622.755 – Introduction to Cybersecurity Summer Term, 2022/23

Project Write Up

Ikram Ounadi 12245856

1 Outline

The focus of the project centers around Yao circuits [Yao], a remarkable technology that facilitates secure joint computations between two parties without compromising the privacy of their data. Throughout the course, we explored a range of private distributed computing methods, including Yao circuits, to understand their significance in safeguarding sensitive information. For my project implementation, I specifically developed the functionality for computing the sum of two sets using Yao circuits.

In this report, we will delve into the profound importance of Yao's protocol in the health domain, considering its implications from the perspectives of Social, Ethical, and Legal (SEL). To provide a comprehensive understanding, the report will follow a structured approach. Section two will present an extensive overview of Yao's protocol, highlighting its functioning and underlying principles. Moving forward, section three will showcase a compelling use case that vividly exemplifies the practical application of Yao's protocol in the health domain. In section four, the protocol will be thoroughly examined through the lenses of SEL. We will address the ethical considerations, and legal aspects associated with the implementation of Yao's protocol in healthcare. Lastly, the report will conclude by summarizing the key findings.

2 Yao's protocol: Overview

Yao's Two-Party Protocol is a computation protocol designed for two parties to jointly compute any function. It combines two essential components: a circuit garbling scheme and oblivious transfer. In simple terms, one party (referred to as P1) garbles a circuit by assigning random labels to each wire, including input and output wires. P1 then shares the garbled circuit and the labels for its input wires with the other party (P2). Both parties engage in an oblivious transfer protocol to transfer the labels corresponding to P2's inputs to P2. P2 then evaluates the garbled circuit using the input labels, resulting in the computation's output. [3]

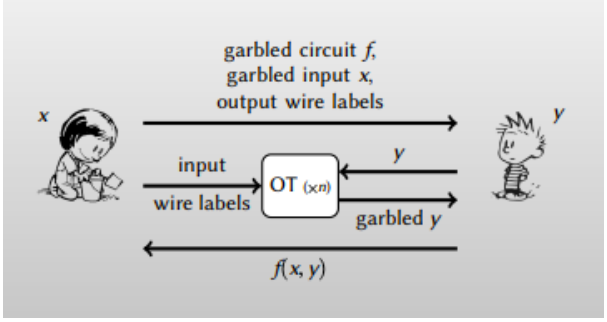

Figure 1: Yao's overview [5]

3 Yao's Protocol in health industry

Protecting data security and privacy is crucial in the healthcare industry.[4] Advanced cryptographic protocols have evolved to overcome these issues, and Yao's protocol has shown to be one of them. This protocol is very useful in the healthcare sector since it permits safe calculations between two parties without disclosing their confidential inputs.

One significant use of Yao's protocol is in protecting privacy while carrying out necessary calculations, such adding two values which is the approach I followed in my implementation project . Sensitive information is kept private while producing valuable insights by building a "garbled circuit" that depicts the intended calculation and assessing it using personal inputs. In the context of healthcare, privacy-preserving data analysis is a fundamental prerequisite for cooperation and research involving sensitive patient data analysis. Healthcare facilities can use Yao's protocol to compute aggregate statistics, such as the sum of various medical parameters, across multiple patient groups without disclosing individual patient data. This method allows for significant analysis while maintaining anonymity.

Now I'm going to discuss in general a real-world use case that I found intriguing; it uses precisely what I mentioned before.

3.1 Secure Patient Risk Stratification: A High-Performance Approach

The paper [2] I am going to discuss goes into the world of healthcare by offering advanced approaches in secure multi-party computing (MPC), with a particular emphasis on patient risk classification. Patient risk stratification is an important undertaking in population health management that tries to classify patients based on their anticipated healthcare requirements. Healthcare practitioners may efficiently allocate resources and conduct focused interventions to enhance patient outcomes by precisely identifying high-risk patients. However, due to data fragmentation, privacy issues, and regulatory limits, doing risk stratification across various healthcare institutions presents considerable hurdles.

To overcome these issues, the paper suggests using secure MPC protocols based on Yao's protocol and the integration of the sum function. Secure MPC allows several people to collaborate while protecting the privacy and security of sensitive medical data. Yao's protocol, a cutting-edge cryptographic technology, enables secure computing on encrypted data, allowing healthcare organizations to evaluate patient data collectively without disclosing individual-level information.

The integration of the sum function improves the analysis by safely aggregating pertinent patient data from many institutions. This allows for the merging of disparate data sources, resulting in a full picture of patients' comorbidities,previous healthcare resource consumption, and other risk factors. Traditional data aggregation solutions, such as centralized data repositories or trusted third parties, are resource-intensive, time-consuming, and potentially subject to security breaches.[2]

3.2 Secure Computation System for Healthcare Statistics

The purpose of this article [1] is to look at the possibility of secure computing, with an emphasis on Yao's protocol and the sum function, in allowing secondary usage of medical databases while protecting patient privacy.As medical record digitalization improves and data processing platforms evolve, such as the shift to cloud-based systems, there is a growing interest in utilizing medical records for reasons outside than their main usage. Due to the sensitive nature of patient information, however, strict security management is required to preserve privacy. While typical security control techniques, such as access restrictions and database encryption, are important for external access to databases, the article acknowledges that they may not provide total protection against risks and threats. These dangers include ineffective internal controls, administrative mistakes, and external assaults. Furthermore, even when medical records have been de-identified, there is a danger of re-identification when unique medical data is involved. Individuals may be uniquely recognized by comparing de-identified medical data to other databases, according to research.

4 Ethical and Legal Aspects of Secure Computation Systems in Healthcare.

It is critical to consider ethical and legal issues while building secure computing systems in healthcare. This section will look at the ethical issues and legal obligations that go along with these systems, highlighting their relevance in protecting patient privacy and ensuring compliance with relevant legislation.

4.1 Ethical Aspect

Yao's protocol and other secure computing systems stress patient autonomy and privacy. These systems ensure patient confidentiality and prevent illegal access or exploitation of medical information by utilizing modern encryption algorithms. These systems guarantee that individuals have power over how their data is used and shared while adhering to ethical values of privacy, fairness, and beneficence. This builds confidence between patients and healthcare professionals while also upholding ethical norms in the industry.

4.2 Legal Aspect

Secure computation systems must adhere to data protection regulations and confidentiality requirements. Laws provide guidelines for handling, sharing, and storing healthcare information. Implementing secure computation systems, including Yao's protocol, ensures compliance with these legal obligations. Failure to adhere to legal requirements can result in data breaches, legal consequences, and potential harm to patients.

4.3 Risks of Misusing Secure Multi-Party Computation

When sensitive patient data is exchanged without a genuine need or sufficient authorization, this is an example of an unreasonable usage of secure multi-party computation in healthcare. In this scenario, healthcare institutions may collaborate and do collaborative analysis utilizing secure computing platforms without regard for ethical or legal concerns. As a result of patient information being accessible to many parties without proper explanation or protections, this might result in privacy violations.

5 Conclusion

Finally, my project focused on the implementation of Yao's protocol in secure computing systems, emphasizing its usefulness and possible advantages in real-world healthcare applications. Yao's technique provides useful solutions in the healthcare sector by enabling collaborative analysis while protecting patient privacy. However, it is critical to underline the importance of ethical issues and legal compliance. Responsible patient data management, clear norms, and effective data governance policies are critical to ensuring safe computation systems' ethical and legal compliance. Healthcare companies may realize the full potential of secure computation while protecting patient privacy and sustaining confidence by establishing a balance between technology improvements and ethical-legal frameworks.

References

[1] Koji Chida, Gembu Morohashi, Hitoshi Fuji, Fumihiko Magata, Akiko Fujimura, Koki Hamada, Dai Ikarashi, and Ryuichi Yamamoto. Implementation and evaluation of an efficient secure computation system using 'r' for healthcare statistics. *Journal of the American Medical Informatics Association (JAMIA)*, 21(e2):e326–e331, 2014.

[2] Xiao Dong, David A. Randolph, Chenkai Weng, Abel N. Kho, Jennie M. Rogers, and Xiao Wang. Developing high performance secure multi-party computation protocols in healthcare: A case study of patient risk stratification. *Journal of Healthcare Informatics*.

[3] Sanjam Garg et al. Secure computation with yao's garbled circuits. *UC Berkeley*, 2016.

[4] Kundan Munjal and Rekha Bhatia. Secure computation system for healthcare statistics. *Journal of Medical and Biological Engineering*, 2022.

[5] Mike Rosulek. Cryptabit: Secure computation made easy. `https://web.engr.oregonstate.edu/~rosulekm/cryptabit/1-overview.pdf`, 2016.