

Biometric Security with AI

CS 228

Fall 2026 Section 01 In Person 3 Unit(s) 08/19/2026 to 12/07/2026 Modified 08/18/2026

Contact Information

Instructor: Dr. Amith Kamath Belman

Email: amith.kamathbelman@sjsu.edu

Office: MH 411

Office Hours

Tuesday and Thursday, 12 PM to 1 PM, In person at MH 411

Course Information

Lecture

Tu Th 10:30AM - 11:45AM

MH 422

Course Description and Requisites

Applied biometric security with AI and ML, including biometrics systems, such as fingerprint, face, Iris, palm, gait, keystroke. Machine Learning and Deep Learning driven authentication and analysis. Security of ML approaches, data poisoning attacks and spoof resistant systems. A substantial course project is required.

Prerequisite(s): CS 171 or instructor consent. Graduate student standing in Computer Science, Bioinformatics, Data Science. Or instructor consent.

Grading: Letter Graded

* Classroom Protocols

Regular attendance is an integral part of the learning process. Please arrive to class on time and make sure your cell phones are silent during the lecture.

Class time will be spent in interactive lecture. You are required to bring your wireless laptop to class. Your laptop must remain closed except for designated activities.

This class is designed with a heavy emphasis on peer learning. Many sessions are spent with peers presenting their work as a method of knowledge sharing. Students are expected to be respectful and courteous in all such interactions.

Recording and Privacy

Recording any class activities, including lectures, is only allowed with the instructor's permission. You are not permitted to share or distribute class recordings. Instructor-generated materials (like syllabi, lectures, and presentations) are protected by copyright. Violation may result in referral to Student Conduct and Ethical Development office.

Program Information

Diversity Statement - At SJSU, it is important to create a safe learning environment where we can explore, learn, and grow together. We strive to build a diverse, equitable, inclusive culture that values, encourages, and supports students from all backgrounds and experiences.

Course Goals

This course aims to:

- Provide a comprehensive understanding of biometric security concepts.
- Enable students to analyze vulnerabilities and security risks in biometric systems.
- Equip students with practical skills in designing, implementing, and testing biometric security systems.
- Foster the ability to critically evaluate recent research in biometric security and develop the skills to write and present research papers on advanced topics in the field.

Course Learning Outcomes (CLOs)

At the completion of this course, students will be able to:

- Explain foundational principles underlying biometric security systems.
- Develop algorithms for feature selection and authentication using biometric data.
- Evaluate literature in the vulnerabilities of biometric security systems and vulnerabilities in algorithms.
- Explain and develop spoofing attacks on basic biometric authentication systems.
- Develop a deep and comprehensive final paper.

Course Materials

Research papers

- There is no text book for this course. All material is from research publications in conferences or journals.
- PDF copies of research publications and notes will be provided on canvas.

Software

- Any programming language with strong support for ML and AI libraries (Python or Weka or R or MATLAB).
- Students are expected to provide a working demonstration of their project by the end of the semester.

Datasets

- Sample datasets will be provided for initial discussions. (Student projects can be based on datasets outside of those provided)
- Sources for open source datasets will also be shared.

Other Readings

- (Optional) Introduction to Biometrics, Anil K. Jain , Arun A. Ross , Karthik Nandakumar , Thomas Swearingen. Springer Cham, ISBN: 978-3-031-61675-4.
- (Optional) Introduction to Machine Learning with Applications in Information Security, Mark Stamp, CRC Press, ISBN: 9781032207179

Course Requirements and Assignments

Quizzes

There are 2 quizzes in the course covering recently discussed topics. Quizzes will be conducted either on canvas or on paper during class time.

Midterm Exams

There are two midterm exams that will take place in the classroom during class time. These are handwritten exams to be submitted on paper.

Final Culminating Activity

The final research paper must be submitted by 11:00 AM on Dec 10th as part of final culminating activity for the course. (NO LATE SUBMISSION ALLOWED)

Assignments

There are two course assignments. These assignments are a mix of mathematical problems that require solving by hand and coding-based questions that require various ML operations to be performed on biometric datasets. For implementation-based questions students can use any coding language to clearly demonstrate the requirements. Screenshots, code, and clear explanations are required for each task. All work must be done individually. Violating this will result in an assignment grade of zero and possible academic dishonesty penalties.

Late submissions are not accepted.

Project and Research paper

As the course progresses students, either individually or as groups of two, must choose a topic for further exploration and pose a clear problem statement to be solved within the semester's time frame. Deliverables include detailed research paper (ACM or IEEE conference format), periodic presentations, results, code, dataset (if any) and reference papers. This project component includes proposal presentation, two project checkpoint assignments, final presentation and a final research paper submission.

Late submissions are not accepted.

Attendance

You are expected to attend all class meetings as you are responsible for all the material discussed. Active participation is essential to ensure maximum benefit. If students are absent from class, it is students' responsibility to check on announcements made while students were absent.

There are certain presentation days when student groups are assigned to present their project proposals and final projects. The students must attend and present their work on the assigned dates. No rescheduling is allowed without compelling reasons and permission from the instructor.

✓ Grading Information

The final grade in the course will be calculated based on the assignments, quizzes, midterms and project . No extra credit options will be given

Note: no make-up exams or quizzes, except emergency cases verified with official documents.

Late Work

Late work will not be accepted unless an emergency occurs, and an extension has been approved.

Academic Dishonesty

Students who are found cheating will be referred to the Student Conduct and Ethical Development office and depending on the severity of the conduct, will receive a zero on the assignment or a grade of F in the course. Grade Forgiveness does not apply to courses for which the original grade was the result of a finding of academic dishonesty.

Criteria

Type	Weight	Topic	Notes
Homework Assignments	20%		Two Homework Assignments
Quizzes	10%		Two Quizzes
Midterm Exams	30%		Two Midterm Exams
Project	40%		Includes project proposal presentation (5%), two project checkpoint assignments (5% total), final presentation and demonstration (15%) and research paper submission (15%).

Breakdown

Grade	Range	Notes
A +	98 to 100%	
A	93 to 97.99%	
A -	90 to 92.99%	
B +	87 to 89.99%	
B	83 to 86.99%	
B -	80 to 82.99%	
C +	77 to 79.99%	
C	73 to 76.99%	
C -	70 to 72.99%	
D	60 to 69.99%	
F	below 60%	

University Policies

Per [University Policy S16-9 \(PDF\)](http://www.sjsu.edu/senate/docs/S16-9.pdf) (<http://www.sjsu.edu/senate/docs/S16-9.pdf>), relevant university policy concerning all courses, such as student responsibilities, academic integrity, accommodations, dropping and adding, consent for recording of class, etc. and available student services (e.g. learning assistance, counseling, and other resources) are listed on the [Syllabus Information](https://www.sjsu.edu/curriculum/courses/syllabus-info.php) (<https://www.sjsu.edu/curriculum/courses/syllabus-info.php>) web page. Make sure to visit this page to review and be aware of these university policies and resources.

Course Schedule

Tentative Course Schedule

Week	Date	Day	Topics	Quizzes, exams, assignments, project
1	Aug 20	Thu	Course logistics, introduction, syllabus review	Syllabus quiz (due Mon Aug 24)
2	Aug 25	Tue	Basics math refresher 1: distributions, gradients, Hough transforms, ML concepts, feature definition, extraction and reduction, foundational classifiers	
2	Aug 27	Thu	Basics math refresher 1 (continued)	
3	Sep 1	Tue	Working of a biometric system; secure enclaves, TEEs	Project proposal assignment out (due Sep 24)
3	Sep 3	Thu	Basics refresher 2: foundational classifiers, neural networks	
4	Sep 8	Tue	Performance evaluation	Assignment 1 out (due Sep 29)
4	Sep 10	Thu	Performance evaluation (continued)	
5	Sep 15	Tue	Fingerprints and facial recognition	
5	Sep 17	Thu	Fingerprints and facial recognition (continued)	
6	Sep 22	Tue	Facial recognition, iris and palmprint	
6	Sep 24	Thu	Facial recognition, iris and palmprint (continued)	Project proposal due
7	Sep 29	Tue	Proposal presentations	Assignment 1 due Project checkpoint 1 assignment out (due Oct 22)
7	Oct 1	Thu	Proposal presentations	

Week	Date	Day	Topics	Quizzes, exams, assignments, project
8	Oct 6	Tue	Proposal presentations (remaining teams); iris and palmprint	
8	Oct 8	Thu	Quiz 1 and Midterm 1 review	Quiz 1
9	Oct 13	Tue	Midterm Exam 1	Midterm 1
9	Oct 15	Thu	Voice authentication	
10	Oct 20	Tue	Introduction to continuous authentication and behavioral biometrics	Project checkpoint 2 assignment out (due Nov 19)
10	Oct 22	Thu	Continuous authentication and behavioral biometrics (continued)	Project checkpoint 1 due
11	Oct 27	Tue	Adversarial machine learning: attacks and defenses on biometric systems	Assignment 2 out after the data poisoning lecture (due Nov 12)
11	Oct 29	Thu	Adversarial machine learning: attacks and defenses on biometric systems (continued)	
12	Nov 3	Tue	Attacks and defenses on biometric systems	
12	Nov 5	Thu	Attacks and defenses on biometric systems (continued)	
13	Nov 10	Tue	Attacks and defenses on biometric systems	
13	Nov 12	Thu	Attacks and defenses on biometric systems (continued)	
14	Nov 17	Tue	Frontier topics	
14	Nov 19	Thu	Quiz 2 and Midterm 2 review	Quiz 2 Project checkpoint 2 due
15	Nov 24	Tue	Midterm Exam 2	Midterm 2
15	Nov 26	Thu	Thanksgiving holiday, no class (campus closed)	
16	Dec 1	Tue	Final project presentations (day 1)	
16	Dec 3	Thu	Final project presentations (day 2)	
	Dec 10	Thu	Culminating activity: research paper due 11:00 AM	Culminating activity