Homomorphic Encryption: Revolutionizing Data Security in the Digital Age

The Social Construction of Homomorphic Encryption: Impacts and Implications Across Stakeholder Groups

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By
Jonghyun Lee

November 8, 2024

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISORS

Prof. Gerard J. Fitzgerald, Department of Engineering and Society

Introduction

In the realm of cryptography, Homomorphic Encryption (HE) emerges as a transformative technology, promising to revolutionize data security in our increasingly digital world. As organizations and individuals grapple with the ever-present threat of data breaches, HE offers a novel solution that could fundamentally alter our approach to data protection and utilization. Consider the current landscape of data security: In conventional systems, data must be decrypted for processing, creating vulnerabilities at every point of computation. HE, however, presents a paradigm shift. It enables computations on encrypted data without the need for decryption, maintaining data confidentiality throughout the entire process. This capability has profound implications for various sectors, from healthcare and finance to government and private enterprise.

The potential applications of HE are vast and diverse. In medical research, for instance, it could facilitate the analysis of sensitive patient data across multiple institutions without compromising individual privacy. In the financial sector, it could enable sophisticated fraud detection algorithms to operate on encrypted financial records, enhancing security while preserving client confidentiality. As cloud computing continues its exponential growth – with market projections reaching hundreds of billions of dollars – the need for robust security solutions becomes increasingly critical. HE aligns perfectly with this trend, offering a method to harness the power of cloud computing while maintaining unprecedented levels of data privacy.

However, the implementation of HE is not without challenges. Technical hurdles, such as computational overhead and efficiency, must be addressed. Moreover, the widespread adoption of HE will require a shift in organizational practices and regulatory frameworks. This paper aims to explore the technical intricacies of HE, its potential applications across various sectors, and its

broader societal implications. We will examine how this cutting-edge technology is not merely a tool for data scientists and cryptographers, but a key that could unlock a future where privacy and technological progress coexist harmoniously.

As we stand at the threshold of this new era in data security, we invite readers to embark on a journey through the forefront of cryptography. We will delve into how HE is poised to redefine the landscape of data security, one encrypted computation at a time, and consider its potential to shape our digital future.

Technical Research

Homomorphic Encryption (HE) is a revolutionary advancement in cryptography that promises to transform data security. Unlike traditional encryption methods that require decryption for processing, HE enables computations on encrypted data without compromising confidentiality. This allows direct operations on ciphertexts, producing encrypted results that, when decrypted, match the output of operations on the original plaintext (Gentry, 2009).

To grasp this complex concept, consider a simplified analogy: imagine a special lockbox that not only protects items inside but also allows manipulation without opening. If you put two numbers in separate lockboxes and want to add them, you could shake both boxes in a specific way, causing the numbers inside to combine. When you eventually open the box, you get the sum of the original numbers. This is essentially how homomorphic encryption works, but with highly complex mathematical operations instead of shaking boxes. HE addresses a critical challenge in information security, particularly in cloud computing environments where sensitive data processing is essential. With HE, encrypted values E(a) and E(b) can be computed to E(a+b)

without decryption, maintaining data privacy throughout the entire process (Yi et al., 2014, pp. 28-29). This capability is invaluable as cloud services often involve storing and processing sensitive information on remote servers, which can pose significant security risks. The adoption of cloud computing has demonstrated significant economic advantages for businesses and organizations. Gartner projects the global public cloud services market to grow 23% in 2021, reaching $332.3 billion (Gartner, 2021). This rapid growth, driven by cost savings and operational efficiencies, underscores the need for robust security solutions like HE across industries.

In conventional encryption schemes, data must be decrypted before any operations can be performed, forcing users to sacrifice privacy when utilizing cloud services. HE, however, allows third parties to operate on encrypted data without decryption, enabling secure outsourcing of complex computations while maintaining data confidentiality. This is crucial in today's always-on, Internet-centric world, where data privacy plays an increasingly significant role. For highly sensitive systems such as online retail and e-banking, HE offers a promising solution to protect users' accounts and assets from malicious third parties. Unlike the current norm of sharing encryption keys with service providers and cloud operators, HE allows users to maintain control over their sensitive data's privacy, even when utilizing cloud services. This approach effectively mitigates risks associated with untrusted providers retaining sensitive data and user credentials long after the service relationship ends (Acar et al., 2018).

These advancements are paving the way for broader adoption of HE in real-world applications. In healthcare, HE can enable secure analysis of patient data across multiple institutions, accelerating medical research while maintaining patient privacy. In finance, it can facilitate secure multi-party computations, allowing banks and financial institutions to

collaborate on fraud detection and risk assessment without exposing sensitive client data. As Deloitte points out in their 2021 report, cloud adoption is no longer just an IT concern but a key business strategy impacting entire organizations (Deloitte, 2021). HE technology aligns perfectly with this trend, offering a solution that addresses both the operational benefits of cloud computing and the critical need for data security in the digital age.

As HE continues to evolve, it has the potential to revolutionize how we handle and process sensitive information, ensuring end-to-end data privacy from end-devices to end-users. Ongoing research and development in this field promise to unlock new possibilities for secure data processing across various industries. By leveraging HE, organizations can confidently embrace digital transformation, driving innovation and efficiency while upholding the highest standards of data protection in our increasingly interconnected world.

STS Research

Based on the principles of the social construction of technology (SCOT), the connection between society and technology will be presented in this section (Bijker, Wiebe E., 2015). Regarding the potential roles of HE in leveraging data security level and its applications applied in various social groups, the SCOT theory offers an appropriate lens. HE presents a new shift in

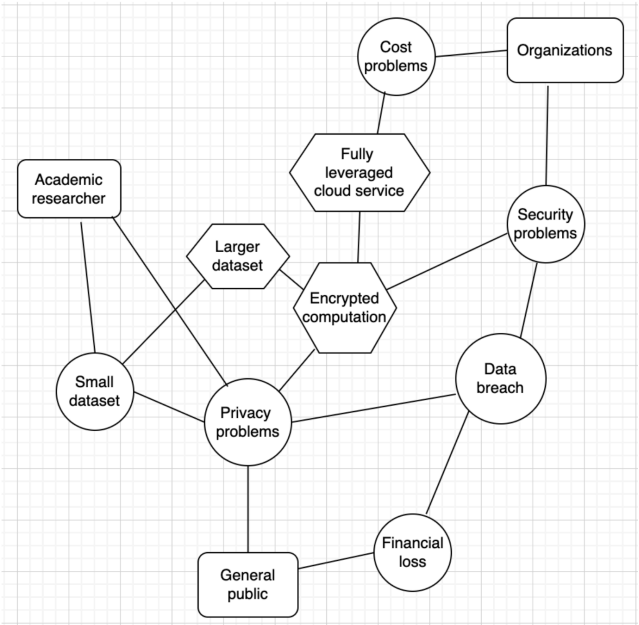

Figure 1: A social construction of technology (SCOT) diagram illustrating the relationship between homomorphic encryption and various social groups.

data computation and involves various social groups, including researchers, organizations, and the public (Figure 1).

Academic researchers represent a significant stakeholder group benefiting from HE. The new encryption method enables researchers to perform computations on encrypted data, allowing them to access and analyze large volumes of data sets without violating privacy. The potential of HE in expanding study capabilities is already being demonstrated in various fields. Research with increased datasets will lead to research findings with higher credibility and reliability, as larger sample sizes typically result in more robust statistical analyses and more generalizable results (Button et al., 2013).

Research conducted with unprecedentedly huge datasets enabled by HE will have the power to positively impact people's lives worldwide, which makes the general public as another stakeholder. For instance, a study conducted in the field of bioinformatics utilized HE to securely analyze genomic information of a large population to reliable results (Bonte et al., 2018). The researchers developed solutions that scale logarithmically with the number of subjects, allowing for efficient analysis of genome-wide association studies (GWAS) as population sizes grow. They also proposed a new masking-based comparison method that enables efficient comparisons in the HE setting without compromising data privacy. This advancement demonstrates the potential of HE in accelerating genomic research while maintaining strict privacy standards, potentially leading to breakthroughs in understanding complex diseases and developing personalized treatments.

In the perspective of organizations managing users' credential data, the application of HE is a lucrative business opportunity. Fully homomorphic encryption allows data to remain encrypted at all times, enabling it to be shared even in untrusted domains of the cloud. As a

result, organizations can not only enhance their data security levels but also fully leverage the economic benefits of cloud services. Beyond these immediate financial benefits, the adoption of homomorphic encryption can enhance customer loyalty and trust. If companies gain trust from customers, they can turn data-driven innovation and data privacy into competitive advantages (Schäfer et al., 2023). This approach aligns with the growing public awareness of privacy issues and the importance of data security in the digital age.

The improved security levels in the digital world and fine quality research outcomes position the general public as the third major stakeholder. Data breaches resulting from inadequate security measures often leave the general public bearing the brunt of the damage. A stark example of this is the Equifax data breach in 2017, which exposed sensitive personal information of approximately 147 million people. This breach resulted in a settlement of up to $700 million, including $425 million to help affected consumers (Federal Trade Commission, 2019). However, the upgraded security level provided by HE can reduce the risks associated with data breaches for the general public. With the adoption of HE, the general public can be largely freed from potential financial losses due to data breaches, ensuring their residence in a safer digital world where their personal information remains secure.

The application of homomorphic encryption demonstrates the intricate relationship between technology and society, as outlined by the Social Construction of Technology (SCOT) theory. The widespread adoption of homomorphic encryption could lead to a paradigm shift in how data is handled, processed, and protected across various sectors of society. This technological advancement not only addresses current data security challenges but also paves the way for innovative research and business practices, ultimately contributing to the improvement of people's lives.

Conclusion

Based on the comprehensive analysis of Homomorphic Encryption (HE) from both technical and societal perspectives, we can draw several significant conclusions: The research findings illuminate the performance capabilities, computational costs, and accessibility of HE algorithms across various sectors. The technical analysis reveals that HE addresses critical challenges in information security, particularly in cloud computing environments, by enabling computations on encrypted data without compromising confidentiality. This capability is especially valuable as cloud services increasingly involve processing sensitive information on remote servers.

Integrating these technical insights with the STS analysis demonstrates the profound societal implications of HE. By making pragmatic HE methodologies more affordable and accessible, this technology has the potential to democratize data security, allowing individuals and organizations across different socioeconomic strata to enjoy enhanced protection of their sensitive information while still benefiting from data-driven insights and services. Moreover, the research underscores the alignment of HE with broader trends in cloud adoption and digital transformation. As organizations increasingly rely on cloud services for operational efficiency and cost savings, HE offers a solution that addresses both the economic benefits of cloud computing and the critical need for data security in the digital age.

Looking forward, the ongoing development of HE promises to unlock new possibilities for secure data processing across various industries. By enabling organizations to confidently

embrace digital transformation without compromising on data protection, HE has the potential to reshape our approach to data security in our increasingly interconnected world.

In conclusion, this research not only advances our understanding of HE's technical capabilities but also illuminates its role in addressing societal concerns about data privacy and security. As HE continues to evolve, it stands as a testament to how technological innovations can be harnessed to create a more secure and equitable digital future for all.

References

Gentry, C. (2009). A fully homomorphic encryption scheme [Doctoral dissertation, Stanford University]. Stanford Digital Repository. https://crypto.stanford.edu/craig/craig-thesis.pdf

Yi, X., Paulet, R., & Bertino, E. (2014). Homomorphic Encryption and Applications. SpringerBriefs in Computer Science. https://www.semanticscholar.org/paper/Homomorphic-Encryption-and-Applications-Yi-Paulet/4be948fc9dc533d11497a38b76f65076ffb89cbd

Gartner. (2021, April 21). Gartner forecasts worldwide public cloud end-user spending to grow 23% in 2021. https://www.gartner.com/en/newsroom/press-releases/2021-04-21-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-23-percent-in-2021

Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2019). A Survey on Homomorphic Encryption Schemes: Theory and Implementation. ACM Computing Surveys, 51(4), Article 79. https://doi.org/10.1145/3214303

Deloitte. (2021). Cloud computing: More than a CIO conversation. https://www2.deloitte.com/us/en/insights/industry/technology/technology-media-and-telecom-predictions/2021/cloud-migration-trends-and-forecast.html

Bijker, W. E. (2015). Technology, social construction of. In J. D. Wright (Ed.), International Encyclopedia of the Social & Behavioral Sciences (2nd ed., pp. 135-140). Elsevier. https://www.sciencedirect.com/science/article/pii/B9780080970868850382

Button, K. S., Ioannidis, J. P. A., Mokrysz, C., Nosek, B. A., Flint, J., Robinson, E. S. J., & Munafò, M. R. (2013). Power failure: why small sample size undermines the reliability of

neuroscience. Nature Reviews Neuroscience, 14, 365–376. https://doi.org/10.1038/nrn3475

Bonte, C., Makri, E., Ardeshirdavani, A., Simm, J., Moreau, Y., & Vercauteren, F. (2018). Towards practical privacy-preserving genome-wide association study. BMC Bioinformatics, 19, 537. https://doi.org/10.1186/s12859-018-2541-3

Schäfer, F., Gebauer, H., Gröger, C., Gassmann, O., & Wortmann, F. (2023). Data-driven business and data privacy: Challenges and measures for product-based companies. Business Horizons, 66(4), 493-504. https://doi.org/10.1016/j.bushor.2022.10.002

Federal Trade Commission. (2019). Equifax data breach settlement. https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement