CIRI | CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE

A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

PASS+ Toward a Safe, Secure and Resilient Cyber Environment

Author: Ederson Mazariego
Faculty Advisor: Dr. Zhixiong Chen from Mercy, Dr. Deming Chen from UIUC

MERCY COLLEGE NEW YORK

Homeland Security Challenge

Trustworthiness is important for the Cyber Infrastructure to build a safe, secure, resilient cyber environment. Recent attacks such as SolarWinds, Kaseya, and Codecov have shown the fragility of software supply chain, and the profitability it has for the attackers. The challenge we propose is a multi-party multi-level cryptographic token system known as Portfolio Artifact Service System (PASS). PASS allows a subject known as a holder to tokenize their portfolio artifacts such as diplomas, badges, knowledge, skills, and to store them in a decentralized verifiable data registry. This ensures trust between holders and their use applications. As an example, an applicant can present his/her PAs to a potential employer, and the employer could trust the presented claims without needing to manually check.

PASS+ Objectives

The objective of the PASS+ project is to build a trust environment in a 3D (Web3) Internet

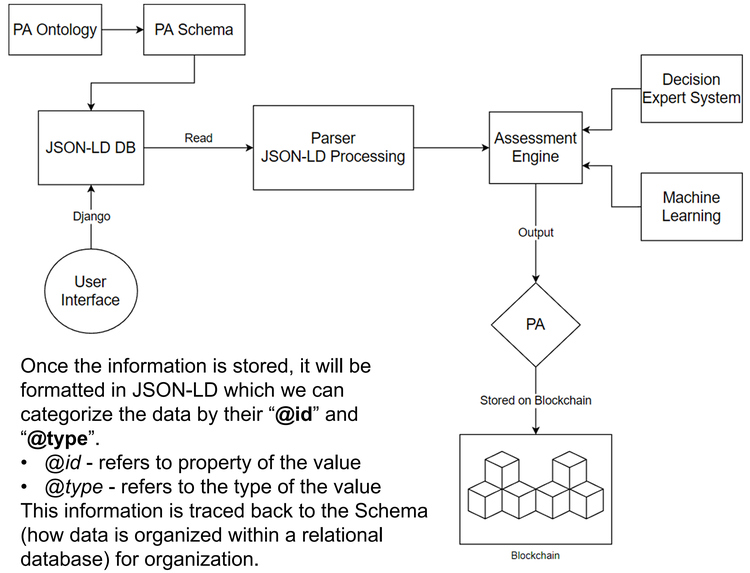
1. Use ontology to structure portfolio artifacts (PAs) systematically
2. Develop JSON-LD schema to realize the PA structures
3. Design a decision expert system and develop machine learning models to build an engine to assess skill competency
4. Create portfolio artifacts (PAs) that are digitally signed, approved, or assessed by the assessment engine
5. Store these PAs in a decentralized blocks using Blockchain technology
6. Design and develop a platform that connects holders, certifiers or issuers, and end applications
7. Design and develop smart contracts that could create and retrieve PAs
8. Explore and design a consensus protocol, proof of me (PoM), to build secure and high performance blockchain

Approach

My focus - Use ontology and JSON-LD to organize data structurally and extensibility, to communicate among machines, and to model and analyze the trust environment formally. Using Django SQLite to create an API system that could Add, Delete, Update or Search user information within a database.

Methodology

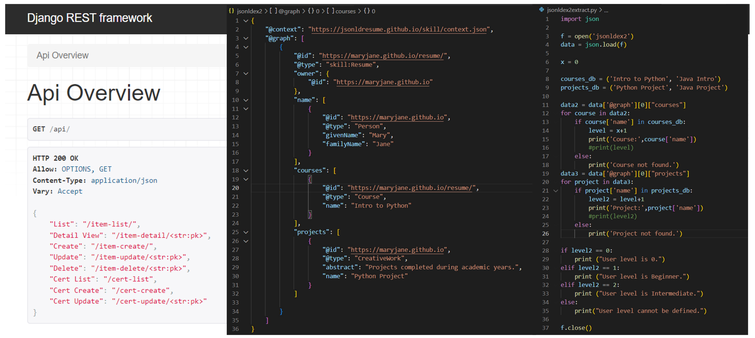
Ontology Workflow



Once the information is stored, it will be formatted in JSON-LD which we can categorize the data by their "**@id**" and "**@type**".

- *@id* - refers to property of the value
- *@type* - refers to the type of the value

This information is traced back to the Schema (how data is organized within a relational database) for organization.



Results

After establishing the API in Django SQLite, users can interact with an interface to enter their data. This data would be saved onto the SQLite database in the format of JSON-LD. The database is then parsed and ran through an Assessment Engine. Using machine learning and having an established decision expert system a user's skill competency is assessed. Once completed a signed PA is created which can be requested and later stored on the blockchain.

References

- "Documentation." *JSON*, https://json-ld.org/learn.html.
- "Documentation." *Django*, https://docs.djangoproject.com/en/4.0/.
- "Documentation." *Schema*, https://schema.org/docs/documents.html.

Conclusion

With the work our team has accomplished there is still much more to do in order to achieve our goal. As of now we have a foundation where we can continue to build and expand upon. We have a functioning API where data can be stored and modified as well as a means of formatting the information. Currently we have a basic means of assessing a user's competency which can be expanded into a more sophisticated decision expert system.

Acknowledgements

This research was performed under an appointment to the U.S. Department of Homeland Security (DHS) Science & Technology (S&T) Directorate Office of University Programs Summer Research Team Program for Minority Serving Institutions, administered by the Oak Ridge Institute for Science and Education (ORISE) through an interagency agreement between the U.S. Department of Energy (DOE) and DHS. ORISE is managed by ORAU under DOE contract number DE-SC0014664. All opinions expressed in this paper are the author's and do not necessarily reflect the policies and views of DHS, DOE or ORAU/ORISE.

ILLINOIS