Privacy-Preserving Diabetes Analytics using Homomorphic Encryption in the Cloud: A Review

Mr. Ayyapparaj T,
Research Scholar,
Department of Computer Science,
KPR College of Arts Science and Research,
Coimbatore

Dr. K. Pradeepa,
Associate Professor & Head,
Department of Computer Science,
KPR College of Arts Science and Research,
Coimbatore

Abstract

This review investigates the convergence of homomorphic encryption, cloud computing, and the analysis of diabetes data. It brings together recent progress in methods that protect user privacy. The paper also looks at how different system designs work. It then compares how well various homomorphic encryption types perform. These include Partially Homomorphic Encryption (PHE), Somewhat Homomorphic Encryption (SHE), and Fully Homomorphic Encryption (FHE). PHE allows specific operations, like addition or multiplication, on encrypted data. SHE permits a limited number of both addition and multiplication operations. FHE, the most advanced, allows any computation on encrypted data. The study also covers rules about data privacy. This is especially important for laws like HIPAA in the United States and GDPR in Europe. These rules aim to safeguard sensitive health information. Finally, the work offers a visual way to think about processing diabetes data securely in the cloud. This framework helps users understand how their information stays private. It addresses the critical need for secure handling of personal health information in the growing field of cloud-based health analytics.

1. Introduction

Diabetes cases are climbing steadily worldwide. This trend creates an urgent need for swift analysis of patient information. Healthcare providers must track disease progression and treatment effectiveness in real-time. This allows for quicker interventions and better patient outcomes. Imagine a doctor needing immediate data on blood sugar trends for a patient. Real-time analytics provide this vital information. Processing sensitive health data, like patient records, brings significant privacy worries. When this data moves to cloud systems, these concerns intensify. Protecting patient confidentiality is paramount. Unauthorized access or data breaches could have severe consequences. Patients trust healthcare systems with their most personal information. Maintaining that trust requires robust security measures.

Homomorphic encryption (HE) offers a powerful solution. It allows computations on data while it remains encrypted. This means sensitive information can be analyzed without ever being decrypted. Think of performing calculations on a locked box. The result is available, but the contents stay hidden. This technology enables secure processing of health data in the cloud. It safeguards patient privacy while unlocking the benefits of data analytics.

2. Background

2.1 Diabetes Analytics

Diabetes analytics relies on a rich dataset. This includes real-time glucose levels. It also captures insulin dosage details. Lifestyle metrics form another crucial part. These metrics can track physical activity. They might also record dietary intake. Sleep patterns are also analyzed. Understanding these data points is vital. The primary goals of diabetes analytics are multifaceted. One key objective is prediction. This involves forecasting future glucose trends. It helps in anticipating hypoglycemic or hyperglycemic events. Anomaly detection is another critical aim. This identifies unusual patterns in glucose readings. Such deviations might signal a problem. Personalized recommendations are also generated. These suggestions aim to improve diabetes management. They can be tailored to individual needs. For example, an analysis might suggest adjusting meal timing. It could also recommend specific exercise routines. The ultimate aim is better health outcomes.

2.2 Homomorphic Encryption Explained

Homomorphic encryption allows computations on encrypted data. This means you can process sensitive information without decrypting it first. This technology is a significant advancement for data privacy.

Partially Homomorphic Encryption (PHE) is the simplest form. PHE schemes support either addition or multiplication operations on ciphertexts. For example, a PHE scheme might let you add two encrypted numbers together. The result, when decrypted, is the sum of the original numbers. However, it cannot perform both addition and multiplication on the same encrypted data. This limits its practical applications for complex tasks.

Somewhat Homomorphic Encryption (SHE) offers more capability. SHE allows for a limited number of additions and multiplications. The main challenge with SHE is noise. Each operation adds noise to the encrypted data. Too much noise corrupts the result, making decryption impossible. Therefore, SHE is suitable for specific tasks where the number of operations is predictable and small. For instance, it could be used for simple statistical analysis on encrypted datasets.

Fully Homomorphic Encryption (FHE) is the most advanced. FHE enables arbitrary computations on encrypted data. This means you can perform any calculation, like addition, multiplication, and complex logic, on ciphertexts. The noise issue is managed through a process called "bootstrapping." Bootstrapping effectively resets the noise level without decrypting the data. This allows for an unlimited number of operations. FHE opens the door to truly secure cloud computing and advanced data analysis. Imagine running complex machine learning models on encrypted patient records without ever seeing the raw data. This level of privacy protection is transformative.

Table 1: Comparative Analysis of HE Schemes

Feature	PHE	SHE	FHE
Supported Operations	Addition or Multiplication	Limited Add & Multiply	Arbitrary Computation
Performance	Fast	Moderate	Slow
Noise Management	Minimal	Requires Bootstrapping	Complex Bootstrapping
Suitability for	Basic Stats	Trend Analysis	Predictive Modeling

Diabetes Use			
Cloud Compatibility	**High**	**Moderate**	**Low (due to overhead)**
Regulatory Alignment	**Partial**	**Strong with safeguards**	**Strongest (end-to-end)**

2.3 Cloud Computing Models: Public, Private, and Hybrid Clouds

Cloud computing offers flexible ways to use technology. We can categorize these by who manages the infrastructure. These categories are public, private, and hybrid clouds.

- A **public cloud** is like renting computing power. Many users share the same hardware. Companies like Amazon Web Services (AWS) and Microsoft Azure offer public clouds. They manage the servers and networks. Users pay for what they use. This model is cost-effective. It offers great scalability.
- A **private cloud** is different. It is used by only one organization. The infrastructure can be on-site. Or, a third party can host it. This offers more control and security. It is good for sensitive data. Many financial institutions use private clouds.
- A **hybrid cloud** combines both. It links public and private clouds. This offers the best of both worlds. Organizations can use public clouds for less sensitive tasks. They can keep private clouds for critical data. For example, a company might use a public cloud for website hosting. It uses a private cloud for customer records. This setup balances cost, security, and flexibility.

The Role of Edge Computing in Latency-Sensitive Diabetes Monitoring

Diabetes management often needs quick responses. Continuous glucose monitoring (CGM) is a key tool. CGMs track blood sugar levels in real-time. They send data to a user's device. This data needs fast processing. Delays can be dangerous. High blood sugar or low blood sugar needs immediate attention.

Traditional cloud computing can have delays. Data must travel to a central server. Processing happens there. Then, the results return. This round trip takes time. This is called latency. For diabetes monitoring, high latency is a problem. It can mean a delayed alert.

Edge computing helps solve this. Edge computing processes data closer to the source. The CGM device itself can do some processing. Or, a nearby device like a smartphone can process it. This reduces the distance data travels. It lowers latency significantly.

With edge computing, alerts are faster. A CGM user gets timely warnings. They can take action quickly. This might mean eating something. Or, it could mean taking insulin. Faster data processing means better glucose control. It helps prevent dangerous highs and lows. Edge computing makes diabetes monitoring more responsive. It improves patient safety. It offers a more immediate way to manage health.

3. Literature Review

3.1. Noise-Resilient Homomorphic Encryption Framework

Shuriya et al. (2024) proposed a Fully Homomorphic Integrity Model (HIM) that overcomes the noise accumulation problem of FHE. The model brings down encryption and decryption latencies by almost 35ms and 140ms respectively and reduces ciphertexts to ~4KB. While the diabetes application received no demonstration, the framework is of massive potential for real-time, cloud-based encrypted analytics.

3.2. Practical Evaluation of FHE in Healthcare

The deployment viability of FHE in practical healthcare applications was assessed by Rauthan (2025). Quality control systems and diagnostic neural networks were the two use-cases that were evaluated. The study demonstrates that FHE can be incorporated into clinical workflows while maintaining a reasonable accuracy and processing time trade-off. Cloud-based diabetes prediction models can easily adopt the methodology.

3.3. GuardML: Hybrid Homomorphic Encryption for Machine Learning

GuardML is a framework that combines symmetric encryption and FHE with Hybrid Homomorphic Encryption (HHE), as described by Frimpong et al. in 2024. As seen in ECG-based categorization, this model improves computing speed while maintaining privacy. Low-latency diabetes prediction models for mobile health applications might be supported by the same infrastructure.

3.4. Multiparty HE for Federated Survival Analysis

A Multiparty Homomorphic Encryption (MHE) method for federated Kaplan–Meier survival analysis was created by Veeraragavan et al. in 2024. With this technique, several institutions can work together to calculate survival curves without disclosing patient-level information. It is especially pertinent to the secure analysis of diabetes long-term outcomes across hospitals.

4. Future Directions

There are a number of important subjects that demand consideration and investigation in the field of future research and development. Integrating Homomorphic Encryption (HE) with Blockchain and Federated Learning technologies is a crucial path toward improving overall data security across a range of applications. While allowing for cooperative data processing and analysis across decentralized networks, this integration has the potential to greatly enhance privacy and security protocols.

The optimization of HE systems designed especially for time-series diabetes data is another crucial area of emphasis. This entails improving current techniques to make sure they effectively manage the subtleties and complexity present in time-series data, which are crucial for precise diabetes monitoring and treatment.

5. Conclusion

A strong option for privacy-preserving analytics in diabetes treatment is homomorphic encryption, which permits calculations on encrypted data without jeopardizing patient privacy. Its usefulness is demonstrated by recent developments in noise handling, performance, and real-world implementation. Adapting these methods to the particular complexity of diabetic data and utilizing cloud platforms for safe, scalable analytics should be the main goals of future research. A big step toward data-driven, privacy-conscious healthcare solutions has been taken with this integration.

References

1. Shuriya, B., Vimal Kumar, S., & Bagyalakshmi, K. (2024). *Noise-Resilient Homomorphic Encryption: A Framework for Secure Data Processing in Health care Domain*.
2. Rauthan, J. S. (2025). *Homomorphic Encryption in Healthcare Industry Applications for Protecting Data Privacy*.

3. Frimpong, E., Nguyen, K., Budzys, M., Khan, T., & Michalas, A. (2024). *GuardML: Efficient Privacy-Preserving Machine Learning Services Through Hybrid Homomorphic Encryption*.
4. Veeraragavan, N. R., Boudko, S., & Nygård, J. F. (2024). *Multiparty Homomorphic Encryption for Federated Kaplan–Meier Survival Analysis*.