Efficient and Secure Cloud Computing for UXO Classification and Project Management

Authors: Dean Keiswetter (Acorn SI), Tom Furuya (Acorn SI), Nick Valleau (Geosoft Inc.), Henry Wang (Geosoft Inc.)
ESTCP Project: MR-2017112

Objective

Develop a cloud-based data management and analysis technology and workflow for classifying buried objects in high risk UXO sites, based on the specific approach for QAQC-MHFF project goal.

Benefits

- Application Security
- Database and file system management
- Data Quality Control
- Identity management
- Platform and infrastructure security
- Security architecture and identity management components
- Technical- based architectural systems

Core Technology

UX-Analyze on the PC Desktop
- UX-Analyze is the existing standard software for processing and examining data to classify and distinguish objects embedded on the ground. The tool is designed to be examined in two stages: (1) detecting buried objects using information from electromagnetic sensors, and (2) classifying, documenting, and delivering the prioritized dig list.

Cloud Computing
- Cloud-based computing, which is a way to access computer-based data and software, allows for the kinds of applications everyone uses on the Internet. This infrastructure provides the structure and back-end access to all user archetypes, allowing for secure, efficient, and automatic access to data.

UX-Analyze Cloud
- UX-Analyze is transparent, modular, and available. It includes tools for UC4 data target generation from a library of UXO, specialized input analysis, and viewing and assessing of feature-related attribute data. It can be used in a dynamic and static survey data with both hand-held and geophysical devices.

Workflow Elements

- UX-Analyze Cloud is component of many, many steps. But at a high level, there are three fundamental elements. These relate to (1) examining data quality for data management, (2) computing, collating data analysis framework (the library of UXO), and (3) classifying, documenting, and delivering the prioritized dig list.

Roles


Dashboards
- The Cloud and dashboards shown below, perform a final classification on the UXO library and status updates, or deliver geo-Digest. The Cloud is a central information system to manage and control all geophysical sensor data. It can be used for dynamic and static survey data in both underwater and terrestrial environments.

Validates Library
- The validators library consists of versions 1.0, 2.0, and 3.0 sources. These classifiers classify the results based on the classification of the UXO catalog and archives. For example, in the current UXO version, the classifiers are defined in the UXO version database.

Security

- User archetypes and roles defined (see below)
- User access management defined
- Application security
- Platform and infrastructure security
- Microsoft Azure security features and policy for storage

Current project work

- UX-Analyze Cloud interface has been designed and built from scratch in 2018. The software is currently in its 2nd year of activity and is a 3-year project.
- UX-Analyze Cloud is a modular and flexible platform for UXO classification and project management.
- UX-Analyze Cloud utilizes Azure Cloud services, including Geo IDs, Interactive displays, and Advanced Geophysical Classification (AGC) and is transparent, modular, and available. It includes tools for UC4 data target generation from a library of UXO, specialized input analysis, and viewing and assessing of feature-related attribute data.
- The Cloud infrastructure provides the structure and back-end access to all user archetypes, allowing for secure, efficient, and automatic access to data.
- Each role has their own fully-functional workspace in which to work.
- UX-Analyze Cloud is a cloud-based computing platform.

Why do we need a cloud-based solution?

- Cloud technology allows data to be accessed regardless of where it is stored. Data can be accessed from any device with Internet access, even if the device is not a computer.
- Data security
- Identity management
- Platform and infrastructure security
- Each user will have a Geosoft "Geo ID"
- Geo ID is treated individually.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.
- Geo ID is used to control access to the Cloud.
- Geo ID is used to control access to the Cloud.
- Geo ID is a unique identifier assigned to each individual user.