International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.com | editor@ijrai.com | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 4, Issue 3, May-June 2021||

DOI:10.15662/IJRAI.2021.0403001

Secure Multi-Party Computation for Analytics-as-a-Service

Ritu Vikram Gupta

Singhania University, Pacheri Bari, Rajasthan, India

ABSTRACT: Secure Multi-Party Computation (MPC) offers a compelling cryptographic framework enabling multiple parties to collaboratively compute analytical results while preserving the privacy of each participant's data. In the context of **Analytics-as-a-Service (AaaS)**, MPC promises a secure path for clients to benefit from powerful analytics without exposing private inputs. This paper examines pre-2020 developments in MPC tailored to AaaS scenarios, including lightweight MPC applications, hybrid protocols, and real-world deployments. A notable instance is the deployment of an MPC web application in Boston for analyzing wage disparities—allowing organizations to compute aggregated statistics without revealing individual data points OpenBU. Tools like Conclave (2019) offer a hybrid approach, compiling analytical queries into a combination of local plaintext operations and MPC steps, dramatically improving scalability for big-data analytics arXiv. Foundational MPC principles—including secret sharing, homomorphic encryption, and garbled circuits—support the development of these secure analytic services DatatasWikipedia. This paper synthesizes such research, providing a focused literature review, and summarizes advantages (e.g., privacy, regulatory compliance), challenges (e.g., computational and communication overhead), methodological strategies, and deployment results. The analysis concludes with reflections on future trajectories that might enable broader adoption of MPC-based AaaS.

KEYWORDS: Secure Multi-Party Computation (MPC), Analytics-as-a-Service (AaaS), Privacy-Preserving Analytics, Secret Sharing, Homomorphic Encryption, Garbled Circuits, Hybrid MPC Protocols, Big-Data Analytics

I. INTRODUCTION

In the era of data-driven decision-making, "Analytics-as-a-Service" (AaaS) enables organizations to access advanced analytics delivered remotely. However, sharing sensitive data for such analytics carries significant privacy risks. **Secure Multi-Party Computation (MPC)** mitigates these risks by allowing parties to compute upon encrypted inputs, revealing only the final aggregated result while keeping individual data private.

MPC is underpinned by cryptographic techniques such as **secret sharing**, **homomorphic encryption**, and **garbled circuits**, invented over the late 20th century and formalized by early works on secure function evaluation WikipediaDatatas. MPC suits AaaS contexts because it eliminates the need for a trusted third party—critical for ensuring compliance with privacy regulations and safeguarding proprietary data.

A practical embodiment of MPC-based AaaS is demonstrated in a Boston University web application (2016) developed for computing wage disparity metrics. This lightweight MPC service allowed employer organizations to collaborate on analytics without exposing individual compensation values OpenBU. For large-scale data, tools like **Conclave** (2019) hybridize local, cleartext processing with MPC for scalable execution of analytics on big data sets arXiv.

This paper explores such early efforts toward embedding MPC in analytics services, evaluating their designs, benefits, and limitations. It highlights how MPC supports privacy-preserving analytics, enabling collaborative insights without compromising security.

II. LITERATURE REVIEW

Foundational MPC Concepts

- **Secret Sharing**, **Homomorphic Encryption**, and **Garbled Circuits** are core to MPC, allowing distributed computation with confidentiality safeguards Datatas.

| ISSN: 2455-1864 | www.ijrai.com | editor@ijrai.com | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 4, Issue 3, May-June 2021||

DOI:10.15662/IJRAI.2021.0403001

- The theoretical roots trace back to cryptographic protocols from the 1970s and 1980s that formulated secure computation without trusted third parties Wikipedia.

MPC in Analytics-as-a-Service

- **Boston University Web Application (2016)**: Demonstrated a lightweight web-app for MPC in analytics. It enabled organizations to calculate wage disparities collaboratively without revealing individual-level data OpenBU.
- **Conclave (2019)**: Addressed MPC's scalability issue by allowing big-data analytics using a hybrid of local plaintext processing and MPC for selected operations. This design allowed Conclave to scale across datasets several orders of magnitude larger than standard MPC frameworks arXiv.

Benefits and Key Use-Cases

- MPC enables **federated analytics**, such as fraud detection, medical research, and aggregated client analytics, without compromising data privacy DatatasOpenMined.
- It addresses regulatory and compliance demands by ensuring data never leaves its owner's control in plain form DatatasPlainSignal.

Challenges Identified

- The **high computational and communication overhead** of MPC can be a bottleneck, especially for real-time or large-scale analytics Medium+1GeeksforGeeks.
- Usability and adoption hurdles persist, as technical expertise in cryptography remains rare in many organizations Medium+1.

III. RESEARCH METHODOLOGY

1. **Protocol Implementation & Application Development**
   - A Boston University team developed a **web-based MPC framework** facilitating lightweight analytics services. The interface allowed non-experts to engage in secure computations such as wage analysis without requiring specialized cryptographic infrastructure OpenBU.
2. **Hybrid Protocol Design (Conclave)**
   - Conclave introduces a **query compiler** that decomposes analytics tasks into:
     - Local, data-parallel computations executed in cleartext;
     - MPC-secured operations for sensitive steps.
   - This reduces reliance on MPC for the entire query, balancing security and efficiency. Execution targets include Spark and Python environments with MPC back-ends like Sharemind or Obliv-C arXiv.
3. **Usability and Deployment Evaluation**
   - In practice, prototypes measure functionality, scalability, and user experience. The web app was deployed for two campaigns within Boston's Women's Workforce Council (2015–2016), collecting feedback on usability and privacy compliance OpenBU.
4. **Performance Metrics & Scalability Analysis**
   - Conclave's performance was evaluated across data sizes, demonstrating orders-of-magnitude improvement over existing MPC systems in both speed and capacity arXiv.

IV. ADVANTAGES

- **Strong Privacy Guarantees**: Ensures individual inputs remain encrypted and private, revealing only aggregated results.
- **No Trusted Third Party Required**: MPC protocols avoid reliance on external intermediaries.
- **Regulatory Friendly**: Aligns with data protection laws (e.g., GDPR) by design DatatasPlainSignal.
- **Broadened Usage**: Lightweight implementation (web app) shows MPC can be accessible even to non-experts OpenBU.
- **Scalability via Hybrid Models**: Approaches like Conclave allow big-data analytics through intelligent division of computation arXiv.

| ISSN: 2455-1864 | www.ijrai.com | editor@ijrai.com | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 4, Issue 3, May-June 2021||

DOI:10.15662/IJRAI.2021.0403001

V. DISADVANTAGES

- **Performance Overhead**: Cryptographic operations and communication rounds introduce latency and high resource usage Medium+1GeeksforGeeks.
- **Complex Setup**: Implementing MPC systems requires cryptographic and distributed systems expertise, posing adoption hurdles MediumDatatas.
- **Limited Expressiveness**: Early implementations targeted basic statistical tasks; complex or non-linear analytics remain challenging.
- **Bandwidth Demands**: MPC protocols often require frequent data exchanges, increasing network costs.

VI. RESULTS AND DISCUSSION

- **Practical Deployment**: The web-based MPC service successfully supported sensitive wage analytics collaboration in real-world settings, maintaining usability and privacy OpenBU.
- **Scalable Analytics with Conclave**: Conclave enabled processing of "big data" queries by decomposing them smartly into local vs. secure steps—achieving performance improvements of orders of magnitude over pure MPC frameworks arXiv.
- These outcomes confirm that MPC for AaaS is viable, particularly when designs emphasize usability and split workloads to optimize performance.

VII. CONCLUSION

Pre-2020 research reveals that **Secure MPC can serve as a robust foundation for Analytics-as-a-Service**, balancing privacy and insight. Lightweight tools proved accessible in real settings, while hybrid architectures like Conclave extended applicability to big-data scenarios. Despite performance and complexity challenges, early successes suggest MPC's potential to redefine secure analytics.

VIII. FUTURE WORK

- **Optimization of MPC Protocols**: Focus on reducing computational and communication loads to support real-time, scalable analytics.
- **User-Friendly Platforms**: Build turnkey MPC-enabled AaaS tools requiring minimal technical expertise.
- **Extended Analytics Support**: Expand support to complex machine learning tasks within MPC frameworks.
- **Hybrid Architectures**: Further development of systems blending local and secure computation judiciously.
- **Standardization Efforts**: Create frameworks and best practices for integrating MPC into AaaS platforms.

REFERENCES

1. Lapets, A.; Volgushev, N.; Bestavros, A.; Jansen, F.; Varia, M. (2016). *Secure Multi-Party Computation for Analytics Deployed as a Lightweight Web Application*. BU-CS-TR 2016-008. OpenBU
2. Volgushev, N.; Schwarzkopf, M.; Getchell, B.; Varia, M.; Lapets, A.; Bestavros, A. (2019). *Conclave: Secure Multi-Party Computation on Big Data*. arXiv preprint. arXiv
3. Overview of MPC in big-data analytics, including secret sharing, homomorphic encryption, garbled circuits Datatas
4. Historical context and formal definitions of MPC protocols Wikipedia
5. Challenges of MPC: computational and communication overhead, usability hurdles Medium+1GeeksforGeeks
6. Benefits of MPC in analytics pipelines and SaaS contexts