Design Document – Initial draft (V0.0)

Design of Overall Framework and Modular Experiential Learning Modules (ELMs)

Flexible Framework

The framework is designed to be flexible to be adaptable. Currently, it consists of three loosely coupled levels plus distilled flexible micromodules (FMMs). FMMs will be completed in Year 2. The three levels are foundational, intermediate, and advanced. These are suitable to the following groups of learners.

1. Foundational: Undergraduates in CS 1 and CS 2 classes, and senior high school with some computing / programming background.
2. Intermediate: Undergraduates taking 3- and 4- level classes.
3. Advanced: Undergraduate and graduates taking 5- and 6- level classes, and practitioners in industry or government organizations that already have a CS degree or equivalent.

Note that these are not strict divisions, rather these are indicative of the level of standard preparedness for the modules. For example, it is possible for advanced students in their peer group to benefit from modules intended at a higher level. In addition, modules are designed to be loosely coupled within the framework. This means it is not necessary to follow any specific sequence.

About 14 new modules will be developed in the implementation project. The flexible framework allows for future expansion. For example, it will be possible to integrate practitioner-oriented modules and distilled micromodules within the framework. Fig. 1 illustrates the framework pictorially.

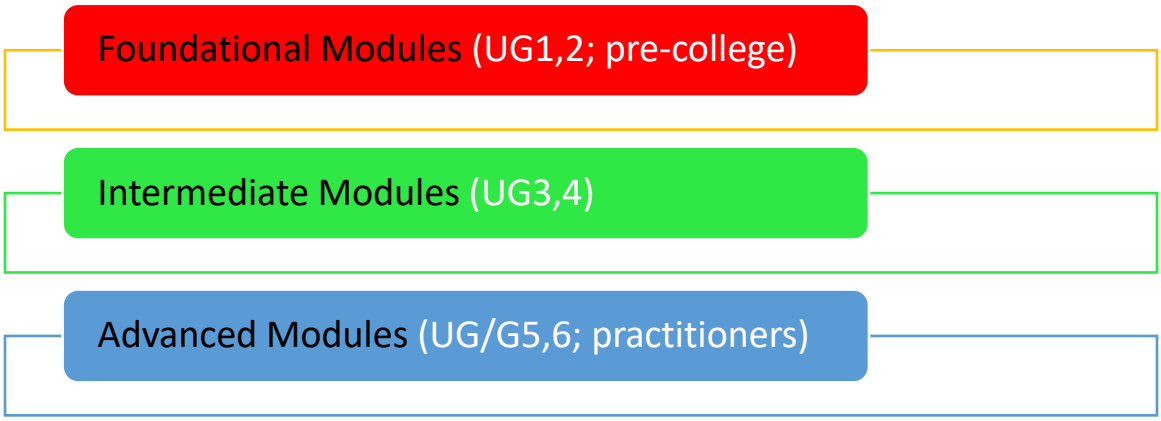

Fig. 1. Flexible framework.

Module Design

The proposed experiential learning modules (ELMs) span all levels, from basic literacy to advanced treatment of topics. Evidently, they focus on the emerging needs of fundamental research communities and resolving bottlenecks in the convergent area of SSR AI that leverages HPC CI. There is an emphasis on keeping the modules agnostic in terms of programming languages. Learners can choose their preferred language, e.g. Python, R, or C, but will in any case be encouraged to use open-source libraries and resources. Examples and data will be drawn from real-world sources, e.g. social media and news outlets, so learners can relate their study to their daily activities and include topics that they care about. The modules will be designed such that they can be used as standalone learning modules or integrated into existing courses.

For consistency, each module should be designed based on one of the following recommended formats:

Format A: Learning through positive and/or negative examples

1. Introduction to background information by course instructor (if integrated) or domain expert.
2. Guided exploration leading to awareness and good comprehension of a problem or issue; how it fits in the bigger picture.
3. Implement an instance of the problem or issue to gain insight; it becomes "real" no matter how vague or incredible it seemed initially.
4. Using in-course knowledge and/or other resources, develop a countermeasure strategy / design based on set goal and problem (solving in principle).
5. Implement and evaluate the countermeasure (solving in practice).
6. Reflect on the outcome: could anything have been done differently / better? This is done in class (if integrated) or via a virtual study group.

Format B is a simplified version of Format A, which focuses on positive example(s).

1. Introduction. Some background information. Point users to reputable available resources as appropriate.
2. Guided exploration using one or multiple positive examples.
3. Get learners to go through design, implementation, and evaluation phases.

Deviation from the recommended formats is possible. Advanced modules will tend to cover all steps; other modules will give more emphasis on some aspects than others. For example, more emphasis will be put on exploration leading to awareness than solving a problem in the foundational modules. The reason is that early-stage learners are not expected to possess a significant amount of knowledge and skills to perform substantive problem-solving tasks. They will instead focus on experimenting with strategies toward problem solving based on the theory they have learned (solving in principle vs. solving in practice). The advanced modules, especially, will be developed with CI practitioners and CI contributors in mind.

Although the modules will be designed to run in a sequence, starting with 1- level courses, they will not be tightly coupled. This means the flexible framework will allow learners to select modules (or sequence of modules) that they think are most relevant or interesting, in the order they desire. Further, because in-class modules are fully integrated into existing courses with a balance between theory and practice and between learning and applying, there will be no net increase in time to degree completion for students. The latter is an important practical consideration in the design of modules, if they are to be used in existing courses.

Specifically, when modules are used in "integrated mode", the scope, nature, and level of difficulty of each module will be harmonized with the "host" courses. Otherwise, when the modules are used in "standalone mode", they can be completed as separate self-directed learning units.

Experiential Learning

There is an emphasis on "learn by doing". Below is a figure that summarizes possible experiential learning activities (source: NSF 23-507 Experiential Learning for Emerging and Novel Technologies (ExLENT)).

Most intended users of the new learning materials will be adults (college students, working professionals), but out outreach activities will include high school students. The recommended strategy is to focus on the needs of the primary group of adult learners, and then customize a small selection of materials for HS students. This is the approach we took in the pilot, and it worked well.

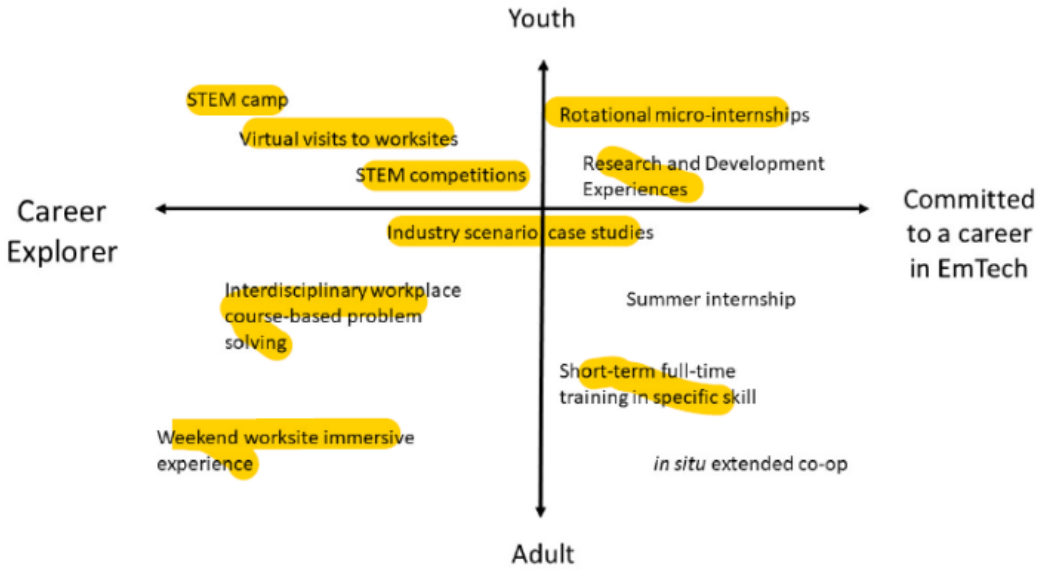

Figure 1. Examples of experiential learning activities

Step 1 (12 months) Enhancement of original ELMs and development of new ones.

Summary of original modules

#	level	Module Name	Lead
1	F	Math Toolkit for SSRAI running on HPC CI	SB
2	F	Algorithmic Exploration and Exploitation of an Intelligent System's weakness	SB
3	F	Modular and Structured Software Development for Robust Intelligent Systems that run on HPC CI	
4	I	Data Structures for SSRAI running on HPC CI.	
5	I	Deep learning with HPC	AF
6	A	SSRAI Software Development for HPC CI deployment	
7	A	Vulnerabilities of Machine Learning.	AF
8	A	Beyond current generation AI and Toward Artificial General Intelligence	AF
9	A	Adversarial Machine Learning and Robust Trust Scoring Models	SB
10	A	Societal Impact of AI	AF
11	A	Pitfalls of applying AI to Information Retrieval tasks	AF
12	A	Real-Time SSRAI with HPC CI	

The following is a list of the *new* modules that are envisaged. The list is provisional at the time of developing this Design Doc. Changes are possible especially after receiving feedback from the panel of experts.

Summary of new modules

#	Level	Name	Lead
NM1	F	What is safe, secure, and reliable (SSR) AI?	

NM2	F	Applications of AI in daily life	
NM3	F	ML paradigms	
NM4	I	SmartX enabled by AI	
NM5	I	AI techniques for scientists and engineers	
NM6	I	AI-induced biases and mitigation with Explainable AI	
NM7	I	Optimization for ML and adversarial ML	SB
NM8	I	Partnering with AI	
NM9	A	AI for accelerated scientific discovery	
NM10	A	Creative AI and deepfakes	
NM11	A	Evolutionary ML	AF
NM12	A	AI for extremely complex problems	
NM13	A	Security in federated learning	SB
NM14	A	AI frontiers	AF

Description of each NM:

NM1 What is safe, secure, and reliable (SSR) AI? Foundational

Define AI, ML, DL, etc. in the context of SSR AI. SSR are pillars that support trust and fairness in AI. What types of problems are amenable to an AI solution, how to formulate a problem for possible AI solution. Branches/capabilities of AI beyond learning, e.g., reasoning, planning, knowledge representation. Related synergistic fields in broader computational intelligence, e.g., memetic computing, genetic programming. Learning outcomes: understand SSR AI, identify problems amenable to an AI solution, able to formulate such problems for a possible AI solution to perform CI-enabled big data analysis. Potential MetX: from several sample problems drawn from different S&E domains, determine which one(s) can be formulated for an AI solution; sketch the steps involved toward solving the problem(s) in principle.

NM2 Applications of AI in daily life (on a personal level) Foundational

Explore how AI is used in a wide range of consumer products and services: social media, reviews, recommendations, games, home appliances, Siri and similar digital assistants, intelligent search engines, chatbots like ChatGPT, etc. Learning outcomes: technical, behavioral, and societal appreciation of how AI is integrated into everyday life for learning, working, entertainment, socializing, shopping, etc.; importance of CI-enabled big data analysis needed to support these applications. Potential MetX: immerse into the “lives” of digital assistants and chatbots as they interact with human users. What could go wrong?

NM3 ML paradigms Foundational

Sample a range of learning paradigms, e.g., supervised, unsupervised, semi-supervised, lifelong, reinforcement, adversarial. DL for MASDA. Cloud ML/DL. Quantum ML. Learning capacity, model selection, and hyperparameter tuning. Understand the pros and cons of each method and when to use what. Learning outcomes: make informed decisions on what ML method(s) to apply to a given problem, practical experience in finetuning ML model parameters and hyperparameters, and ability to apply suitable CI-enabled ML algorithms to big data. Potential MetX: from several sample problems drawn from different S&E domains, select a problem and develop one or more ML algorithms to solve the problem in practice.

NM4 SmartX enabled by AI (on a societal level) Intermediate

Here X = healthcare [23], home [25], transportation, manufacturing, education e.g., [108-110], agriculture, power grid, etc. Possible focus on AI for commerce and industry case studies, e.g., AI-powered time series analysis for commodity trading. Learning outcomes: knowledge of actual use cases of CI-enabled AI for big data analysis for smartX in multiple settings. Potential MetX: immerse into the "life" of a smart transportation hub AI agent as it interacts with human users, vehicles, etc.

NM5 AI techniques for scientists and engineers Intermediate

AI for computer vision, optimization techniques, conceptual analysis, NLP tools based on our recent work that encompasses large language models, transfer learning, and GPT-series transformers, reusable NLP toolkit, etc. developed based on our technical advances made in the pilot, e.g., [20-23]. Learning outcomes: ability to rapidly apply AI tools to a range of S&E problems; quantify the effectiveness of the AI solution. Potential MetX: from several sample problems drawn from different S&E domains, select a problem and use AI tool(s) to solve the problem in practice and quantify the solution's effectiveness.

NM6 AI-induced biases and mitigation with Explainable AI Intermediate

Our findings in [19] will lay the groundwork for this investigative study to identify sources and manifestations of AI biases. Learning outcomes: practical skills for data collection and handling; ability to develop effective mitigating strategies by ensuring the machine generated results are highly explainable. Potential MetX: experience varying amounts of AI biases with no or different mitigating strategies; experience how an AI agent can explain its output after processing a sea of big data.

NM7 Optimization for ML and adversarial ML Intermediate

Deep understanding of data poisoning and evasion attacks on ML approaches can be fully understood when students thoroughly understand various convex and non-convex and non-linear optimization methods.

Learning outcomes: Students will get visual intuition into the multi-dimensional nature of the parameter constraints and how constrained and unconstrained problems, affect changes in geometry of the loss function space, inner and outer solutions of bi-level optimization problems using smart metering infrastructure as a proof of concept. Potential MetX: Visualize the moving parts of the complex geometry of multiple linear and non-linear constraints, bi-level optimization problems.

NM8 Partnering with AI Intermediate

Building and maintaining trust in human-AI partnerships; future of work with AI; companions (humanoid robots and robotic pets). Based on our pilot study in safe, secure, and reliable (SSR) AI, we promote trust using SSR as the key pillars and lay the groundwork for effective and harmonious human-AI partnerships. Learning outcomes: practical skills for establishing and maintaining trust in human-AI partnered MASDA. Potential MetX: varying effectiveness in human-AI partnerships vs. degrees of SSRAI.

NM9 AI for accelerated scientific discovery Advanced

Applications of AI and ML to proteomics, discovery of new materials, new pharmaceutical drugs, new medical treatments, space exploration, deep sea exploration, etc. Learning outcomes: ability to use powerful AI/ML to expedite scientific discovery in a discipline of interest. Potential MetX: accelerate discovery of new knowledge in a domain-specific or cross-discipline use of CI-enabled AI for MASDA.

NM10 Creative AI and deepfakes Advanced

Get under the hood to see and practice how machines can paint like Picasso, write like Shakespeare, or compose music nearly half as good as Bach's. Possible focus: chatbots and text-to-image tools. With democratization of machine-generated content comes elevated risks of harmful malcontent, e.g., deepfakes and misinformation. What to do about them? Learning outcomes: understand how creative AI tools work; ability to create new artifacts with such tools; abilities to identify fake content and develop effective mitigating strategies. Potential MetX: Friendly battle between fake content creation and mitigation.

NM11 Evolutionary ML (EML) Advanced

Explore ways to expand the capability of ML algorithms through synergistic applications of established and novel evolutionary computational intelligence methods, such as genetic programming (GP) and memetic computing. Topics include: 2-way nexus (EC for AI/ML and EML in EC), GP-based evolutionary DL for feature extraction and classification, computational cost, scalability for MASDA, generalization for a range of problems, and interpretability of the results. Learning outcomes: ability to solve problems using EML; understand the 2-way nexus. Potential MetX: experience the synergistic contributions of evolutionary methods towards making ML more effective than before.

NM12 AI for extremely complex problems Advanced

AI that can potentially save the world and humanity – solving very complex problems like climate change, food and water shortages, public health challenges, the next pandemic, conflict (war) avoidance, etc. Learning outcomes: ability to leverage MASDA to develop strategies for solving highly complex problems in principle. Potential MetX: experience the effectiveness of a possible solution.

NM13 Security in federated learning Advanced

In smart connected communities (e.g., smart metering microgrids) and wireless networks, federated machine learning is important to train ML models while keeping privacy of the data by keeping data local to client. Learning outcomes: Students will learn fault tolerate secure aggregation protocols where the aggregation happens over encrypted weight updates via Secret Sharing and which enable students to understanding vulnerabilities in federated learning algorithms. Potential MetX: Secure federated learning creates a conceptual hurdle of understanding the complex web of various exchanges between clients, servers, and the trust third part key providers for encrypted weight updates.

NM14 AI frontiers Advanced

S&E researchers help shape future AI. Venture into the realms of the extraordinary. An investigative look at the frontiers of AI/ML research, see what is on the horizon, and extrapolate further into the future. Topics include quantum ML, efficient algorithms using less energy and fewer samples, AI in metaverse, neurolink/singularity and other forms of augmented intelligence, and the long road toward AGI, will super AI succeed us? Learning outcomes: knowledge of where cutting-edge AI/ML research is going; ability to contribute to meaningful debate. Potential MetX: experience seemingly boundless future possibilities.

Step 2 (12 months) Development of flexible micro modules FMMs and MetX immersive AR experiences

Details later.