2026 ASEE ANNUAL CONFERENCE June 21–24, 2026 | Charlotte Convention Center, NC
Host Sponsor UNC Charlotte
Paper ID #51793

WIP: Privacy-Aware Biometric Interface for Blockchain Micro-Credentialing in Engineering Education

Yahia Tawfik, Virginia Polytechnic Institute and State University

Yahia Tawfik is a Ph.D. student in the Bradley Department of Electrical and Computer Engineering at Virginia Polytechnic Institute and State University, where he received his B.S. in Computer Engineering. He is exploring research in blockchain micro-credentialing, decentralized identifiers, and AI for security applications. His work on this paper reflects early-stage contributions to privacy-preserving assessment and competency-based credentialing infrastructure for engineering education.

Prof. Christiana Chamon Garcia Ph.D., Virginia Polytechnic Institute and State University

Christiana Chamon Garcia received the B.S. degree in electrical engineering from the University of Houston, Houston, TX, USA, in 2017 and the M.S. and Ph.D. degrees in electrical engineering from Texas A&M University, College Station, TX, USA, in 2020 and 2022, respectively. She is currently an Assistant Professor for the Bradley Department of Electrical and Computer Engineering at Virginia Tech, Blacksburg, VA, USA, where she directs the Stochastic Noise and Cyber Innovation Lab (SNACIL). In 2016 she was a Hardware Design Intern and in 2017 a Product Management Intern with Hewlett Packard Enterprise. In 2022, she was an Applications Engineer at Vidatronic Inc, and from 2022 to 2024, she was an Instructional Assistant Professor for the Department of Computer Science and Engineering at Texas A&M University, College Station, TX, USA. Her research interests include stochastic processes, physical unclonable functions, decentralized networks, cyber-physical systems, security in artificial intelligence, engineering education, human-computer interaction, accessibility in engineering and kinesiology, and exercise science. Dr. Garcia is a 2024 CCI Faculty Fellow, 2023 Future Faculty Diversity Program (FFDP) Fellow, 2023 WISCPROF: Future Faculty in Engineering Workshop Fellow, 2020-2021 Ebensberger Fellow, and a member of ACM, IEEE, and Eta Kappa Nu (HKN).

Leyla Nazhandali, Virginia Polytechnic Institute and State University
Dr. Vinod K. Lohani, Virginia Polytechnic Institute and State University

Dr. Vinod K. Lohani is a Professor of Engineering Education and also serves as the Director of education and global initiatives at an interdisciplinary research institute called the Institute for Critical Technology and Applied Science (ICTAS) at Virginia

Dr. Dayoung Kim, Virginia Polytechnic Institute and State University

Dr. Dayoung Kim is an Assistant Professor in the Department of Engineering Education (College of Engineering) at Virginia Tech and a Director of the LABoratory for Innovative and REsponsible ENgineering workforce (LAB-IREEN). She also serves as an Executive Committee Member and Affiliate Faculty of the Center for Future Work Places and Practices (CFWPP). Her Engineering Practice research examines the practice of engineers across a range of employment settings, including business organizations – from startups to large, established firms – and government agencies. Building on insights from this work, her Engineering Workforce Development research focuses on developing the future engineering workforce capable of contributing innovatively and responsibly within their own contexts. Across her research, teaching, and service, she aims to bridge academia, industry, and government by translating insights from engineering practice into scalable systems for education, workforce development, and science and technology policy. She received her Ph.D. in Engineering Education from Purdue University and her B.S. and M.S. in Chemical Engineering from Yonsei University and Purdue University, respectively. She was the 2022 Christine Mirzayan Science & Technology Policy Graduate Fellow at the National Academies of Sciences, Engineering, and Medicine (NASEM).

WIP: An Instructor-Mediated Workflow for Privacy-Aware Micro-Credentialing in Engineering Education

Abstract

As engineering programs seek more granular ways to document and communicate student competencies, micro-credentials have emerged as a promising complement to traditional grades and transcripts. However, existing credentialing implementations rarely integrate into active assessment workflows, and remote proctoring solutions that support assessment integrity have raised serious equity and privacy concerns — particularly for students from underrepresented groups. This paper introduces a privacy-aware micro-credentialing platform designed for deployment in Electrical and Computer Engineering courses. Rather than treating credentialing as a post-hoc administrative act, credential issuance is embedded directly into the assessment process through three principled design decisions: instructor judgment is preserved through a human-in-the-loop approval model, no biometric templates are collected or stored at any stage, and issued credentials are tamper-evident and independently verifiable without contacting the issuing institution. An IRB-exempt internal pilot with six students (n = 6) established feasibility, confirmed the core workflow functions as intended, and surfaced early signals that warrant closer investigation in larger deployments. A phased deployment in a 280-student embedded systems course is planned to examine how students perceive the fairness of instructor-mediated credentialing, how review burden compares to automated proctoring, and whether competency-based credentials serve as meaningful skill signals for students transitioning to internships and employment.

Key words

micro-credentialing, privacy-preserving assessment, instructor-mediated review, engineering education, competency verification

Introduction

Engineering students graduate with transcripts that tell employers very little. A grade reflects completion and rarely tells an employer, a graduate program, or even the student themselves which specific competencies were actually demonstrated along the way. A student who completes an embedded systems course may know how to debug a memory allocation error, document a hardware interface, or implement a secure communication protocol, but none of that shows up in a letter grade. Micro-credentials offer a more granular alternative: short, competency-focused certifications tied to discrete, verifiable skills rather than broad course completion. As engineering programs seek richer ways to document and communicate student learning, this gap between what students learn and what they can verifiably show has become the central problem this work addresses.

This gap has become more urgent in recent years for many reasons but we focus on two of them. First, the rapid growth of generative AI tools has complicated how instructors verify that submitted work reflects individual student understanding, making assessment integrity harder to maintain in digital learning environments [1]. Second, the expansion of remote and hybrid learning has accelerated the adoption of automated proctoring platforms, many of which rely on behavioral monitoring and biometric data collection that students often perceive as invasive, inequitable, and disproportionately burdensome for underrepresented groups [2]. Engineering programs therefore face a dual challenge: strengthening the credibility of individual assessment while earning and maintaining student trust in how that assessment is conducted.

This paper builds directly on our prior FIE structured abstract and prototype design [3], and introduces a structured workflow integrating coding assessment, privacy-conscious proctoring, and blockchain-based credential issuance. The workflow is built around three core principles: instructor judgment is preserved through a human-in-the-loop approval process; student privacy is protected by design with no biometric templates collected or stored; and credentials are tamper-evident and independently verifiable without contacting the issuing institution.

This system's functionality has been validated through an IRB-exempt internal prototype deployment (n = 6) confirming technical functionality as a foundation for the planned large-scale deployment in a 280-student embedded systems course. Early dissemination of this workflow is not to report evaluation outcomes but to introduce the workflow design, surface the tradeoffs it embodies, and open a set of research questions that the engineering education community is well-positioned to engage with.

The workflow raises a set of research questions about assessment fairness, scalability, and competency signaling that the engineering education community is well-positioned to investigate. These questions are introduced in the Discussion and Future Work section alongside the deployment plan designed to begin addressing them.

This paper makes three contributions:

1. A deployable workflow architecture integrating assessment, privacy-aware proctoring, and instructor-mediated credential issuance into a single process — providing engineering programs a structured path to competency-level documentation beyond traditional grades.
2. A design framework explicitly avoiding persistent biometric template storage while supporting assessment integrity verification — demonstrating that credible oversight does not require surveillance-style data collection.
3. A human-in-the-loop credential issuance model that preserves faculty authority over deciding whether a student has actually demonstrated the skill a credential represents — the step that most existing credentialing platforms either automate or treat as a separate administrative act.

The workflow uses blockchain-based credentials for tamper-evident verification, but the contributions above are not dependent on any particular credentialing technology. The value of this work lies in the integrated process, not the anchoring mechanism.

Background and Literature

Micro-credentials have gained traction in higher education as a way to document discrete, competency-level achievements that traditional transcripts cannot capture. However, most implementations focus narrowly on issuance and verification, with limited integration into active assessment workflows or alignment with course-level learning outcomes [4, 5]. Existing platforms typically treat credentials as separate from the assessment process itself, with little attention to how integrity is maintained or how student privacy is protected during that process. Recent implementations have further demonstrated the feasibility of blockchain-based credential generation across university networks, while also surfacing unresolved challenges around scalability, data privacy, and institutional adoption [6]. This work addresses those challenges directly by embedding credentials into the active assessment process for Electrical and Computer Engineering courses, with a privacy-first design and phased deployment approach.

Traditional credentialing has a trust problem. Transcripts and certificates can be falsified, and verification requires contacting the issuing institution, creating a single point of failure. Blockchain-based credentials eliminate this dependency: they are tamper-evident after issuance and self-verifiable [7], meaning any employer or institution can confirm authenticity independently without relying on institutional trust [8].

Several credentialing platforms and institutional processes already support faculty-controlled credential issuance, and some universities require instructors to document how student achievement is measured before credentials are released. However, these approaches typically treat assessment and credentialing as separate steps — the instructor evaluates student work in one process and a credential is issued through another. The workflow presented in this paper connects these steps directly: the same instructor review that determines whether a student has demonstrated competence is the step that triggers or blocks credential issuance, with no administrative layer in between.

Remote proctoring has grown rapidly in online and hybrid courses, but its use has raised real concerns about student equity and trust. Studies have found that students with high test anxiety perform worse under online proctored conditions than in other settings, suggesting that the monitoring environment itself can get in the way of students showing what they actually know [9]. Research has also shown that students broadly perceive these systems as surveillance tools rather than fair assessment practices, raising questions about autonomy and whether the technology treats students equitably [10]. These concerns are further supported by documented accounts of automated flagging systems working against students of color, disabled students, and other underrepresented groups due to built-in biases in how the software was designed [11]. This work responds to these concerns by starting with instructor-mediated review — faculty make all approval decisions and no biometric templates or behavioral profiles are collected or stored at any stage.

However, instructor manual review alone is not scalable to large-enrollment courses. As deployments grow, some degree of automation becomes necessary, but the design question is not simply whether to automate. Rather, it is how to do so in ways that preserve student perceptions of fairness, maintain assessment quality, and reduce instructor burden without reintroducing the surveillance concerns that plague existing platforms. Limited prior work has examined this tradeoff within engineering education workflows. The system presented in this paper represents a first step toward answering these questions in a real engineering course context.

System Overview

The blockchain layer is implemented through BCdiploma, a third-party credentialing service that handles all blockchain anchoring and credential issuance on the platform's behalf, meaning the platform itself does not manage blockchain infrastructure or private keys. This layer is modular by design — the workflow does not depend on blockchain specifically, and the credential issuance step could be served by other verifiable credential systems without altering the assessment or review process. Figure 1 maps the end-to-end process across all four roles and serves as a reference for the description that follows.

From the student's perspective, the process begins with authenticated login and assessment selection. Students complete the assigned assessment, which may include multiple-choice and short free-response questions or a coding problem, and submit their work alongside a webcam and screen recording captured during the session. No biometric templates are extracted from these recordings — they exist solely to support instructor review (Figure 1, Student lane).

The instructor experience is where the most consequential educational decisions happen. Faculty access an administrative dashboard that presents each student submission alongside the corresponding session recording, the AI-generated score and feedback, and the student's submitted code. Instructors can accept the AI score, override it, or reject the submission entirely — the system supports the instructor's decision but does not constrain it. All review actions, score adjustments, and approval decisions are logged, creating an auditable record visible to the student and available for institutional review (Figure 1, Instructor lane). No credential is issued without this step. This design keeps faculty judgment at the center of the credentialing process; the system supports the instructor's decision but does not replace it. For large enrollments, this review process will be supported by automated flagging tools that surface only submissions warranting closer attention, so instructors spend their time on edge cases rather than routine review.

When a submission is approved, a tamper-evident credential is automatically issued and added to the student's portfolio. The credential is tied to a specific course milestone, meaning it represents a demonstrated, verifiable competency rather than a course grade. Students own their credential record and can share it independently by embedding the link in a resume or professional profile. A verifier who receives that link can view the credential directly — including the competencies demonstrated and the course context — and use the credential identifier embedded in the link to confirm its authenticity against the blockchain record, with no need to contact the course instructor or university (Figure 1, Verifier lane).

Preliminary Functional Validation and Prototype Feedback

The prototype was tested internally with six students (n = 6) in an IRB-exempt, formative setting, focusing on whether the workflow functioned as intended. The results are not used to evaluate student perceptions or system effectiveness. Submissions, instructor review, and credential issuance all performed correctly. Instructor reviewers noted that the dashboard was clear and that the approval decision felt straightforward, providing early confirmation that the human-in-the-loop model is workable from a teaching practice standpoint.

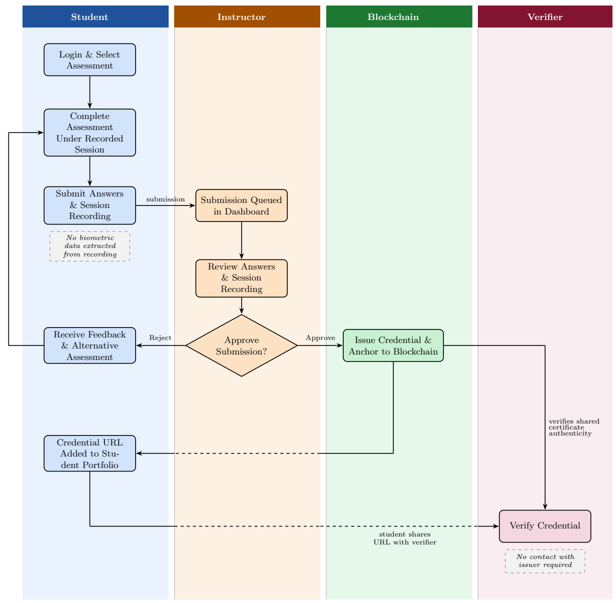

Figure 1: System workflow across student, instructor, blockchain, and verifier roles, from assessment login through credential issuance and independent verification.

As part of this formative pilot, the six students completed an anonymous survey across five dimensions summarized in Table 1. Given the small sample (n = 6) and non-evaluative nature of the pilot, these results should be read as directional signals rather than findings. With that framing, ease of use and educational fit were rated highest, while privacy comfort showed the most variation — suggesting it warrants closer attention in the larger deployment. Two qualitative responses stood out. One participant emphasized the need for clear on-boarding: *"A short introduction or video explaining the system and testing process would help new users understand the purpose of each step."* Another reflected on the potential professional value of competency-based credentials: *"These micro-credentials could help software engineers show specific skills that don't appear on a transcript. That might even make hiring more efficient by showing earned credentials of industry desired skills instead of going through multiple technical interview rounds"*. These are early, formative impressions from a small internal pilot. This pilot does not answer the research questions. It establishes that they are worth asking.

Table 1: Likert-Scale Response Distribution (Internal Prototype Feedback, n=6)

Question	**1**	**2**	**3**	**4**	**5**
Privacy comfort	0	0	1	3	2
System usability	0	0	0	1	5
Fairness / Cheating Deterrence	0	0	1	2	3
Credential value	0	0	2	0	4
Educational Fit	0	0	0	2	4

Note: 1 = Strongly Disagree, 5 = Strongly Agree. Values represent raw participant counts.

Discussion and Future Work

The current design intentionally prioritizes privacy and instructor judgment over automation. This reduces reliance on automated biometric profiling but increases manual review burden. Future iterations will need to balance privacy preservation with scalable automation, without reintroducing surveillance-style data collection. This tension shapes the research questions this workflow is positioned to address. The sections that follow describe the phased deployment plan designed to begin answering them and outline the data collection approach that will support future empirical work.

By introducing this workflow at this stage, the paper opens a set of research questions that structured deployment can now begin to address:

RQ1: How do students perceive the fairness and privacy of an instructor-mediated proctoring and credentialing system, and what design features most influence those perceptions?

RQ2: How does instructor-mediated credential review compare to automated proctoring in terms of workload, scalability, and student trust?

RQ3: How might competency-based micro-credentials serve as meaningful signals of demonstrated skill for students transitioning to internships or employment?

As a work-in-progress paper, this paper does not fully answer these questions. Rather, it introduces the workflow and the feasibility validation that make answering them possible.

To validate the workflow before full-scale deployment, the system follows a four-phase iterative plan designed to build confidence progressively before credentials are used in any high-stakes context.

Phase 1 — Completed (n=6). The internal IRB-exempt pilot study confirmed that the core workflow functions as intended — students completed assessments, instructors reviewed submissions through the dashboard, and credentials were issued correctly for approved work. Instructor reviewers noted that the dashboard presented submissions clearly and that the approval decision felt straightforward for simple problems. However, the small sample and controlled setting mean the pilot cannot speak to student perceptions of fairness, instructor burden at scale, or credential usefulness beyond the immediate workflow — the questions that matter most for engineering education adoption.

Planned Deployment — Phases 2 through 4. The following phases are planned for the current semester, with results expected to be available by the time of the conference:

- **Phase 2 — Student Onboarding (n=200+) (Planned):** Students sign up, log in, and complete a simple mock problem to get familiar with the platform's interface and end-to-end flow. Instructors familiarize themselves with the dashboard before any real assessment begins, surfacing usability issues on both sides before stakes are introduced.
- **Phase 3 — Low-Stakes In-Class Assignment (n=200+) (Planned):** A real but simple coding problem under realistic enrollment conditions. Instructors conduct their first live review of student submissions at scale, providing the first meaningful data on review burden and workflow friction.
- **Phase 4 — Course Midterm (n=200+) (Planned):** Multiple-choice and short

free-response questions with predefined terminology sets. Instructors review only flagged submissions before credentials are issued, stress-testing the human-in-the-loop model at full course scale.

Together, these phases are designed to begin answering RQ1 — how students perceive the fairness and privacy of the system — and RQ2 — how instructor-mediated review compares to automated proctoring in terms of workload and scalability. RQ3, examining whether micro-credentials function as meaningful skill signals beyond the classroom, will require longer-term follow-up with students and industry partners after full deployment. To answer these RQs, we plan to conduct follow-up surveys and interviews with relevant stakeholders. For RQ1, we will interview a selected group of students (n=30) who participated in the course implementation to understand their fairness and privacy perceptions. For RQ2, we will collect instructor work logs from both approaches and conduct a brief survey with students to measure their trust level in each. For RQ3, we will interview instructors and potential employers to understand whether micro-credentials can serve as meaningful signals of job-relevant skills.

In addition to the phased deployment, assessments introduced in Phases 3 and 4 will be designed with ABET student outcome alignment in mind. Prior work has demonstrated that blockchain-based tokens can positively support the assessment of ABET student outcomes in engineering courses [12], suggesting that credential-based approaches are viable within existing engineering education frameworks. The credentials issued through this workflow are not intended as official ABET certifications, but as verifiable records of discrete competency that complement rather than replace traditional grades.

Limitations

The current system has not yet been evaluated at course scale, and no claims about student perceptions, instructor workload, or credential usefulness can be made from Phase 1 alone. The human-in-the-loop review model used in this phase reflects a deliberate choice appropriate for small-scale feasibility validation — one that avoids biometric template collection entirely at a stage where automation is not yet warranted.

As deployments scale, the privacy-first design principle that shapes this work extends naturally to automation. Privacy-preserving techniques under consideration include zero-knowledge proofs for liveness verification [13], biometric hashing to avoid storing raw template data, and selective blurring of session recordings. These approaches are designed to support assessment integrity without reintroducing the surveillance concerns that motivate this work's design.

Future empirical work will build on deployment results from Phases 2 through 4 and will be grounded in established educational theory. Self-Determination Theory (SDT) [14, 15] holds that human motivation is supported when people feel competent in what they are doing, autonomous in how they do it, and connected to others around them. A credentialing system that gives students ownership of verifiable skill records and transparent feedback on demonstrated competencies has the potential to support all three of these needs directly.

Expectancy-Value Theory [16] similarly suggests that students engage more deeply with tasks they perceive as both personally useful and realistically attainable. Micro-credentials explicitly tied to career-relevant competencies may increase both the perceived value of assessments and students' confidence in their ability to succeed. Together, these frameworks will guide the design of survey instruments and interview protocols in future IRB-reviewed studies, connecting empirical findings to broader questions of student motivation and engagement in engineering education.

Conclusion

Engineering education faces a genuine tension between assessment credibility and student trust. Existing approaches to remote proctoring have largely resolved this tension in favor of oversight, at a cost to student privacy and equity that the literature has well documented. This paper takes a different starting point: that credible assessment and privacy protection are not competing priorities but co-equal design requirements, and that meeting both should be possible within a real engineering course context.

The workflow introduced here is a first step toward demonstrating that. At this stage, the human-in-the-loop review model is not a permanent architecture but the most appropriate choice for small-scale feasibility validation — one that avoids biometric data collection entirely while the workflow itself is still being proven. The internal IRB-exempt pilot (n = 6) confirmed that the system is technically functional and that instructor-mediated review is workable in practice. It does not confirm that the system is fair, scalable, or useful as a credentialing mechanism — those questions require the course-scale deployment and IRB-reviewed studies that the phased plan is designed to support.

As the system scales, the privacy-preserving road-map is designed to extend assessment integrity to larger enrollments without reintroducing surveillance-style data collection. The goal is a system that earns student trust not by asking them to accept monitoring as a condition of participation, but by demonstrating that integrity and privacy can be maintained together.

If competency-based micro-credentials issued through this kind of workflow can be shown to be fair, manageable for instructors, and meaningful to employers, the implications extend beyond any single course. They point toward assessment infrastructure that serves students as portable, verifiable records of demonstrated skill — not just institutional records of completion — and that does so in a way the engineering education community can adopt without compromising the equity commitments that should guide it.

References

[1] Q. Xia *et al.*, "A scoping review on how generative artificial intelligence transforms assessment in higher education," *International Journal of Educational Technology in Higher Education*, vol. 21, no. 40, 2024.

[2] A. Johri and A. Hingle, "Students' technological ambivalence toward online proctoring and the need for responsible use of educational technologies," *Journal of Engineering Education*, vol. 112, no. 1, pp. 221–242, Jan. 2023.

[3] C. Chamon *et al.*, "WIP: Leveraging blockchain for secure and verifiable micro-credentialing in engineering education," in *Proc. IEEE Frontiers in Education Conf. (FIE)*, 2025.

[4] N. H. C. Ahmat *et al.*, "Micro-credentials in higher education institutions: Challenges and opportunities," *Asian Journal of University Education*, vol. 17, no. 3, pp. 281–290, 2021.

[5] F. Fernandes and C. Werner, "Towards a blockchain-based software engineering education," arXiv preprint arXiv:2304.04549, Apr. 2023.

[6] R. A. R. Matta, J. Texier, M. M. Larrondo-Petrie, and L. Romero, "Dedicated blockchain for the generation of digital certificates and badges in universities," in *Proceedings of the ASEE Annual Conference and Exposition*, Montreal, QC, Canada, Jun. 2025.

[7] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in *Proceedings of the 11th European Conference on Technology Enhanced Learning*, 2016, pp. 490–496.

[8] A. Mikroyannidis *et al.*, "Smart blockchain badges for open education," in *Proceedings of the European Conference on Technology Enhanced Learning*, 2018, pp. 315–322.

[9] D. Woldeab and T. Brothen, "21st century assessment: Online proctoring, test anxiety, and student performance," *International Journal of E-Learning & Distance Education*, vol. 34, no. 1, pp. 1–10, 2019.

[10] S. Coghlan, T. Miller, and J. Paterson, "Good proctor or "big brother"? Ethics of online exam supervision technologies," *Philosophy & Technology*, vol. 34, no. 4, pp. 1581–1606, 2021.

[11] S. Swauger, "Our bodies encoded: Algorithmic test proctoring in higher education," Hybrid Pedagogy, 2020. [Online]. Available: https://hybridpedagogy.org/our-bodies-encoded-algorithmic-test-proctoring-in-higher-education

[12] I. Heizelman, N. M. Bittner, E. Alvarez Vazquez, D. Ewert, and R. Striker, "Empowering engineering students: Blockchain learning tokens for assessing ABET student outcomes and enhancing quality control in innovation-based education," in *Proceedings of the ASEE Annual Conference and Exposition*, Portland, OR, USA, Jun. 2024.

[13] E. Ben-Sasson *et al.*, "Scalable, transparent, and post-quantum secure computational integrity," *IACR ePrint Archive*, 2018.

[14] R. M. Ryan and E. L. Deci, "Self-determination theory and the facilitation of intrinsic motivation," *American Psychologist*, vol. 55, no. 1, pp. 68–78, 2000.

[15] J. Cawkwell, R. M. Paul, and Y. Jazayeri, "Self-determination theory applied to a second-year engineering classroom," in *Proceedings of the Canadian Engineering Education Association (CEEA-ACG) Annual Conference*, University of Alberta, Edmonton, AB, Canada, Jun. 2024.

[16] J. S. Eccles and A. Wigfield, "Motivational beliefs, values, and goals," *Annual Review of Psychology*, vol. 53, no. 1, pp. 109–132, 2002.