CLOUDSTRUCC INC.

SR&ED Technical Submission for Cloudstrucc

This submission outlines groundbreaking research and development work in data sovereignty and encryption technology. Our team has focused on solving fundamental challenges in digital identity management and data control across cloud platforms, pushing the boundaries of what's possible in secure data management.

Fiscal period that ended on September 30, 2023

Project Name: Digital Organization Vault

The Digital Organization Vault represents a revolutionary approach to data sovereignty in cloud environments. This project aims to fundamentally transform how users and organizations maintain control over their data across various SaaS platforms and cloud services, introducing novel encryption techniques and blockchain-based verification systems.

Project Anticipated Timeline

This multi-year research initiative reflects the complexity and scope of developing new encryption standards and data control mechanisms. The timeline accounts for multiple phases of research, development, and testing required to validate our innovative approaches to data sovereignty.

Start date: October 2020 **Completion date:** September 2025

Technological Uncertainties:

In pursuing this innovative approach to data sovereignty, we encountered several fundamental technological uncertainties that challenged existing paradigms in data security and control. These uncertainties stem from the complex interplay between encryption technologies, cloud platforms, and user requirements for seamless data access and control.

A fundamental challenge in current data security models is the inability to maintain persistent control over data once it leaves a user's direct possession. While existing technologies like DocuSign and Adobe Sign implement digital signatures and encryption, they don't provide true user-controlled data sovereignty, especially after data is stored in third-party SaaS platforms' databases.

Key technological uncertainties we are addressing include:

1. **Novel Encryption Character Integration:**
    - We are investigating whether it's possible to embed a specialized algorithmic key within standard character sets that can maintain encryption properties while meeting SaaS platform validation rules
    - Uncertainty exists around how to implement this "micro encryption artifact" at the character level without disrupting standard data validation patterns or causing system compatibility issues

- We need to determine if this encryption method can survive data transformation processes common in SaaS platforms while maintaining its integrity

2 **Decentralized Key Management:**

- We are exploring how to implement a distributed PKI system using ION2 blockchain technology that can manage multiple sub-keys while maintaining performance
- Uncertainty exists around scaling this system across different cloud providers (Azure, AWS, Salesforce) while maintaining consistent key synchronization
- We need to understand how to implement key revocation that renders stored data unusable without disrupting system operations

3 **Immutable Audit Trail Implementation:**

- Technical challenges exist in creating an algorithmically tamper-proof record of all data interactions, including keystroke-level changes
- We are uncertain how to implement coordinated attestation between employee and employer private keys without creating performance bottlenecks
- Need to determine how to maintain audit trail integrity across distributed systems while ensuring scalability

One challenge we encountered is that encrypted data may not meet SaaS platform validation rules. For example, an encrypted birthdate would fail a system expecting a standard date format. To solve this, we are building a shared trust model, enabling users and vendors to manage encrypted data smoothly. Vendors will also have tools to purge or relocate revoked data, respecting retention policies while allowing users to regain their data if they return to the service.

We are testing this mechanism with Azure Entra Verified ID and Microsoft Power Platform. Our goal is to enable secure, user-controlled data sharing without disrupting SaaS workflows, ensuring compatibility across platforms like Azure, Microsoft 365, Salesforce, and AWS.

We do not know whether Azure Entra Verified ID can scale across multiple cloud platforms. While it performs well in single-cloud environments, we were uncertain how to extend these workflows to hybrid or multi-cloud systems like AWS without latency or performance issues. Our goal is to ensure seamless identity management across platforms without compromising security or user experience.

We are uncertain how to synchronize key rotations across distributed environments without disrupting access. Our vault's encryption requires timely key rotations, but existing technologies struggle to rotate keys without interrupting active sessions. We need to understand why synchronization issues arise across cloud providers like Azure and AWS and how to maintain seamless access during updates.

We need to decide whether biometric authentication should replace or complement MFA. Although biometrics via Azure AD enhance security, we must determine if it should replace MFA or act as an additional factor without adding vulnerabilities or complexity.

We need to understand why encryption algorithms perform inconsistently across hybrid environments. Initial tests showed variations in speed and resource usage across Azure, AWS, and private clouds. We are investigating whether these issues stem from differences in infrastructure or APIs and how to optimize performance across all platforms to maintain consistency.

CLOUDSTRUCC INC.

Work Performed during fiscal 2023

Throughout fiscal 2023, our team conducted systematic research and development activities to address core technological uncertainties. Each month brought new challenges and insights as we iteratively developed and tested solutions for data sovereignty and encryption. The work performed represents a methodical approach to solving complex technical challenges while maintaining alignment with our research objectives.

October 2022

- Fred Pearson developed the architecture for Azure Entra Verified ID integration, focusing on decentralized identity flows and encryption models. He designed key modules to handle identity verification across multiple domains.
- Ali Syed configured identity providers within Azure Active Directory (AAD), enabling seamless authentication across different client environments.
- Iyvan Chandran developed Power Automate workflows to ensure smooth access between the digital vault and Power Platform apps, automating authentication processes and session management.
- Kris D'Crus built the first iteration of encrypted storage within Azure Blob Storage, creating a secure repository for encrypted files and data interactions with the vault.

Result: Established core identity flows and tested encrypted storage integration using Azure services.

November 2022

- Fred Pearson designed a roadmap for Azure Key Vault integration, establishing secure key management and automated key rotation processes.
- Ali Syed implemented multi-tenant identity flows with Entra Verified ID to allow users to switch seamlessly between clients and domains.
- Iyvan Chandran configured Power Apps connectors to facilitate encrypted access to stored data, ensuring compatibility between apps and the digital vault.
- Kris D'Crus optimized query performance for encrypted file retrieval from Azure Blob Storage, reducing latency during data access.

Result: Advanced multi-tenant identity integration and enhanced encrypted data retrieval processes.

December 2022

- Fred Pearson developed fault-tolerant encryption models, ensuring continuous encryption operations even during Azure service interruptions.
- Ali Syed conducted stress tests on identity flows to validate the performance of Entra Verified ID under heavy traffic.
- Iyvan Chandran implemented automated session handling workflows using Power Automate to manage key updates and user authentication efficiently.
- Kris D'Crus introduced real-time logging and monitoring within the vault using Azure Monitor, tracking access attempts and encryption events.

Result: Validated identity workflows under load and introduced automated key updates for session handling.

January 2023

- Fred Pearson expanded the encryption architecture for cross-platform compatibility, ensuring smooth integration between Azure and Power Platform.
- Ali Syed implemented MFA (Multi-Factor Authentication) workflows integrated with Entra ID to improve security.
- Iyvan Chandran developed Power BI dashboards to monitor user activity and access trends within the vault, providing real-time insights.
- Kris D'Crus enhanced data synchronization logic to maintain encryption integrity across multiple cloud platforms.

Result: Improved encryption architecture and developed robust monitoring with Power BI and Azure tools.

February 2023

- Fred Pearson initiated multi-cloud encryption tests, ensuring the vault's operations remained consistent across Azure and AWS.
- Ali Syed enhanced Active Directory role-based permissions, aligning them with the vault's encryption protocols.
- Iyvan Chandran created custom Power Automate workflows to streamline user onboarding and access management.
- Kris D'Crus optimized key exchange processes, improving encryption performance under load.

Result: Completed multi-cloud encryption tests and refined access management workflows.

March 2023

- Fred Pearson developed encryption failover mechanisms to maintain operations during Azure service disruptions.
- Ali Syed integrated Azure Entra Verified ID into the vault, enabling decentralized identity verification.
- Iyvan Chandran built session expiration policies to log users out automatically after inactivity in Power Apps.
- Kris D'Crus tested encryption key rotations across environments using Azure Key Vault, ensuring seamless updates.

Result: Implemented session management policies and validated key rotation processes across cloud environments.

April 2023

- Fred Pearson developed domain-specific encryption policies to allow individual clients to manage data encryption independently within the vault.
- Ali Syed configured conditional access policies in Azure AD to enforce secure access control based on user roles.

- Iyvan Chandran implemented automated key refresh workflows in Power Automate for enhanced security.
- Kris D'Crus developed data backup strategies, ensuring encrypted files remain accessible even during system disruptions.

Result: Advanced encryption management and enhanced automation for key updates and backups.

May 2023

- Fred Pearson ran load tests on Azure Blob Storage, evaluating encryption performance under heavy workloads.
- Ali Syed fine-tuned MFA configurations across Power Platform apps for better user experience.
- Iyvan Chandran developed custom identity verification connectors in Power Automate for seamless integration with the vault.
- Kris D'Crus optimized decryption routines, improving response times for encrypted data access in Power Apps.

Result: Improved encrypted storage performance and refined identity verification processes.

June 2023

- Fred Pearson conducted resilience tests on the encryption layer, simulating network failures across multiple Azure regions.
- Ali Syed enhanced key rotation automation using Azure Key Vault APIs, improving security without disrupting active sessions.
- Iyvan Chandran developed Power BI visualizations for real-time monitoring of identity flows and encryption status.
- Kris D'Crus implemented asynchronous encryption operations, reducing processing time during high-traffic conditions.

Result: Strengthened encryption resilience and optimized performance under load.

July 2023

- Fred Pearson developed interoperability models for the vault's encryption to function seamlessly across Azure and other platforms.
- Ali Syed tested advanced MFA flows, including biometric authentication through Azure AD.
- Iyvan Chandran built dynamic Power BI dashboards to track key metrics related to encrypted data access.
- Kris D'Crus performed deep performance tuning, addressing latency issues across identity and encryption workflows.

Result: Achieved greater interoperability and advanced MFA support.

August 2023

- Fred Pearson aligned encryption processes across multi-cloud environments, ensuring consistent operations between Azure and hybrid setups.
- Ali Syed configured Azure AD conditional access rules to enforce real-time security.
- Iyvan Chandran implemented role-based automation workflows in Power Automate for onboarding processes.
- Kris D'Crus ran encryption load simulations, identifying and resolving bottlenecks in the system.

Result: Strengthened multi-cloud encryption alignment and improved onboarding automation.

September 2023

- Fred Pearson worked on future-proofing encryption policies to ensure compatibility with evolving Azure standards.
- Ali Syed implemented preliminary biometric authentication workflows within Power Platform apps.
- Iyvan Chandran added real-time alerts for abnormal activity using Power Automate.
- Kris D'Crus optimized asynchronous encryption routines for better performance under high-traffic conditions.

Result: Advanced encryption policies and improved real-time monitoring capabilities.

Technological Advancements:

Our research efforts have yielded significant breakthroughs in several key areas of data sovereignty and encryption technology. These advancements represent substantial progress in solving fundamental challenges in data control and security, while introducing novel approaches to user-controlled data management across cloud platforms.

1. **Character-Level Encryption Breakthrough:**
    - Developed preliminary prototypes for embedding encryption artifacts within standard character sets
    - Created a novel algorithm that allows encryption properties to persist through standard data validation processes
    - Implemented test cases showing successful encryption survival through multiple data transformation cycles
2. **Enhanced Key Management System:**
    - Developed a hierarchical sub-key system that maintains granular control over data access
    - Implemented prototype browser plugin demonstrating successful integration with common SaaS platforms
    - Created notification system for real-time permission management and access control
3. **Organizational Vault Enhancements:**

- Developed coordinated attestation system using blockchain technology for tamper-proof record keeping
- Implemented keystroke-level tracking with encryption for comprehensive audit trails
- Created unified viewing interface for authorized parties to access immutable records

4 **Novel Data Sovereignty Features:**

- Implemented revocation mechanism that renders stored data unusable while maintaining database integrity
- Developed system for managing subscription-based access with automatic permission expiration
- Created data lifecycle management system with user-controlled retention policies

The **Digital Organization Vault** ensures **data integrity through advanced encryption models, blockchain integration, and decentralized identities**. Each time a contract, identity record, or transaction is modified, it is **re-hashed** and the vault's state is updated without altering previous records. This creates an **immutable chain of events**, tracked and stored using **ION2 blockchain technology**. This system ensures that sensitive documents and contracts are protected, with all changes securely documented and verifiable, providing a high-assurance framework for legal agreements and identity management.

A key **innovation this year was the decoupling of encryption from identity platforms** like Microsoft Entra ID. Our system allows encrypted data to remain accessible only to authorized users, regardless of the SaaS provider's infrastructure. If a user **revokes access**, the encrypted data becomes immediately unusable. This feature gives users **full control over their data footprint** without impacting the underlying SaaS system. We designed this functionality with **multi-tenant scenarios** in mind, allowing multiple clients or divisions to share infrastructure while maintaining **segregated data access** using encrypted keys tied to identity tokens.

Future Research Directions:

Building on our current achievements, we have identified several critical areas requiring further investigation and development. These research directions reflect both the challenges uncovered during our current work and the opportunities for additional innovation in data sovereignty and security.

1 **Cross-Platform Integration:**

- Need to optimize performance of character-level encryption across different platforms
- Research required to minimize latency in blockchain-based attestation system
- Investigation needed into scaling capabilities across multiple cloud providers

2 **Security Enhancement:**

- Further research needed on sub-key management in distributed environments
- Investigation required into potential attack vectors on character-level encryption
- Need to optimize performance of real-time permission management system

Names and qualifications of people worked on this project during this fiscal period

The following key team members brought extensive expertise in cloud architecture, security, and software development to this research initiative. Their combined experience was crucial in addressing the complex technical challenges encountered during the project.

Names	Qualifications/experience and position title
Iyvan Chandran	Co-lead Architect
Ali Syed	Co-lead Architect
Frederick Pearson	Full stack developer, a Power Platform specialist

Documentation that is available for CRA to review:

Throughout this research period, we maintained comprehensive documentation of our experimental work, development processes, and results. The following list represents the documentation available for review, demonstrating the systematic nature of our research and development activities.

- Records or resources allocated to the project (SDLC/ALM tool report)
- Design, system architecture and source code