Mystiko - A Private Query System & Marketplace in a Zero-Trust World

Sriram Tolety & Kevin Li

1 May, 2023

MYSTIKO

Group Advisor: Boon Thau Loo <boonloo@seas.upenn.edu>
Secondary Faculty Advisors: Andreas Haeberlen <ahae@cis.upenn.edu>
Group Members: Kevin Chen <kevc528@seas.upenn.edu>, Maxwell Du <maxdu@seas.upenn.edu>, Kevin Li <kevinmli@seas.upenn.edu>, Rishi Madabhushi <rmada@seas.upenn.edu>, Sriram Tolety <tsr23@wharton.upenn.edu>

Executive Summary

The demand for high-quality data and the importance of preserving individual privacy have become essential aspects of modern data analytics. Mystiko is an innovative company that aims to revolutionize the way data is published and distributed in a zero-trust world. By utilizing cutting-edge computational techniques, such as differential privacy and trusted execution environments (TEEs), Mystiko seeks to democratize access to data by offering a secure and private method for interacting with uploaded data. Mystiko, a centralized data marketplace, aims to democratize access to robust, vast, and high-quality data while maintaining the privacy of the individuals and companies whose data is being stored. By offering large-scale, differentially private queries, Mystiko provides a unique platform for businesses to share and access valuable data, contributing to social good and creating new revenue streams. This report provides a detailed analysis of Mystiko's technical and business components, discussing its value proposition, stakeholders, customer segmentation, market research, and competition.

1. Technical Overview

1.1 Differential Privacy

Differential privacy is a mathematical concept that ensures data privacy by introducing randomness into queries made on datasets. This process allows data publishers to control the level of privacy associated with their datasets while maintaining the accuracy of query results. Mystiko employs differential privacy to give dataset uploaders complete control over the privacy settings for their data. Differential Privacy (DP) is a cutting-edge privacy-preserving technique that adds a controlled amount of noise to data queries to protect the privacy of individual records within a dataset. The primary goal of differential privacy is to enable data analysis and sharing without compromising the privacy of individuals whose information is included in the dataset. By doing so, DP allows for the extraction of valuable insights from data while ensuring that the risk of re-identification or privacy breaches is minimized. This is achieved through the use of carefully designed algorithms that add a specific level of randomization to the query results, which ensures that the presence or absence of any single individual in the dataset has a negligible impact on the outcome.

A key advantage of differential privacy is that it allows data providers to control the degree of privacy protection by adjusting the amount of noise added to the data. This level of control enables a fine-grained balance between privacy and utility, as data custodians can choose an appropriate privacy level based on the sensitivity of the data and the desired accuracy of the query results. In the context of Mystiko's data marketplace, the implementation of differential privacy not only provides robust privacy guarantees for users, but also empowers them to customize the privacy settings for their datasets, offering a unique and valuable selling point in the competitive landscape of data marketplaces.

1.2 Trusted Execution Environments (TEEs)

TEEs provide a secure environment for data storage and processing, ensuring that data remains encrypted and protected from unauthorized access. Mystiko utilizes TEEs to store uploaded datasets, allowing both data uploaders and users to operate in a zero-trust paradigm. Trusted Execution Environments (TEEs) are secure areas within a processor that protect sensitive data and code from unauthorized access or tampering. These environments provide an additional layer of security, ensuring that the data and applications within the TEE are isolated from the rest of the system. This isolation helps maintain data confidentiality and integrity, even in the presence of compromised software or hardware outside the TEE. TEEs are widely used in various industries, including finance, healthcare, and telecommunications, to safeguard critical data and processes. By incorporating TEEs into its platform, Mystiko ensures a zero-trust paradigm, providing users with enhanced security and privacy when buying or selling datasets in the data marketplace.

1.3 Data Upload and Query Execution

Mystiko has developed a secure and user-friendly system for uploading datasets and executing queries on publicly available datasets. The process begins with users uploading their datasets through encrypted channels, ensuring that the data is protected during transmission. Once the data is uploaded, it is stored within Trusted Execution Environments (TEEs), which provide a secure and isolated environment for data processing and storage. This approach minimizes the risk of unauthorized access or data breaches, as even Mystiko cannot access the data stored within the TEEs.

Once the datasets are securely stored, Mystiko's platform enables users to request access to publicly available datasets and execute queries on them. To ensure data privacy, Mystiko leverages differential privacy techniques, which add a controlled amount of noise to the query results, thereby protecting the privacy of individual records within the dataset. This allows for valuable insights to be derived from the data while maintaining robust privacy guarantees.

1.4 Query Support

Mystiko has worked to provide support for a variety of differentially private (DP) queries on datasets, enabling the extraction of valuable insights while maintaining data privacy. This is achieved through the use of various DP algorithms that return statistical measures such as count, mean, mode, variance, and standard deviation while ensuring data privacy is preserved.

The DP count function, for example, returns the differentially private count of the number of rows in a column by adding Laplacian noise to the true count. This is based on the geometric probabilistic mechanism. Similarly, the DP mean function calculates the differentially private mean of a column using the algorithm described in the book "Differential Privacy: From Theory to Practice." It returns a value within the range of the data, while also taking privacy parameters into account. The DP mode function computes the differentially private mode of a column based on the same book's example, ensuring that the result maintains data privacy by using an exponential mechanism. Additionally, the current codebase supports more advanced DP queries, such as linear regression, k-means clustering, and logistic regression. These advanced queries enable users to perform privacy-preserving data analysis and modeling, allowing them to derive valuable insights from sensitive datasets without compromising the privacy of individual records.

Based on the extensive user interviews and client interviews conducted which will be discussed further down below, Mystiko is currently working towards building general SQL query support, allowing nearly all free-form SQL queries to be executed in a differentially-private manner, using proprietary DP algorithms developed in-house.

1.5 System Design

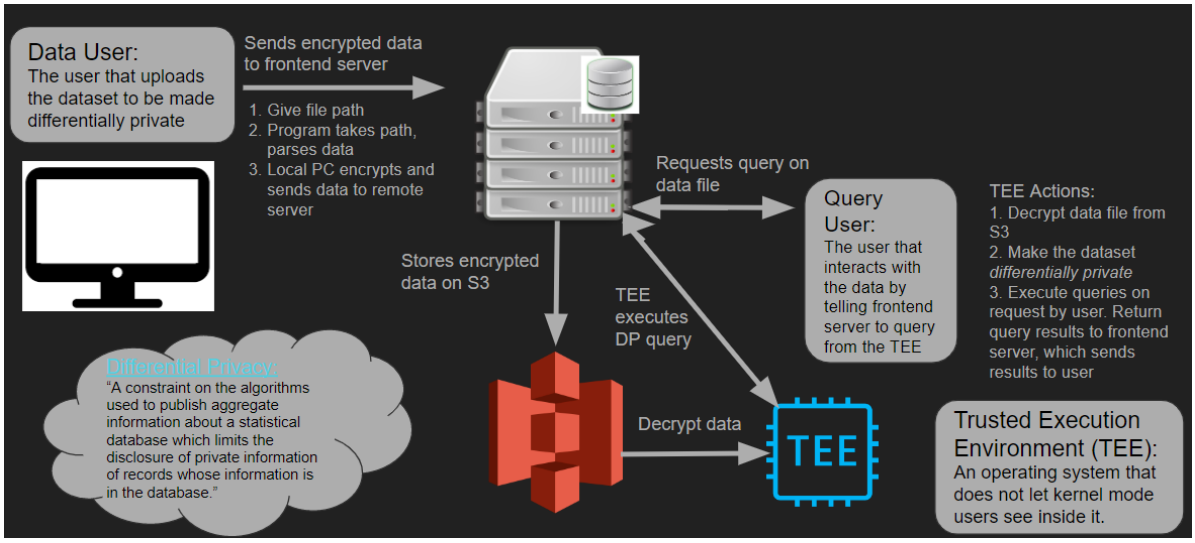

Figure 1: System Architecture of Mystiko

The system architecture of Mystiko has been designed to be robust, scalable, and flexible in allowing for the development of future features.

The frontend application is structured using a modular approach, dividing the application into reusable components and containers. The application employs React Hooks, which simplifies state management and side effects in functional components. Additionally, the frontend leverages Redux as a state management library, using actions and reducers to manage global state changes consistently and predictably. For styling and user experience, the Mystiko frontend uses Material-UI and Tailwind CSS. To handle user authentication, the frontend makes use of JSON Web Tokens (JWT) and browser storage for maintaining user sessions. Overall, the Mystiko frontend showcases the use of modern web technologies and best practices to create a secure, user-friendly, and responsive interface for data analysis while prioritizing data privacy.

We have successfully developed the backend functionality within the frontend server to accept TCP socket connections and offer two services: data upload and query execution. Our integrated data upload service is able to read the stream of data uploaded as a CSV from the frontend, and transmit it using TCP to our data warehouse, wherein it is stored on Amazon AWS S3 servers. Mystiko has integrated additional layers of security to the entire system by building a custom end-to-end encryption scheme for the entire pipeline. The only time data is unencrypted within the scope of Mystiko's service is within the TEE during query execution, wherein Mystiko provides hardware-level guarantees of security and privacy. This means that the data can be directly stored on S3 AWS, eliminating the need for storage on the TEE

which is very expensive. The encryption key is public and used by the frontend, while the decryption key is private and stored on the TEE. To optimize performance, Mystiko is also implementing caching of fully decrypted files on the backend TEE to avoid having to decrypt the data each time a query is made. Additionally, a Postgres database on RDS includes metadata about the data files, making it easier for users to understand what data can be queried and providing the capability to showcase insights on the data marketplace regarding aggregate usage statistics and other relevant information. On the other hand, the query execution service reads the stream of data, containing the file to be queried and the SQL query, and uses the popen() system call to run a DP python process that returns the output via a pipe. The results are then sent back over the socket.

To simplify the use of these services, Mystiko has developed a client class that acts as an API for the two integrated backend services and can be used within the frontend server itself. Lastly, Mystiko's frontend server, which now also serves as the backend, uses HTTP servers built with the CROW framework in C++. It handles HTTP requests for querying and uploading data, as well as providing routes to render frontend pages that utilize the HTTP handlers. This unified server architecture streamlines data processing and enhances the efficiency of the system.

2. Business Overview

2.1 Value Proposition

Mystiko's value proposition is built around two key concepts that address the challenges faced by organizations and individuals when sharing and analyzing data:

Differential privacy: Differential privacy ensures that individual data points cannot be re-identified while preserving the overall utility of the dataset for analysis. By integrating differential privacy into its platform, Mystiko allows dataset uploaders to finely control the privacy settings for their data, striking a balance between privacy protection and data utility. This level of customization empowers users to maintain control over their sensitive information while benefiting from the strong privacy guarantees backed by extensive research literature. As a result, users can share and analyze data with confidence, knowing that their privacy is protected.

Zero-trust paradigm: Mystiko's implementation of Trusted Execution Environments (TEEs) facilitates a zero-trust environment where neither data uploaders nor users need to trust intermediaries, such as data aggregators or service providers. TEEs are secure areas within a processor that protect sensitive data from

unauthorized access and tampering, even when the surrounding system is compromised. By leveraging TEEs, Mystiko ensures that sensitive data is protected from potential threats, both internal and external. This approach overcomes the limitations of traditional privacy mechanisms that rely on centralized data aggregators or trust in third-party service providers, fostering a more secure and private ecosystem for data sharing and analysis.

2.2 Stakeholders

Mystiko's platform caters to a diverse range of stakeholders who have vested interests in data protection and privacy:

2.2.1 Data publishers

These include organizations and individuals who contribute datasets to the platform. By using Mystiko's secure and privacy-preserving platform, data publishers can share their data with others for analysis while maintaining control over its privacy. This capability allows data publishers to monetize their data assets while mitigating the risks associated with data breaches or unauthorized access.

2.2.2 Users executing queries on datasets

This group consists of data analysts, researchers, and other professionals who rely on data-driven insights to make informed decisions. Mystiko provides these users with a secure environment in which they can access and analyze datasets without compromising the privacy of the underlying data. By doing so, Mystiko enables users to gain valuable insights from previously inaccessible data sources, driving innovation and fostering a data-driven culture.

2.2.3 Individuals and entities whose data make up the datasets

This group refers to the data subjects whose information is included in the datasets published on Mystiko's platform. By providing robust privacy guarantees through the use of differential privacy and TEEs, Mystiko ensures that the privacy of these individuals and entities is protected, promoting trust and encouraging participation in the data-sharing ecosystem.

2.3 Customer Segmentation

Mystiko serves three distinct user segments that stand to benefit from secure and private data access and analysis:

Large corporations: Large corporations often possess vast amounts of sensitive data that can be valuable for analysis but must be protected from unauthorized access or breaches. Mystiko's platform offers these organizations the opportunity to securely share and analyze their data without compromising privacy. By leveraging Mystiko's privacy-preserving technologies, corporations can monetize their data assets, collaborate with other organizations, and gain valuable insights, all while maintaining control over their data and adhering to regulatory requirements.

Researchers: Researchers, particularly those in academia and scientific institutions, require access to large datasets to conduct their studies and advance knowledge in their respective fields. However, gaining access to sensitive data can be challenging due to privacy concerns and regulatory restrictions. Mystiko's platform addresses these challenges by enabling researchers to access and analyze data in a privacy-preserving manner. This capability allows researchers to derive valuable insights from previously inaccessible data sources, fostering innovation and contributing to the advancement of knowledge.

Individuals: As data subjects, individuals have a vested interest in the protection of their personal information. They are increasingly concerned about the ways their data is collected, stored, shared, and used by various organizations. Mystiko's platform caters to the needs of individuals by providing a secure environment where their data can be shared and analyzed without compromising their privacy. By participating in the Mystiko ecosystem, individuals can benefit from the democratization of data access and the development of new products and services that rely on data-driven insights.

Furthermore, Mystiko's platform can serve as an enabler for smaller organizations and startups that might not have the resources or expertise to implement advanced data privacy solutions internally. By offering a comprehensive and user-friendly platform, Mystiko allows these smaller entities to benefit from secure data sharing and analysis, driving innovation and fostering a data-driven culture across various industries.

By focusing on the unique needs of its customer segments, Mystiko can establish itself as a trusted and reliable partner for organizations and individuals seeking to harness the power of data while maintaining the highest levels of privacy and security.

2.4 Intellectual Property

Mystiko's innovative approach to data privacy and security incorporates several novel techniques and technologies that could potentially qualify as intellectual property (IP). These include the unique combination of differential privacy and Trusted Execution Environments (TEEs) to create a secure,

private, and customizable data sharing platform. Additionally, the platform's underlying algorithms, protocols, and system architecture may also constitute valuable IP, providing Mystiko with a competitive edge in the data marketplace sector.

Recognizing the value of these innovations and the importance of protecting the company's IP, Mystiko has already engaged with legal counsel from the University of Pennsylvania to explore patent opportunities and safeguard any potential IP. This proactive approach will not only help to secure Mystiko's competitive position in the market but also prevent unauthorized use of the company's proprietary technologies and know-how. By working closely with experienced lawyers who specialize in IP and patent law, Mystiko can ensure that its innovations are adequately protected, enabling the company to maximize the value of its IP portfolio. This protection will further enhance Mystiko's reputation as a leader in the data privacy and marketplace space, attracting interest from potential customers, investors, and partners who recognize the company's commitment to innovation and IP protection. By maintaining a strong relationship with legal counsel and staying up-to-date on the latest developments in IP law, Mystiko can safeguard its valuable innovations and ensure that its cutting-edge technologies remain at the forefront of the data privacy and data-sharing marketplace sectors.

3. Market Research and Competition

3.1 Technologies for Data Privacy

Differential privacy is a leading privacy-preserving technology that adds carefully calibrated noise to the results of data analysis, ensuring that individual data points cannot be identified or reverse-engineered. This approach provides robust privacy guarantees, allowing data to be shared and analyzed without revealing sensitive information about individuals or organizations. Differential privacy has been adopted by major technology companies like Apple, Google, and Microsoft, and is considered a state-of-the-art technique for protecting data privacy while enabling valuable insights to be derived from the data.

Homomorphic encryption is another powerful technology for data privacy, enabling computations to be performed directly on encrypted data without the need for decryption. This technique allows data to be securely stored and processed, with the results of any computations remaining encrypted and private. While homomorphic encryption is a promising approach to data privacy, it has significant computational overhead, limiting its practical applications for large-scale data analysis.

Standard encryption schemes, such as AES and RSA, are widely used for protecting data at rest and in transit. These encryption methods ensure that data can be securely stored and transmitted, but they do not allow for any computation on the encrypted data. As a result, data must be decrypted before it can be analyzed, creating potential privacy risks and exposing sensitive information.

Mystiko's platform combines the strengths of differential privacy and Trusted Execution Environments (TEEs) to create a powerful, flexible solution for data privacy. By leveraging differential privacy, Mystiko provides customizable privacy settings that allow data publishers to control the trade-off between data utility and privacy. In addition, the use of TEEs enables a zero-trust paradigm, ensuring that data is protected from unauthorized access, even by Mystiko itself or other intermediaries. This unique combination of technologies sets Mystiko apart from other data marketplaces, offering a secure and versatile platform for data sharing and analysis.

3.2 Competitors

There are many offerings from both emerging startups and established technology giants which are growing in this space. Examples of personal data marketplaces include firms such as Datum and SynapseAI, while examples of B2B data marketplaces are firms such as Snowflake, Datarade, and Axon. While firms such as Datum market their services as allowing users control of their data, Mystiko also allows users to control the degree of privacy afforded - this enabled a much finer-grained control of privacy which existing competitors do not offer. Furthermore, Datum’s model relies on the DAT token underlying the entire system, introducing increased computational expenses and increased overhead for users when compared to Mystiko. However, it is important to note that usage of blockchain technology does also allow for a zero-trust paradigm, but Mystiko believes again that first, users have stronger trust in existing hardware firms such as Intel and AMD which underlie our TEE technology when compared to blockchain technologies which are still emerging, and second, that the increased computational cost of Datum will allow Mystiko to operate with significantly lower costs. SynapseAI is built using similar blockchain technology, but is targeted toward ML research; their product platform included internally-developed ML models etc, which Mystiko believes will lead to increased costs; there are already many firms which offer ML outsourcing, and so Mystiko believes that SynapseAI’s positioning as attempting to outsource both data collection as well as ML model development is not needed - this is evidenced by their slow user growth which forced the sale of their technology to Microsoft, which killed the entire data marketplace model that SynapseAI was striving towards.

We see larger B2B firms such as Snowflake and Datarade as primarily offering data warehousing services, but Mystiko also differentiates itself from these services in its use of differential privacy as well as TEEs for a zero-trust paradigm which these firms do not allow for. These firms do not offer privacy solutions beyond what is currently regulated by governments, such as GDPR pushing companies to limit data collection and storage. Mystiko's use of DP and TEEs is a revolutionary leap forward in this regard. Mystiko's new technology is an important differentiator as well as a barrier-to-competitiveness against these existing firms. Mystiko is developing proprietary differential-privacy algorithms and integration with custom TEEs to ensure that data privacy is ensured. The close interaction of encryption, differential privacy, and TEE hardware ensures a high barrier to entry from a competitive standpoint, limiting entry of larger firms into this product space.

3.3 User & Client Interviews

Mystiko's Minimum Viable Product (MVP) has been successfully built and deployed end-to-end, demonstrating the platform's potential to address the growing concerns surrounding data privacy, particularly in sensitive fields such as medicine. In particular, Mystiko chose to interview medical researchers since they have similar interest alignment. Mystiko hypothesized that medical researchers have an abundance of valuable collected and extracted data that is highly private, which would be difficult to share. Furthermore, preliminary empirical research showed that there were no immediate consolidated or intuitive ways to share data in the medical research space.

To validate the market potential and assess the level of interest among potential MVP users, Mystiko has reached out to approximately 200 individuals from Penn Medicine and nearby hospitals. The response has been overwhelmingly positive, with over 70% of those contacted expressing a keen interest in using the platform. Researchers have a lot of good data, which they are happy to share. However, they cannot share the data in its raw form due to privacy concerns. Furthermore, current systems are clunky and/or restrictive. This strong reception highlights the demand for robust data privacy solutions in academia and validates Mystiko's initial focus on this sector.

In terms of core takeaways, Mystiko gained valuable insight into the data collection and analytics processes, current data sharing protocol, types of data available and wanted, and current data sharing and transfer systems and their pain points.

3.3.1 Types of Data Used and Wanted

Frequently used and wanted data includes tabular data in the form of electronic health records and survey data. For this kind of data, Mystiko's system makes support for uploading and querying simple. Mystiko also interviewed some researchers who worked with time-series data (i.e. electrocardiogram) or image data (i.e. magnetic resonance imaging). For these data formats, Mystiko does not currently support algorithms on this kind of data. While differential privacy is indeed possible in these cases, this may be a long-term goal for Mystiko.

3.3.2 Data Sharing Protocols

The data sharing protocols are largely determined by who funds the researchers. Most commonly, if funding is through the NIH, the researcher must have a data sharing plan, but this can largely be any plan, with the eventual goal of the NIH being to collate a large and public data repository. Currently, researchers commonly cite currently available data sharing and transfer systems, such as Redcap, in their data sharing plans. However, as discussed earlier in section 3.2, current systems have multiple pain points and do not provide the same level of access combined with privacy guarantees, so Mystiko is in position to serve as the best answer for researchers' data sharing plans.

3.3.3 Data Analysis Methods

Mystiko gained information on what kinds of data analysis methods to support. In the current MVP, Mystiko supports mostly basic aggregation queries as well as standard machine learning algorithms like linear regression, logistic regression, and K-nearest neighbors. From user research interviews, Mystiko learned that medical researchers will frequently use methods such as generalized regressions, genomic equation modeling, as well as t-tests and ANOVAs. As Mystiko expands, one anticipates supporting all of these analysis methods with the same robust and private guarantees Mystiko currently provides.

To analyze this data, user interviews informed Mystiko that tools such as R and SAS were the most common, with some researchers slowly adopting newer tools such as Python. To this extent, Mystiko's systems currently only support queries in R, so these interviews suggest that an API that can be called in R might help Mystiko useability and approachability by medical researchers. Mystiko has already begun prototyping the ability to support free-form SQL queries, and transitioning this technology to also support R is one direction of feature development that Mystiko anticipates prioritizing in the future.

Another common request was to have the ability for Mystiko to join and concatenate datasets together. For example, if there are multiple datasets for a specific research question that have been collected by different researchers, it would be useful to have a system on the backend to concatenate the datasets

together. This is a feature that multiple medical researchers brought up unprompted, noting that current systems do not support tools like this. To this extent, Mystiko also anticipates developing the ability to concatenate similar datasets as a high-priority feature.

3.3.4 Moving Forward

Furthermore, over 90% of the positive responders have indicated their willingness to upload data to the platform, effectively addressing the initial supply challenge often faced by two-sided data marketplaces. This enthusiasm to contribute data underscores the trust and confidence that potential users have in Mystiko's approach to privacy and security. As the platform continues to gain traction, Mystiko is well-positioned to become a leading player in the data privacy and marketplace sectors, offering a valuable solution to the pressing issue of secure data sharing in academia and beyond.

4. Business Model

4.1 Costs

Mystiko currently utilizes Amazon AWS Nitro Enclaves, which are isolated compute environments that provide the TEEs Mystiko uses to process sensitive data. The cost of hosting compute power on Nitro Enclaves depends on several factors, including the number of vCPUs and the amount of memory used, as well as the length of time the compute resources are used. On average, Mystiko expects to pay anywhere from $0.08 to $0.16 per hour for each vCPU and $0.045 to $0.09 per GB of memory per hour. Hosting data warehouses in the cloud also involves costs that Mystiko will have to consider. In our current model, encrypted data will be stored in data warehouses in the cloud, greatly reducing costs from the user's end for interacting with the marketplace and reducing the direction for users when uploading and downloading data, as Mystiko can take care of the backend data warehousing. The cost of hosting a data warehouse in the cloud depends on several factors, including the size of the warehouse, the amount of data being stored, and the amount of compute power required to process the data. On average, Mystiko expects to pay anywhere from $0.25 to $5 per GB per month for data storage, and additional fees for data processing and data transfer.

In addition, Mystiko foresees additional costs (separate from the usual costs such as SG&A, etc.). It is probable to realize significant labor costs arising from paying engineers, especially in today's environment. In addition, Mystiko also has web-hosting costs to have a front-end for users to interact via the internet. However, this cost is minor in comparison to others listed previously.

4.2 Revenue Model

Option 1:

Mystiko facilitates the sales of data, allowing users to charge a price per query, either one that they set or dependent on how "private" the query is. Mystiko then takes a percentage of each query's fee. This can also be changed into a flat fee per number of queries, but from a financial perspective, the revenue will be dependent on the number of queries executed.

Option 2:

Mystiko facilitates the sales of data, charging users to buy datasets, and allowing datasets to be uploaded without cost. Then, for each dataset, Mystiko charges either a percentage of the cost or a flat fee per dataset. In this option, Mystiko models its revenue as dependent on the number of datasets bought, as opposed to queries then executed on the data itself. This will generate higher up-front revenue, but Mystiko sees option 1 as translating to sustained cash flows.

Option 3:

In this case, Mystiko can somewhat pivot to be more enterprise-focused, concentrating on warehousing the data as well as potentially, ML/AI models. This would then pivot Mystiko to be more focused on an Enterprise SaaS firm, enabling firms to better manage data privately. Mystiko would allow firms to either share data/models inter-firm or intra-firm, and differential privacy would enable serving both use-cases (for intra-firm, Mystiko can simply set the privacy thresholds to 0, whereas when selling to other firms, the firms/teams who are uploading/sharing the data can set their desired thresholds). Mystiko can sell this service with an upfront cost and recurring costs based on the amount of data stored.

Based on our user interviews, Mystiko is moving in a direction to offer both SAAS contracts as well as charging individual users upon executing queries. In the current MVP, Mystiko offers support to charge on a per-query basis, determined by the data uploader. Mystiko charges a fixed cost per query dependent upon the size of the dataset being queried, providing flexibility while maintaining margins as larger datasets will require more expensive computation in Mystiko’s backend servers.

4.3 Business Strategy

The company's initial focus is on targeting academia, with plans to expand to additional verticals in the future. This strategic decision is informed by the pressing need for secure and private data sharing solutions within the academic community, as well as the National Institutes of Health's (NIH) mandate requiring all grant holders to have a data-sharing plan in place. The firm plans to begin with a focus on

academia at large, due to the strong signal it would send other firms and potential clients in other verticals, if Mystiko is able to serve clients in a field with such sensitive data. In the long term, Mystiko envisions broadening its market to encompass business in all sorts of verticals, such as finance.

5. Conclusion

In conclusion, Mystiko's innovative approach to data privacy and security offers a unique value proposition that sets it apart from competitors in the data marketplace sector. By combining differential privacy with Trusted Execution Environments (TEEs), Mystiko provides a highly secure and customizable solution for data sharing and analysis, allowing stakeholders to benefit from the democratization of data access while maintaining robust privacy and security guarantees.

The platform caters to a diverse customer base, including large corporations, research organizations, and individuals, with a primary focus on research organizations and large corporations as they stand to gain the most from secure and private data access. By addressing the needs of these key customer segments, Mystiko has the potential to make a significant impact on the rapidly growing data economy.
As the demand for data-driven insights continues to increase, so too does the need for robust privacy and security solutions. Differential privacy, homomorphic encryption, and standard encryption schemes are some of the main technologies currently employed to address data privacy concerns. Mystiko's unique combination of differential privacy and TEEs not only provides customizable privacy settings but also ensures a zero-trust environment where both data uploaders and users do not need to rely on trust in intermediaries.

Mystiko faces competition from a range of players in the data privacy and marketplace sectors, including personal data marketplaces like Datum and SynapseAI, as well as B2B data marketplaces such as Snowflake, Datarade, and Axon. Despite this competition, Mystiko's focus on differential privacy and TEEs enables it to offer a more secure and customizable solution for data privacy, distinguishing it from other data marketplaces and providing a strong foundation for success.
As the market evolves, Mystiko must remain committed to innovation and continuous improvement, staying ahead of the curve in terms of privacy technologies and customer needs. This commitment will enable Mystiko to maintain its competitive edge and solidify its position as a leader in the data privacy and marketplace space. By fostering trust and collaboration amongst stakeholders, Mystiko will create a thriving ecosystem that drives value for all parties involved and contributes to the broader democratization of data access.

As the global data economy continues to expand, the importance of privacy and security cannot be overstated. Data breaches, privacy scandals, and increasing regulatory scrutiny have underscored the need for innovative solutions that protect sensitive information while still enabling organizations and individuals to harness the power of data. Mystiko’s unique approach to data privacy and security addresses these challenges head-on, providing a platform that empowers its users to share and analyze data with confidence, knowing that their privacy is protected. By staying true to its core principles of security, privacy, and customer-centricity, Mystiko has the potential to play a significant role in shaping the future of data privacy and access, driving positive outcomes for businesses, researchers, and individuals alike.

Ultimately, Mystiko's success will depend on its ability to adapt and evolve in a rapidly changing landscape, continually enhancing its platform and services to meet the needs of its customers and stay ahead of the competition. By staying focused on its mission to democratize data access while maintaining the highest standards of privacy and security, Mystiko can make a lasting impact on the data economy and help to shape a more secure, private, and inclusive future for all.