631(UIF)
VOLUME - 9 | ISSUE - 7 | APRIL - 2020

PRIVACY-PRESERVING CRYPTOGRAPHIC PROTOCOLS BALANCING DATA SECURITY AND UTILITY

Mahantesh Radderatti
Research Scholar

Dr. Shashi
Guide
Professor, Chaudhary Charansing University Meerut.

ABSTRACT

Modern computer systems depend heavily on privacy-preserving cryptographic protocols because they allow for safe data processing and sharing while preserving confidentiality. These protocols are especially crucial for sensitive data applications like cloud computing, healthcare, and finance. However, because privacy-enhancing mechanisms frequently introduce computational and communication overhead that can impair system performance, they face the inherent challenge of striking a balance between data security and data utility. The different cryptographic methods used to protect data privacy while permitting useful computations are covered in this abstract. These methods include differential privacy, secure multi-party computation, homomorphic encryption, and trusted execution environments. The degree of privacy protection, data accuracy, and computational efficiency are frequently traded off in these approaches, despite the fact that they offer robust privacy guarantees.

KEYWORDS: *healthcare, and finance, mechanisms frequently introduce computational and communication.*

INTRODUCTION

Protecting sensitive data is more important than ever in today's world, which is becoming more and more data-driven. Because sectors like government, healthcare, and finance depend on extensive data analysis, protecting privacy has emerged as a key issue. In order to ensure that sensitive data can be processed, shared, and analyzed without disclosing private or sensitive information, privacy-preserving cryptographic protocols have become indispensable tools. Even when data is processed or stored in untrusted settings, like cloud computing or third-party services, these protocols are made to preserve its confidentiality, integrity, and authenticity. At the core of privacy-preserving cryptography is the problem of striking a balance between data security and data utility. Despite offering strong privacy guarantees, cryptographic protocols like homomorphic encryption, differential privacy, secure multi-party computation (SMC), and trusted execution environments (TEEs) frequently have performance overheads that can affect an application's usability and effectiveness. For instance, fully homomorphic encryption (FHE) limits its use in real-time systems due to its computational cost and slowness, even though it offers a strong way to perform operations on encrypted data. In a similar vein, methods such as differential privacy can lower data precision to protect individual privacy, which will impact the data's quality and utility.

Aims And Objectives

The purpose of this research is to investigate and evaluate privacy-preserving cryptographic protocols that enable safe data processing while preserving the data's usefulness in diverse computational contexts. It aims to comprehend the difficulties in striking a balance between the necessity of robust data protection and the usefulness of the data, which is frequently jeopardized when privacy measures are implemented. The study looks into protocols like differential privacy, secure multi-party computation, homomorphic encryption, and trusted execution environments in order to evaluate how well they secure data without compromising analytical value or performance.

LITERATURE REVIEW:

The last few decades have seen a major increase in interest in the creation and use of privacy-preserving cryptographic protocols due to the growing use of sensitive data in industries like cloud computing, healthcare, and finance. Sensitive information can be shared or processed by third parties without compromising confidentiality thanks to these protocols, which are made to facilitate data processing while maintaining privacy. However, striking a balance between protecting data security and preserving its computational usefulness is one of the main issues facing privacy-preserving cryptography.One of the most widely used cryptographic techniques for privacy-preserving calculations is homomorphic encryption (HE). Introduced by Gentry in 2009, Fully Homomorphic Encryption (FHE) permits arbitrary computations on encrypted data, allowing sensitive data to stay encrypted while being processed and avoiding exposure. This innovation makes it possible for data analysis and cloud computing to be done securely, without granting the service provider access to the underlying data. Nevertheless, FHE's computational inefficiency is its main flaw. Many real-time applications cannot use encrypted data because operations on it are much slower than on plaintext data. With some success in streamlining key generation and operation schemes, improvements in FHE efficiency have responded by concentrating on simplifying the encryption and decryption procedures.

RESERACH METHOLOGY:

A multi-phase approach is used in the research methodology for privacy-preserving cryptographic protocols with an emphasis on striking a balance between data security and usefulness. This approach aims to thoroughly analyze, compare, and optimize current cryptographic techniques. In order to identify important protocols, their underlying mechanisms, and their practical applications, the research starts with a thorough review of the literature. The theoretical and practical aspects of the protocols under study, including their security guarantees, performance metrics, and effects on data utility, are then thoroughly examined. The study uses qualitative and quantitative analysis techniques to evaluate the efficacy of privacy-preserving cryptographic protocols. Understanding each protocol's conceptual underpinnings and trade-offs, analyzing its advantages and disadvantages, and assessing the real-world effects of applying it in diverse contexts are the main goals of qualitative analysis. This includes a thorough examination of both more recent developments like blockchain and federated learning as well as more established methods like differential privacy, secure multi-party computation, homomorphic encryption, and trusted execution environments.

DISCUSSION:

The continuous conflict between safeguarding private data and facilitating useful computations forms the basis of the debate around privacy-preserving cryptographic protocols, in particular their function in striking a balance between data security and usefulness. The problem still stands: how can cryptographic techniques guarantee strong data protection without materially impairing the usability and computational efficiency of the data, given the increasing demand for privacy-sensitive applications across multiple industries? The ability of homomorphic encryption—in particular, fully homomorphic encryption, or FHE—to carry out operations directly on encrypted data while maintaining privacy has drawn interest. FHE's ability to preserve confidentiality in settings like cloud computing, where data is processed and stored off-premise, is its main benefit. However, FHE is computationally costly due to the

intricacy of its encryption and decryption procedures, which results in slower processing speeds. When dealing with massive amounts of data or when real-time analysis is necessary, this inefficiency becomes a serious problem. The trade-off between security and computational efficiency is still a major concern, even though improvements in FHE scheme optimization have lessened some of these performance bottlenecks. By lowering computational overhead in comparison to FHE, partially homomorphic encryption (PHE), which allows for restricted operations like addition and multiplication, provides a more workable option. PHE may be appropriate for applications with particular requirements, like private voting systems or encrypted financial transactions, but it is ineffective in situations requiring more intricate calculations, which restricts its use in some fields.

CONCLUSION :-

Privacy-preserving cryptographic protocols are essential for protecting private information and facilitating useful calculations for a variety of uses. In today's data-driven world, where privacy concerns are critical in industries like cloud computing, healthcare, and finance, these protocols are crucial. Finding a balance between data security and usefulness is still very difficult, though. Although methods such as differential privacy, secure multi-party computation, and homomorphic encryption offer strong privacy guarantees, they frequently result in performance trade-offs that reduce the usefulness of the data, particularly in real-time or large-scale applications. Despite its ability to perform calculations on encrypted data, homomorphic encryption is still computationally costly, which restricts its applicability and scalability. While secure multi-party computation protects privacy in group settings, it has communication and computational overhead issues, especially when there are more participants or more complex data. Although it frequently compromises data accuracy, differential privacy provides an efficient means of protecting individual privacy in aggregated datasets. Although blockchain technology and trusted execution environments offer promising ways to improve data security and performance, they also have drawbacks, like scalability issues and vulnerability to side-channel attacks.

REFERENCE

- Gentry, C. (2009). *A fully homomorphic encryption scheme*. Stanford University. This seminal work introduced the concept of fully homomorphic encryption.
- Shamir, A. (1979). *How to share a secret*. Communications of the ACM, 22(11), 612-613. This paper introduced the concept of secret sharing, a foundational method in secure multi-party computation (SMC).
- Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006). *Calibrating noise to sensitivity in private data analysis*.
- Intel Corporation. (2013). *Intel Software Guard Extensions (SGX) – Privacy and Security in Cloud Computing*. Intel.
- Boneh, D., & Shoup, V. (2004). *A Graduate Course in Applied Cryptography*. Stanford University. Zhang, Y., & Liu, X. (2017). *Blockchain-based privacy-preserving approaches for healthcare data sharing and computation*.