WHEN PRIVACY MATTERS, BUT MACHINE LEARNING IS NEEDED

AI, Storage, and Compute with Arm, Protopia, and Computational Storage

PRIVACY MATTERS: The ability to interpret and manage data streams from video sources is key for the future, however exposing personal information is not. This creates a new need that is solved here.

MACHINE LEARNING: As the term states, it is performed by machines. Machines look for patters, objects, and other data that does not necessarily have to exists in a raw data format. We will explain this unique transformation capability.

THREE PILLARS OF SUPPORT: With the partnership created by the underlying Arm architecture, NGD Systems and Protopia have created a new way to use AI without exposing critical data.

Reach NGD Systems: Info@NGDSystems.com
www.NGDSystems.com
Reach Protopia: Info@Protopia.ai
www.Protopia.ai
Arm AI Partner Program
https://www.arm.com/why-arm/partner-ecosystem/ai-ecosystem-catalog

INTRODUCTION

The Challenge of Video Processing: There is a lot of data being generated by video capture today. Whether that is by governments, businesses, or individuals. With the advent of the IoT explosion, the amount of raw video being consumed has grown into the Exabytes of images, faces, objects, and in some cases very personal and private data. There is a need in the market to find a path forward to ensure data analytics occur, but personal data, personal images, and other private information is not exposed in the process.

This is where Computational Storage Drives (CSD) from NGD Systems, partnered with the Responsible AI software from Protopia come together to create the perfect holistic solution. All with the support and ecosystem that comes from Arm architectures.

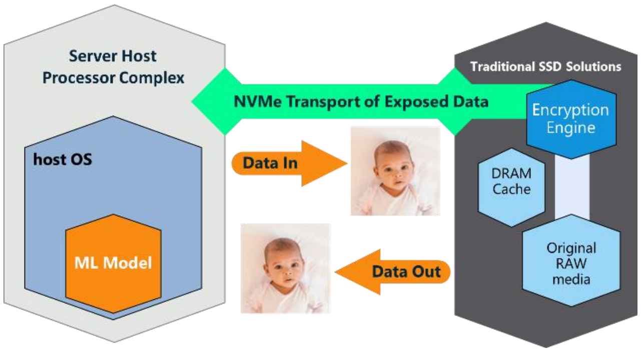
This whitepaper describes a solution using NGD Systems' new disruptive NVMe Computational Storage Drive (CSD) technology together with Protopia's Responsible AI Software to create a method of video/data capture, analysis, and results with private data never leaving the initial storage device. This one-of-a-kind platform is easy to deploy, requires no customization and can be deployed at scale, even to the Far Edge where IoT and Edge Computing meet.

TECHNICAL OVERVIEW

Computational Storage Drives offer a novel capability to perform computation within the storage before the data leaves the drive. This capability can lead to significant performance improvement using the Linux-based integrated ARM CPU cores within the NGD Systems storage device. Going beyond just performance, NGD Systems has partnered with Protopia AI to bring a new dimension to the value these on-board ARM cores can provide. This new dimension of data protection enables privacy-preserving machine learning and AI services that safely span the edge-to-cloud continuum ensuring the original data is never at risk of exposure after capture.

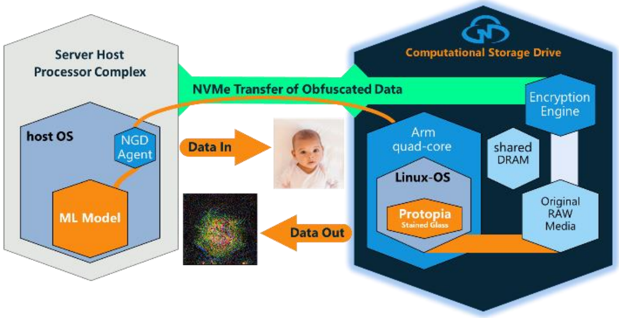
NGD Systems is integrating revolutionary technology from Protopia AI that transforms data to a garbled representation using a stochastic transformation before it is shared with an ML service. This partnership enables NGD CSDs to protect sensitive information within each data record before the data is exposed to the ML process. Protopia AI's software-only transformation, dubbed "Stained Glass," is a mathematical solution that garbles each individual data record using an innovative Protopia algorithm. These transformations uniquely enable *an unchanged* deep learning model to consume the data and still accurately make predictions without exposing the original raw information. The Stained Glass solution requires a lightweight use of computation that makes it a perfect fit for computational storage.

As the following diagram illustrates, data is commonly encrypted at rest and is protected in the storage devices and it ensures ownership retained, through traditional encryption methodology. When data needs to leave the storage for computation beyond what is possible at the CSD, the data is exposed when transferred out of storage to the inference service at the Edge or to the cloud.



This exposure of the data to the ML service is like allowing ownership of the raw data to the service operating on it and has historically been an unfortunate evil. This is now overcome with NGD Systems' and Protopia AI's partnership to protect the raw data from being exposed.

With the integration of Protopia's Stained Glass solution with NGD Systems Computational Storage Drives, there is a pragmatic way to minimize the exposure at the raw data level.



Using NGD Systems CSD's embedded ARM cores to run Protopia AI's lightweight transformation, AI/ML models can safely span the edge-to-cloud continuum without any host level software modifications. The most computationally intensive part of a model can now be executed on transformed/obfuscated data in the drive, at the edge, or in the cloud, while the raw data remains safely stored in the NGD Systems CSDs that now serve as a root-of-trust. All of this is made possible by using standard NVMe host platforms from IoT Gateways, Edge Servers, or Rack-level solutions.

This solution using technology from Arm, NGD Systems and Protopia showcases one of many solutions for Computational Storage that were previously never possible. In addition to this new capability, the security of data in-flight is now more protected than ever as the amount of exposed data is growing over 2x each year.

You can see, from the diagram below, the communication path of the Protopia solution with the data is over a traditional NVMe command protocol path and the data in and out of the drive is still protected by traditional encryption models in use today, like TCG-OPAL.

This is a great example of where the AI Partner Ecosystem from ARM has created a collaboration platform that enables the broad market to preserve raw data while still allowing for ML processing to occur.