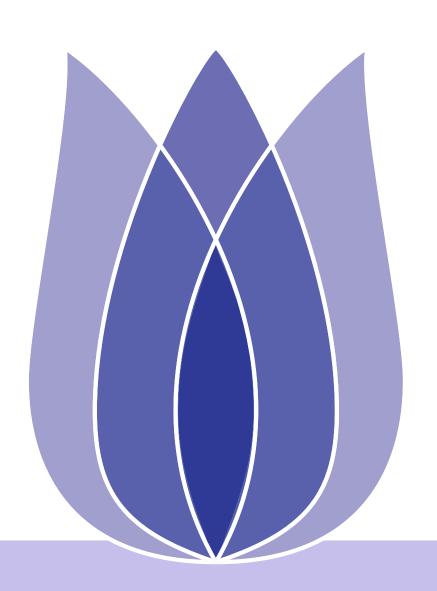
# FUNDAMENTALS OF LEARNING AND INFORMATION PROCESSING

# SESSION 20: TULIP APPROACH TO RESEARCH (II)





Gang Li

Deakin University, Australia

2024-03-19



### **Table of Content**

Opportunities for Research Students

Opportunities for Faculty Members

Road to Success

### Opportunities for Research Students

Experience

Mentorship

Skills

Frontiers

**Publications** 

### Opportunities for Faculty Members

Collaboration

Leadership

Mentoring

Growth

Grants





### Opportunities for Research Students

Experience

Mentorship

Skills

Frontiers

Publications

Opportunities for Faculty Members

Road to Success

# Opportunities for Research Students





### Students Opportunities > Experience

Opportunities for Research Students

#### Experience

Mentorship

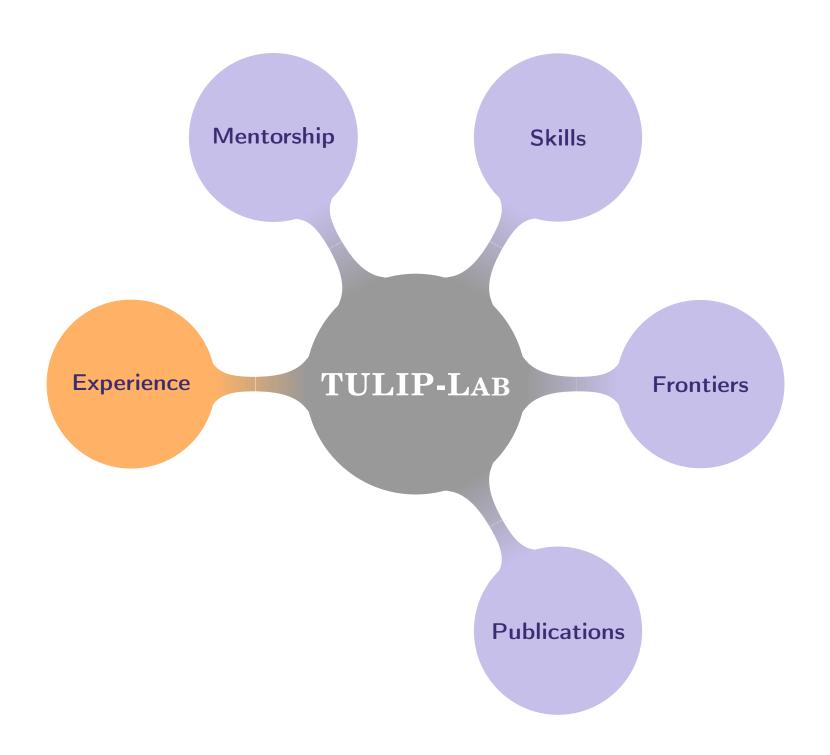
Skills

Frontiers

**Publications** 

Opportunities for Faculty Members

Road to Success





Cutting-edge AI, cybersecurity & privacy research topics





## Students Opportunities > Experience

Opportunities for Research Students

#### Experience

Mentorship

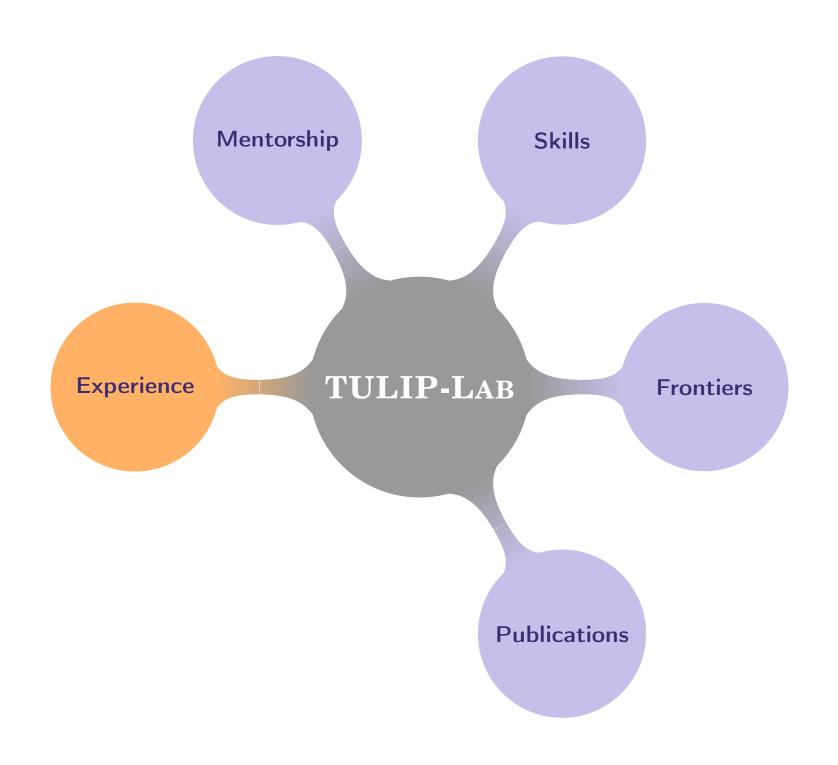
Skills

**Frontiers** 

**Publications** 

Opportunities for Faculty Members

Road to Success





Cutting-edge AI, cybersecurity & privacy research topics

### State of the Art.

gain immersive practical experience working on the frontlines of AI, cybersecurity and privacy research.





### Students Opportunities - Experience

Opportunities for Research Students

#### Experience

Mentorship

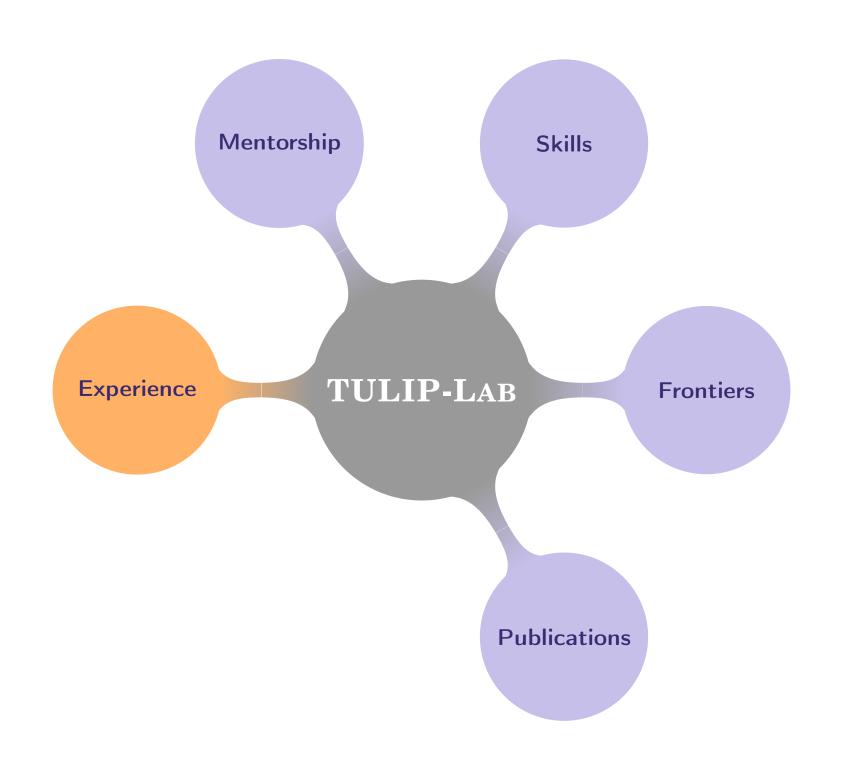
Skills

Frontiers

**Publications** 

Opportunities for Faculty Members

Road to Success





Cutting-edge AI, cybersecurity & privacy research topics

### State of the Art.

- gain immersive practical experience working on the frontlines of AI, cybersecurity and privacy research.
- develop new models, test defensive strategies, analyze real-world data for privacy risks





### Students Opportunities - Experience

Opportunities for Research Students

#### Experience

Mentorship

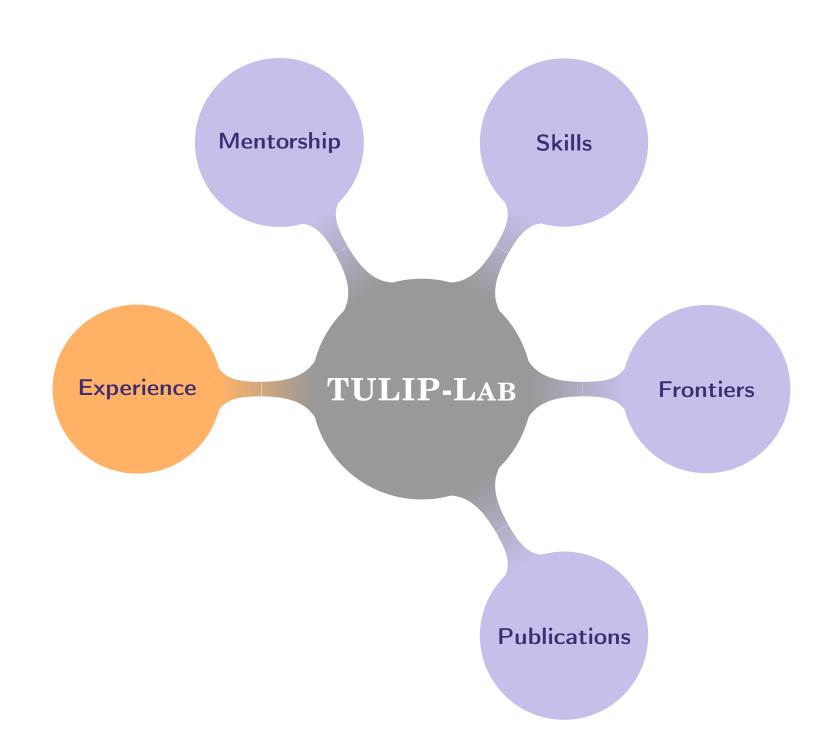
Skills

Frontiers

**Publications** 

Opportunities for Faculty Members

Road to Success





Cutting-edge AI, cybersecurity & privacy research topics

### State of the Art.

- gain immersive practical experience working on the frontlines of AI, cybersecurity and privacy research.
- develop new models, test defensive strategies, analyze real-world data for privacy risks
- contribute to innovative research prototypes and systems.





### Students Opportunities > Mentorship

Opportunities for Research Students

Experience

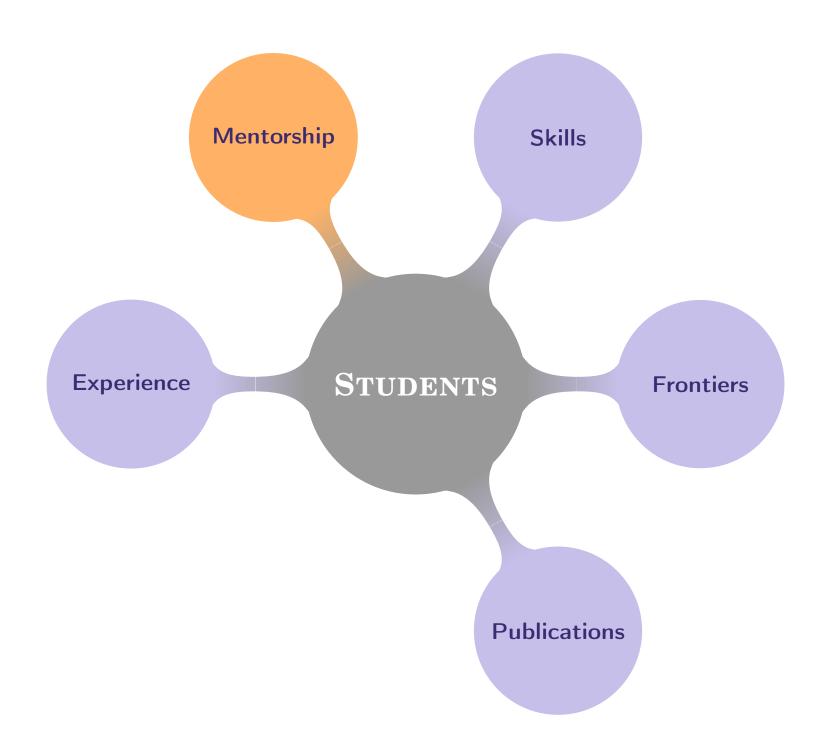
#### Mentorship

Skills

Frontiers

Publications

Opportunities for Faculty Members









### Students Opportunities > Mentorship

Opportunities for Research Students

Experience

#### Mentorship

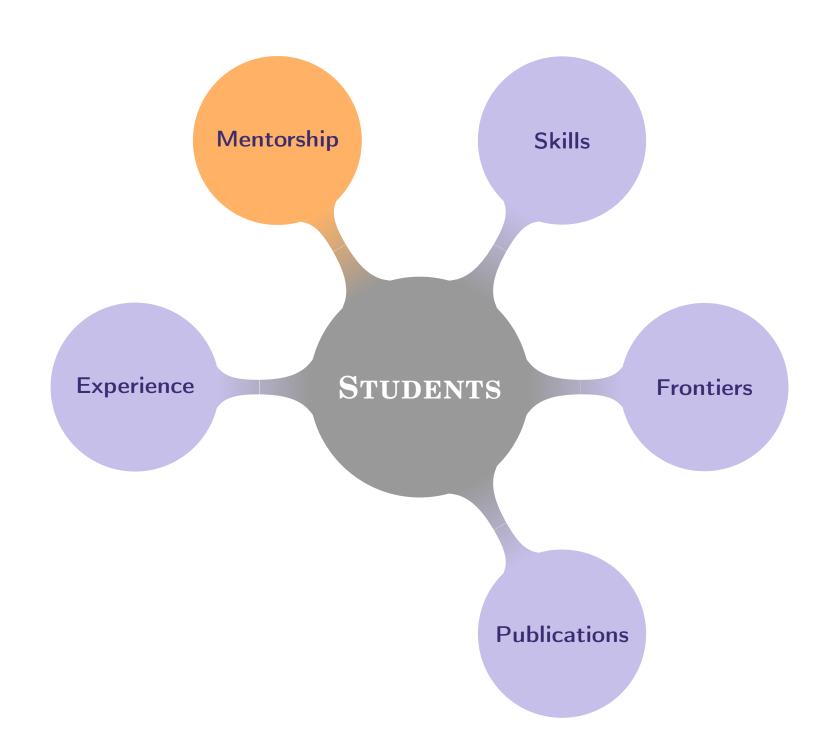
Skills

Frontiers

Publications

Opportunities for Faculty Members

Road to Success





 receive close mentorship from TULIP-LAB faculty members





### Students Opportunities > Mentorship

Opportunities for Research Students

Experience

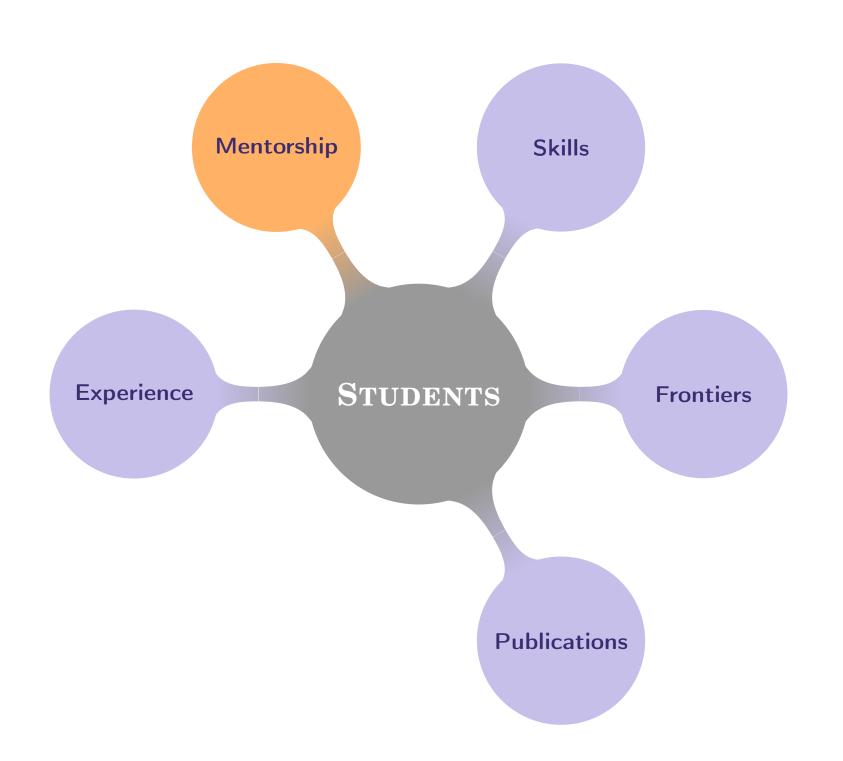
#### Mentorship

Skills

Frontiers

Publications

Opportunities for Faculty Members





- receive close mentorship from TULIP-LAB faculty members
- mentors will guide students through the research process from ideation to the technical report.





## Students Opportunities > Skills

Opportunities for Research Students

Experience

Mentorship

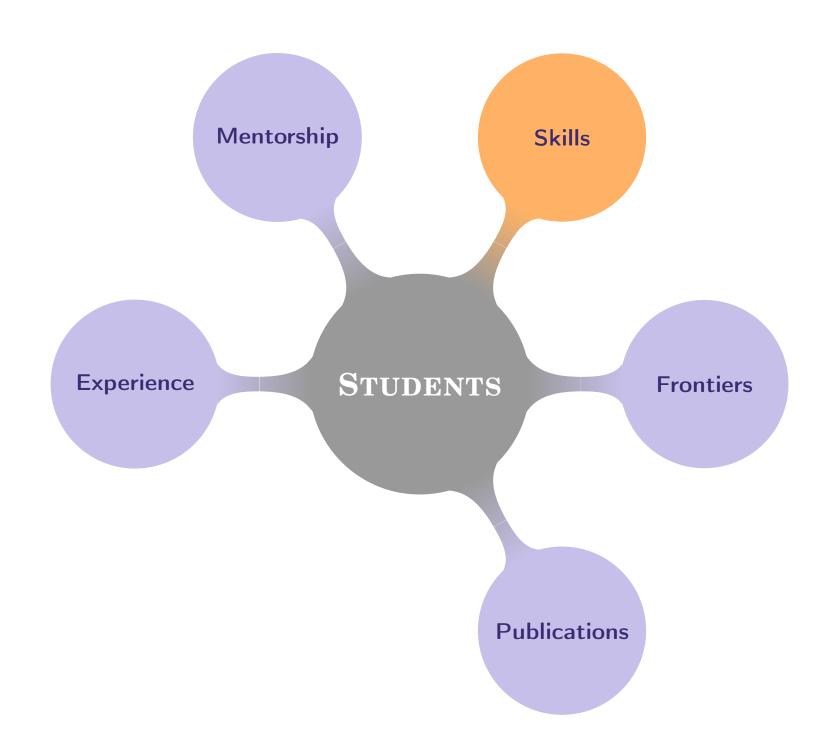
#### Skills

Frontiers

**Publications** 

Opportunities for Faculty Members

Road to Success





Highly valuable technical and analytical abilities





### Students Opportunities > Skills

Opportunities for Research Students

Experience

Mentorship

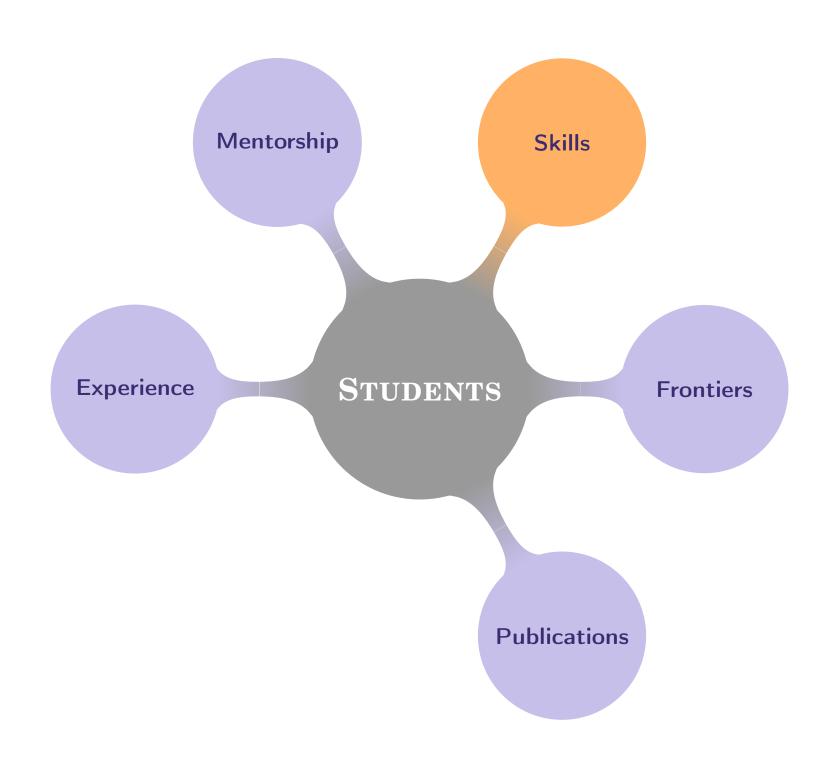
#### Skill

Frontiers

**Publications** 

Opportunities for Faculty Members

Road to Success





build comprehensive skills for research and industry



### Students Opportunities > Skills

Opportunities for Research Students

Experience

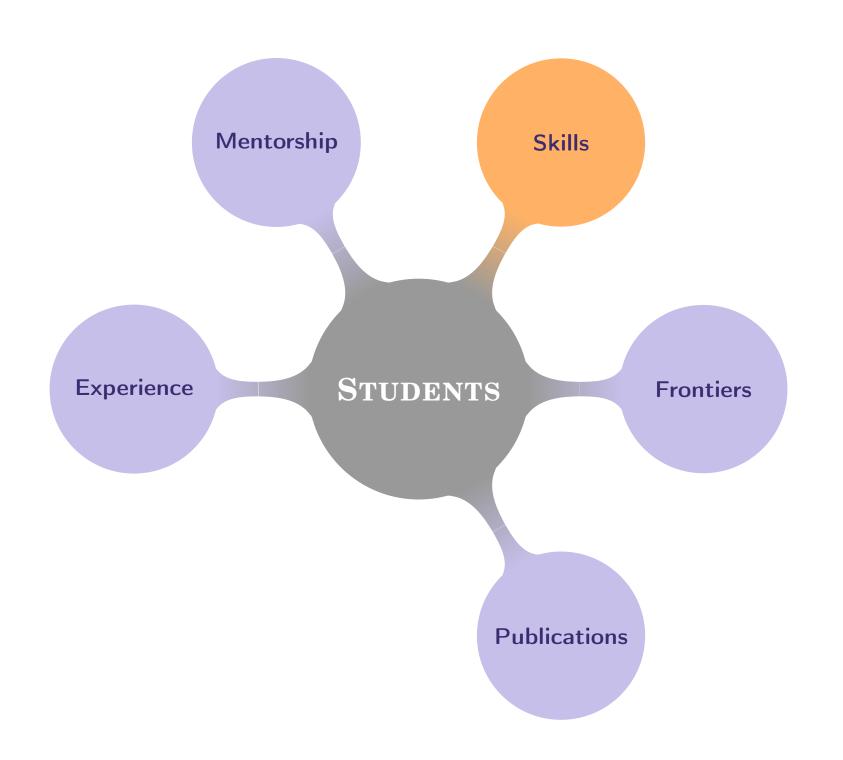
Mentorship

#### Skil

Frontiers

Publications

Opportunities for Faculty Members





- build comprehensive skills for research and industry
- expected research skills





# **Expected Research Skills**

Opportunities for Research Students

Experience

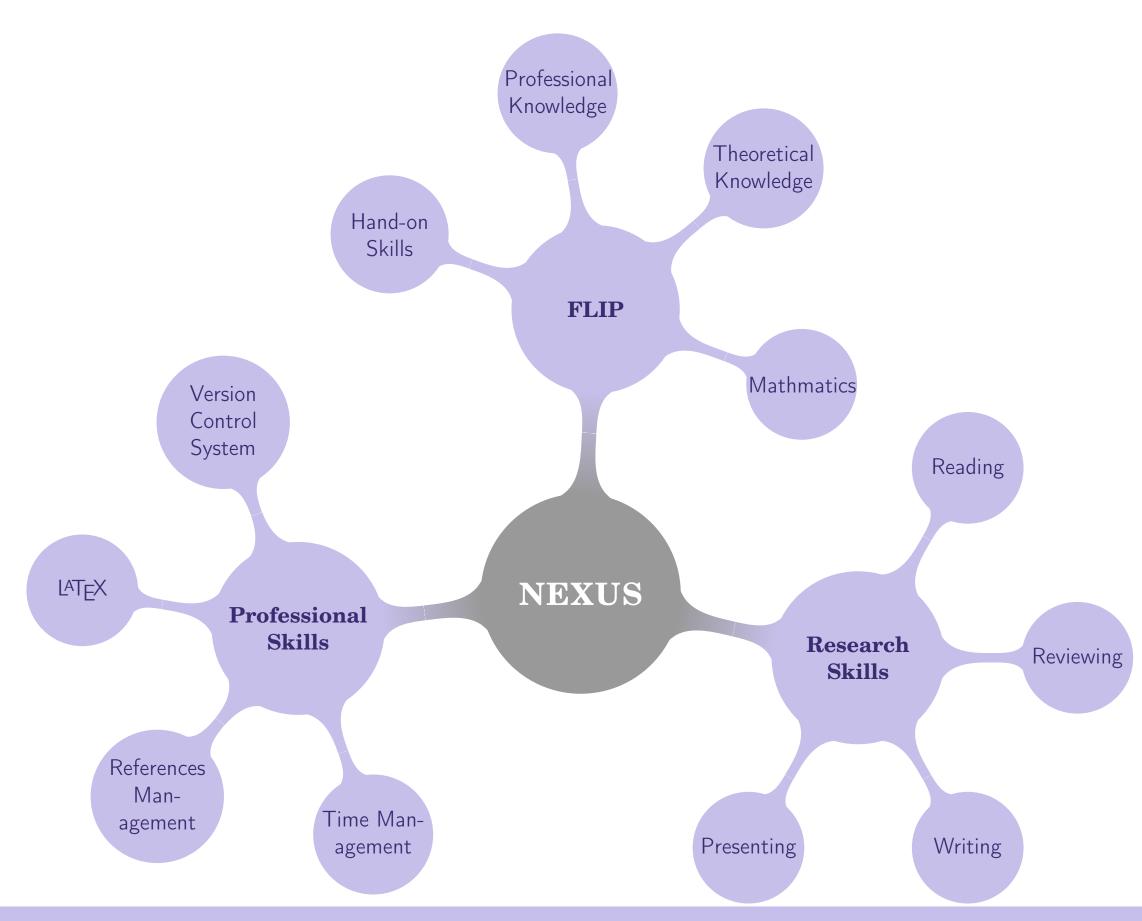
Mentorship

Skills

Frontiers

**Publications** 

Opportunities for Faculty Members







### **Students Opportunities** > Frontiers

Opportunities for Research Students

Experience

Mentorship

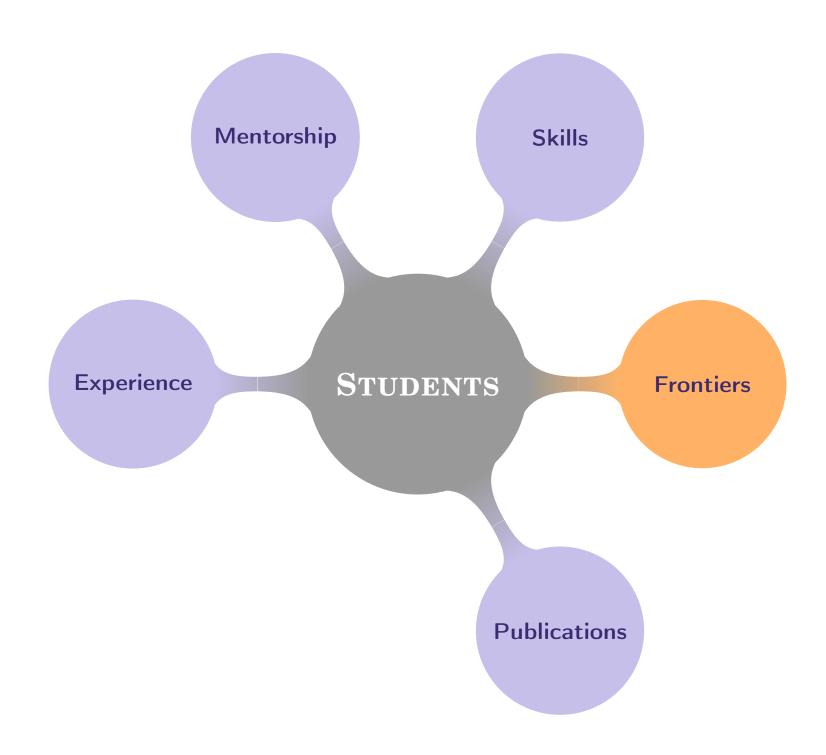
Skills

#### Frontiers

**Publications** 

Opportunities for Faculty Members

Road to Success





Explore state-of-the-art advancements in AI, S&P etc.





### **Students Opportunities** Frontiers

Opportunities for Research Students

Experience

Mentorship

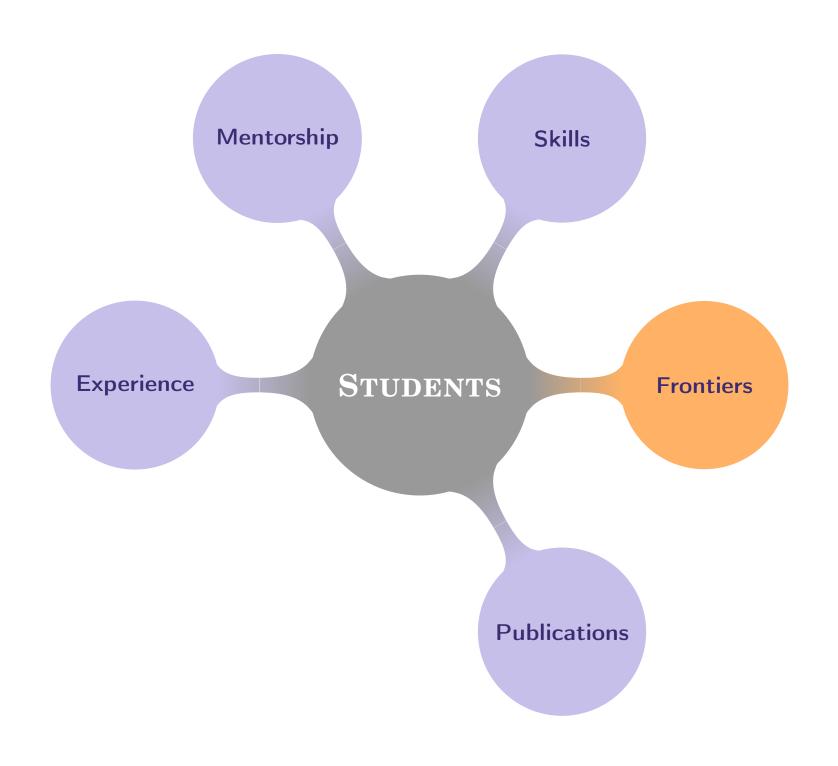
Skills

#### Frontiers

**Publications** 

Opportunities for Faculty Members

Road to Success





Explore state-of-the-art advancements in AI, S&P etc.

works on the bleeding-edge of AI capabilities and emerging cybersecurity & privacy challenges.





### Students Opportunities > Frontiers

Opportunities for Research Students

Experience

Mentorship

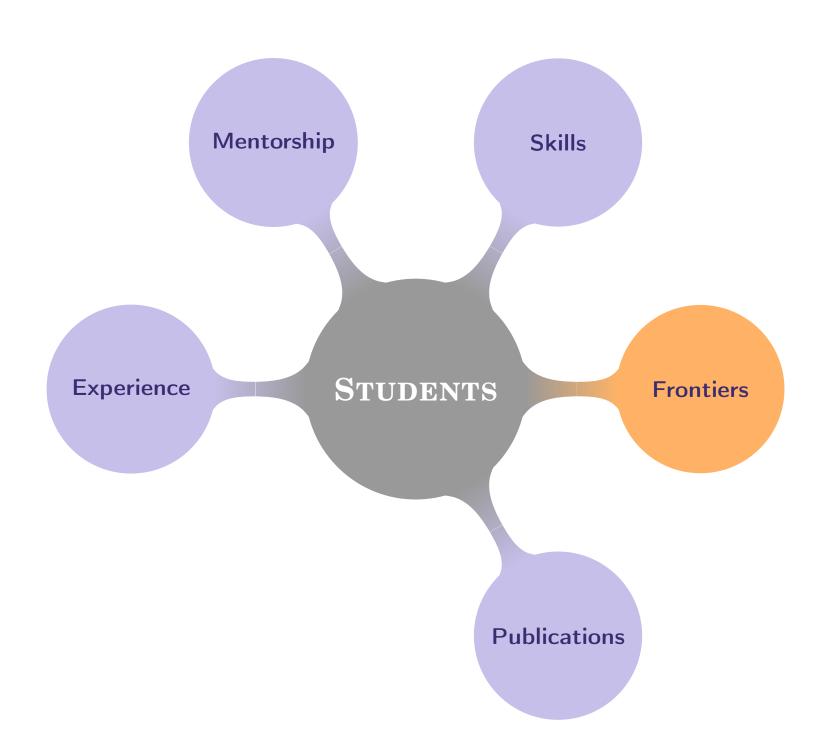
Skills

#### Frontie

**Publications** 

Opportunities for Faculty Members

Road to Success





Explore state-of-the-art advancements in AI, S&P etc.

 works on the bleeding-edge of AI capabilities and emerging cybersecurity

& privacy challenges.

attend seminars, conferences and meetings to learn about the latest directly from pioneers in these rapidly evolving fields.





# Students Opportunities > Publications

Opportunities for Research Students

Experience

Mentorship

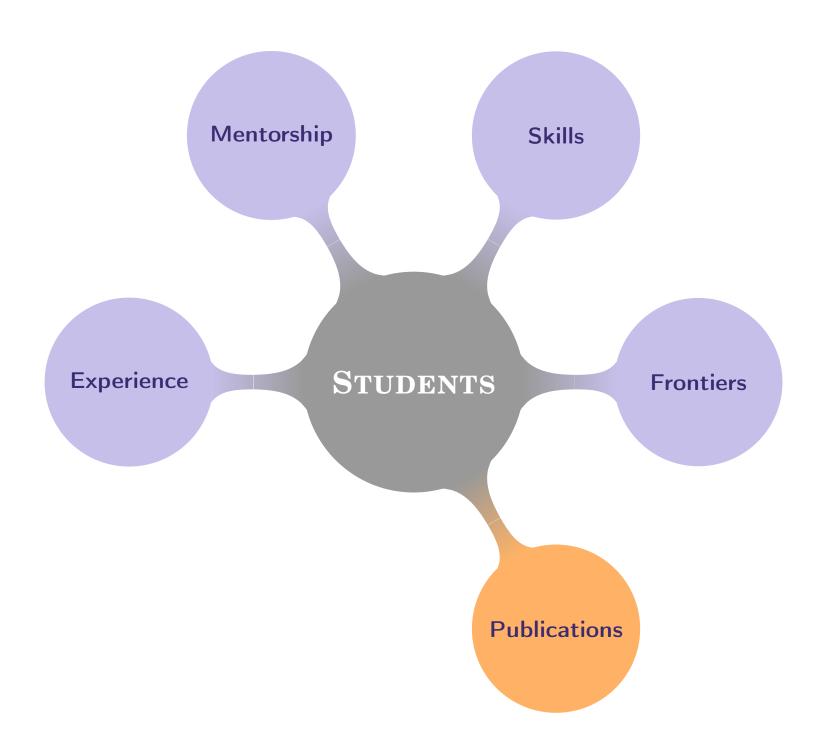
Skills

Frontiers

#### Publications

Opportunities for Faculty Members

Road to Success





Opportunities to co-author impactful research





### Students Opportunities > Publications

Opportunities for Research Students

Experience

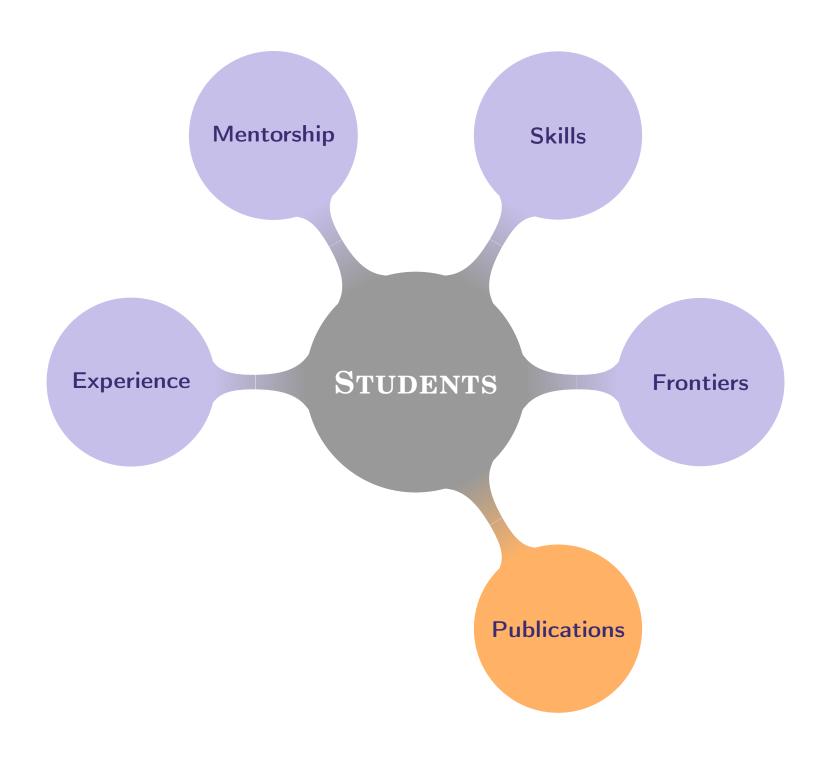
Mentorship

Skills

**Frontiers** 

Opportunities for Faculty Members

Road to Success





Opportunities to co-author impactful research

By contributing to cutting-edge projects, top students can co-author publications in prestigious AI, security and privacy venues.





### Students Opportunities > Publications

Opportunities for Research Students

Experience

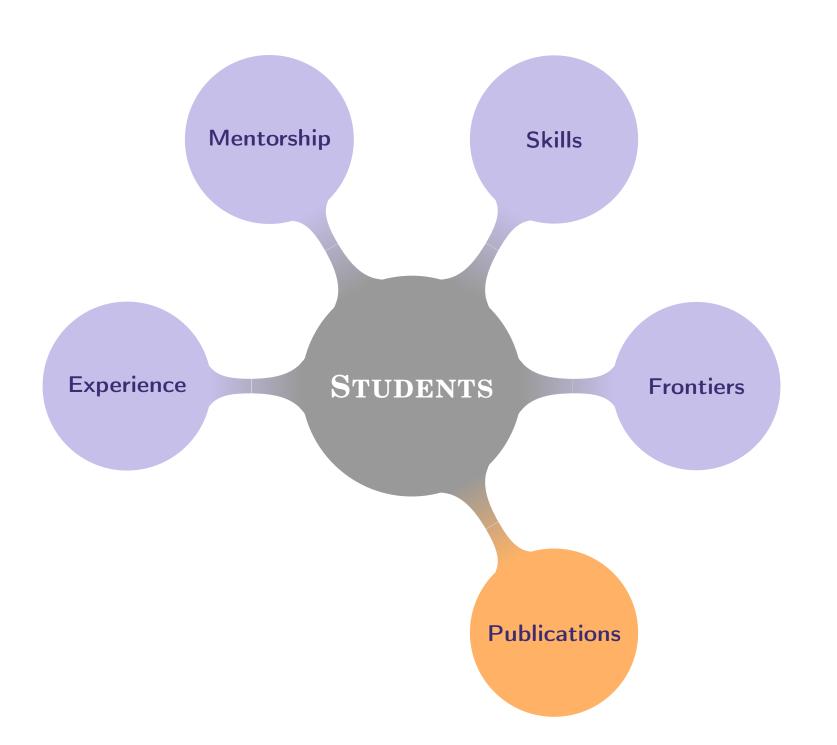
Mentorship

Skills

**Frontiers** 

Opportunities for Faculty Members

Road to Success





Opportunities to co-author impactful research

- By contributing to cutting-edge projects, top students can co-author publications in prestigious AI, security and privacy venues.
- This provides exposure, bolsters academic credentials and allows mastering the publication process from conducting rigorous research to communicating findings effectively through publications and presentations.





Opportunities for Research Students

#### Opportunities for Faculty Members

Collaboration

Leadership

Mentoring

Growth

Grants

Road to Success

# Opportunities for Faculty Members





# Faculty Opportunities - Collaboration

Opportunities for Research Students

Opportunities for Faculty Members

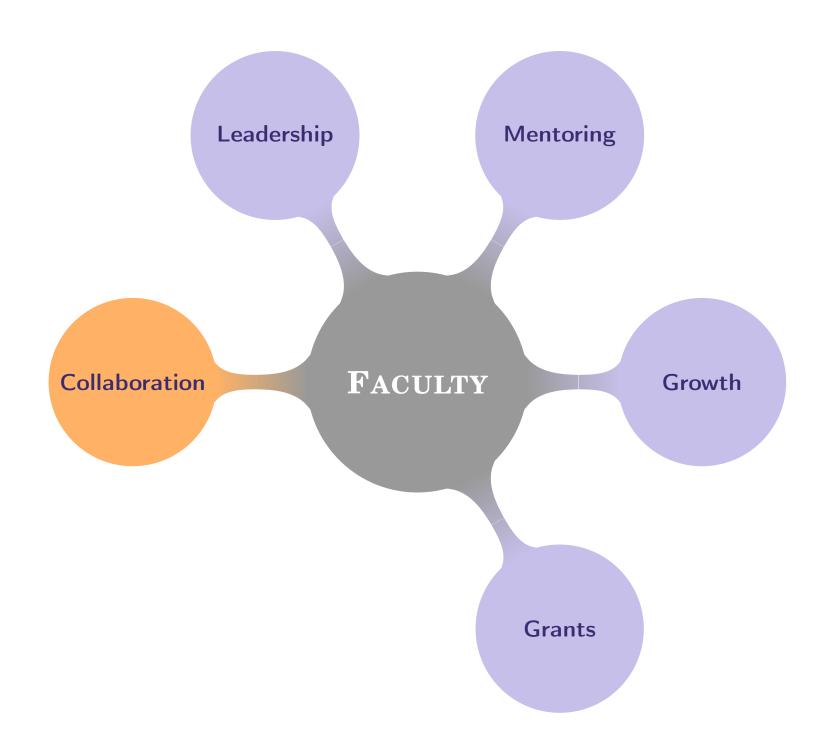
#### Collaboration

Leadership

Mentoring

Growth

Grants









# Faculty Opportunities - Collaboration

Opportunities for Research Students

Opportunities for Faculty Members

#### Collaboration

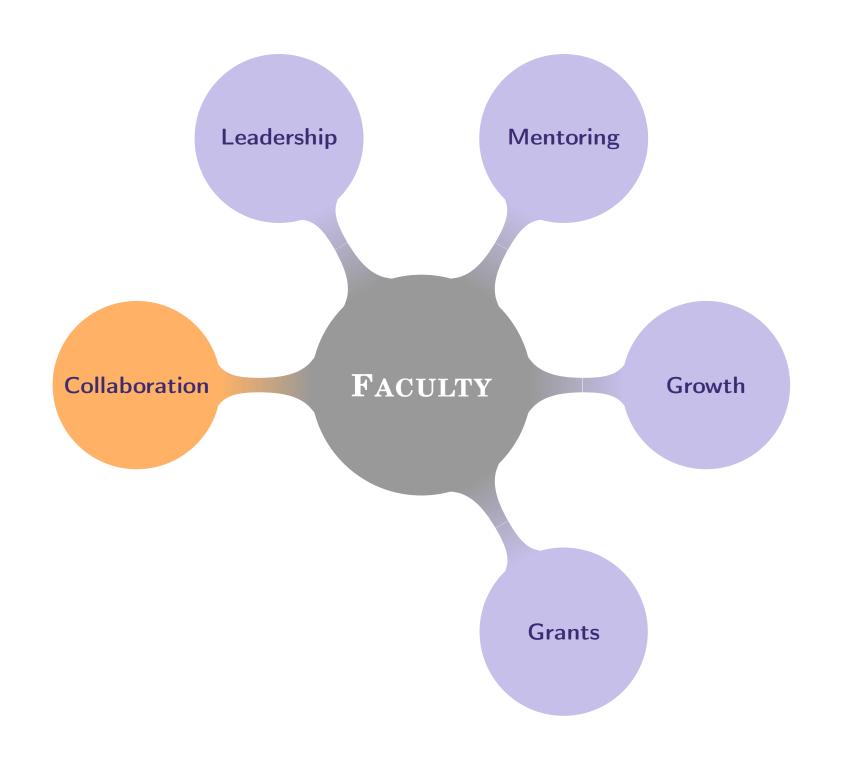
Leadership

Mentoring

Growth

Grants

Road to Success





Collaborate with faculty across disciplines across different sectors to tackle complex, multifaceted AI risk challenges.





### Faculty Opportunities Collaboration

Opportunities for Research Students

Opportunities for Faculty Members

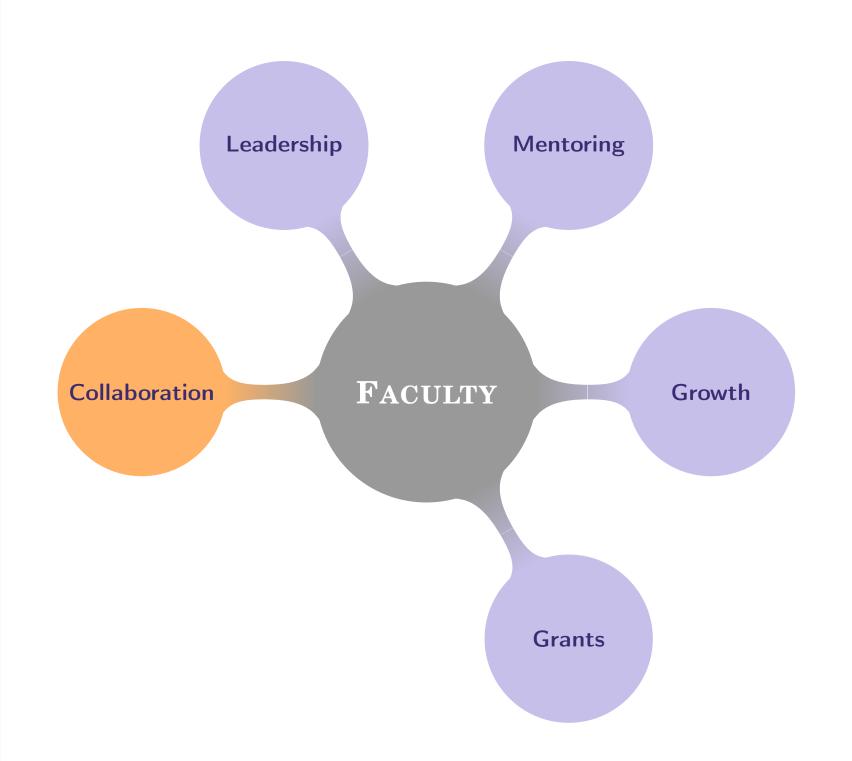
#### Collaboration

Leadership

Mentoring

Growth

Grants





- Collaborate with faculty across disciplines across different sectors to tackle complex, multifaceted AI risk challenges.
- Work within collaborative cross-functional teams that unite diverse AI, security, software engineering and domain expertise.





## Faculty Opportunities - Leadership

Opportunities for Research Students

Opportunities for Faculty Members

Collaboration

#### Leadership

Mentoring

Growth

Grants

Road to Success





Driving innovative research initiatives





### Faculty Opportunities > Leadership

Opportunities for Research Students

Opportunities for Faculty Members

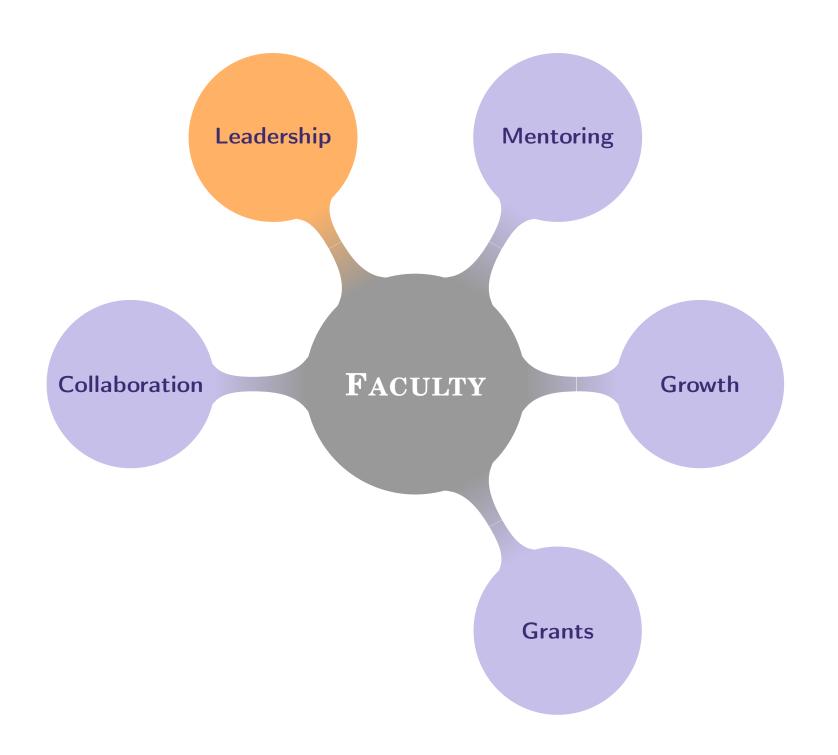
Collaboration

#### Leadership

Mentoring

Growth Grants

Road to Success





lead groundbreaking work on areas like secure and trustworthy AI, AI-powered cybersecurity, privacy-preserving machine learning and more from conceptualization through execution.





### Faculty Opportunities > Leadership

Opportunities for Research Students

Opportunities for Faculty Members

Collaboration

#### Leadership

Mentoring

Growth Grants





- lead groundbreaking work on areas like secure and trustworthy AI, AI-powered cybersecurity, privacy-preserving machine learning and more from conceptualization through execution.
- spearhead impactful projects that advance AI capabilities while proactively addressing related cybersecurity and privacy risks.
  - ◆ ACM TOPML Special Issue
  - ♦ National Science Review



### Collaborative Leadership Examples @ TULIP-LAB

Opportunities for Research Students

Opportunities for Faculty Members

Collaboration

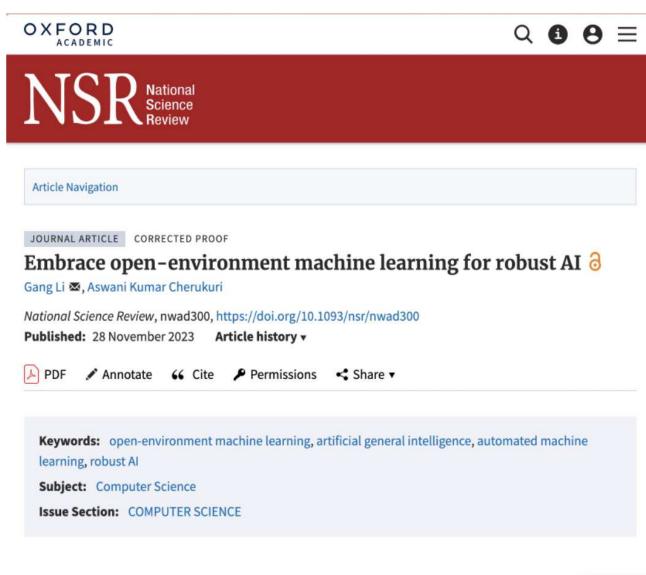
Leadership

Mentoring

Growth

Grants

Road to Success



Humans possess an extraordinary ability to continuously learn and apply knowledge across differentiation of the environments and tasks, and this ability to understand and acquire diverse intellectual capabilities referred to as artificial general intelligence (AGI). The realization of AGI requires the development of artificial intelligence systems [1] that can operate effectively and safely in complex and uncertain real-world scenarios. Despite significant advances in conventional machine learning over the last few decades, achieving robust AI or ultimate AGI remains a challenge, especially in the era where practical machine learning applications have expanded into open-environment scenarios, such as cybersecurity and multi-



#### **ACM Transactions on Probabilistic Machine Learning**

Special Issue on Probabilistic Methods for Reliable Machine Learning in Open Environments

#### **Guest Editors:**

- Dr Lan Du, Monash University, Australia, lan.du@ieee.org
- Prof. Aswani Kumar Cherukuri, Vellor Institute of Technology, India, <a href="mailto:cherukuri@acm.org">cherukuri@acm.org</a>
- Prof. Gang Li, Deakin University, Australia, gangli@acm.org
- Prof. De-Chuan Zhan, Nanjing University, China, <a href="mailto:zhandc@nju.edu.cn">zhandc@nju.edu.cn</a>

Recent advances in machine learning, particularly in deep neural networks and large language models, have driven significant progress in artificial intelligence. These advanced models have achieved state-of-the-art performance in various domains, including natural language processing and computer vision. However, deploying these technologies in open environments, where they encounter diverse real-world data, presents unique challenges like evolving data distributions and emerging classes. These challenges are especially critical in safety-critical systems such as healthcare, autonomous vehicles, and pharmacology, where AI performance directly impacts human wellbeing.

To ensure transparency and trust and to enable human oversight, understanding the decision-making processes of machine learning models is essential. Probabilistic methods play a crucial role in illuminating the inner workings of these models, quantifying uncertainty, and assessing the reliability and robustness of predictions. This is vital in safety-critical applications where informed and responsible decisions are paramount.

In addition to probabilistic methods, enhancing machine learning models with human-understandable reasoning behind predictions is key to increasing their trustworthiness and facilitating collaboration between humans and machines. Balancing model performance and interpretability makes even complex models comprehensible, unlocking the full potential of machine/deep learning while keeping their decision-making processes transparent and open to scrutiny. The pursuit of Interpretability and Explainability in artificial intelligence promises to lead to accountable AI systems that positively impact various aspects of human society.

With the surge of applications and data from open-environment scenarios, the learning tasks become a grand challenge due to the presence of "unknown unknowns". Embracing these techniques sets the stage for Al applications that align with human values and goals while navigating complex and uncertain real-world environments with greater accuracy and integrity. This special issue invites original contributions that advance the theory and practice of reliable machine learning in Open Environments by employing approaches that use statistical and probabilistic methodologies.

**-**--!--



## Faculty Opportunities > Mentoring

Opportunities for Research Students

Opportunities for Faculty Members

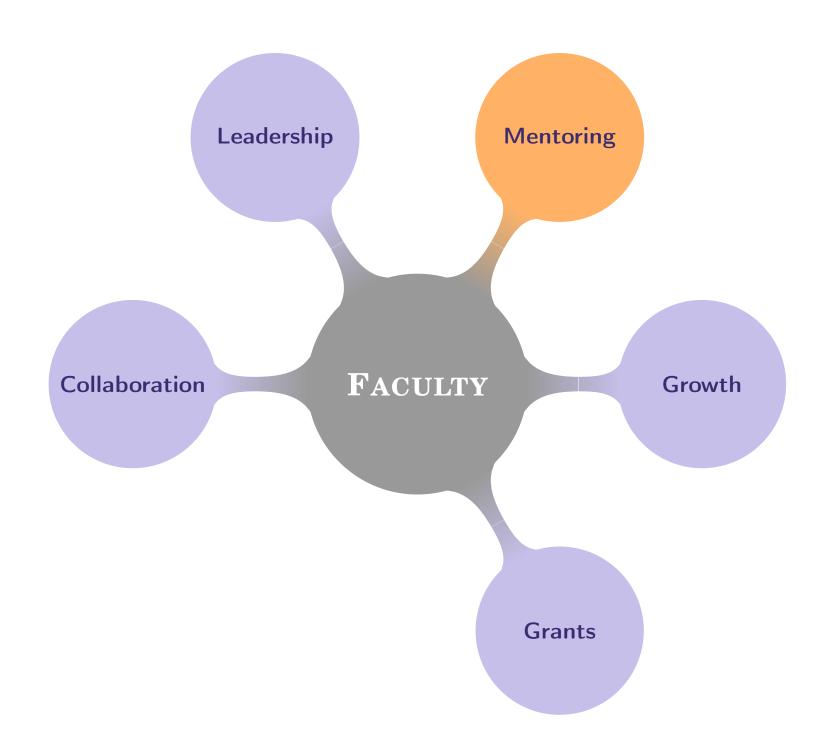
Collaboration

Leadership

Mentoring

Growth Grants

Road to Success





Shaping the next generation innovators





### Faculty Opportunities > Mentoring

Opportunities for Research Students

Opportunities for Faculty Members

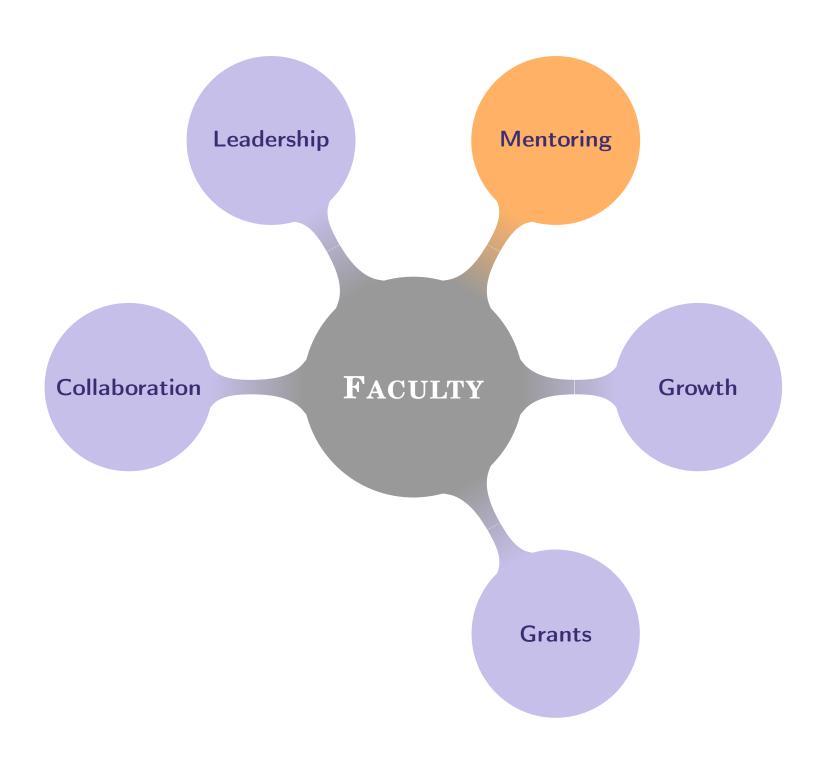
Collaboration

Leadership

Mentoring

Growth Grants

Road to Success





mentor students and junior researchers, imparting deep technical expertise in related domains.



### Faculty Opportunities Mentoring

Opportunities for Research Students

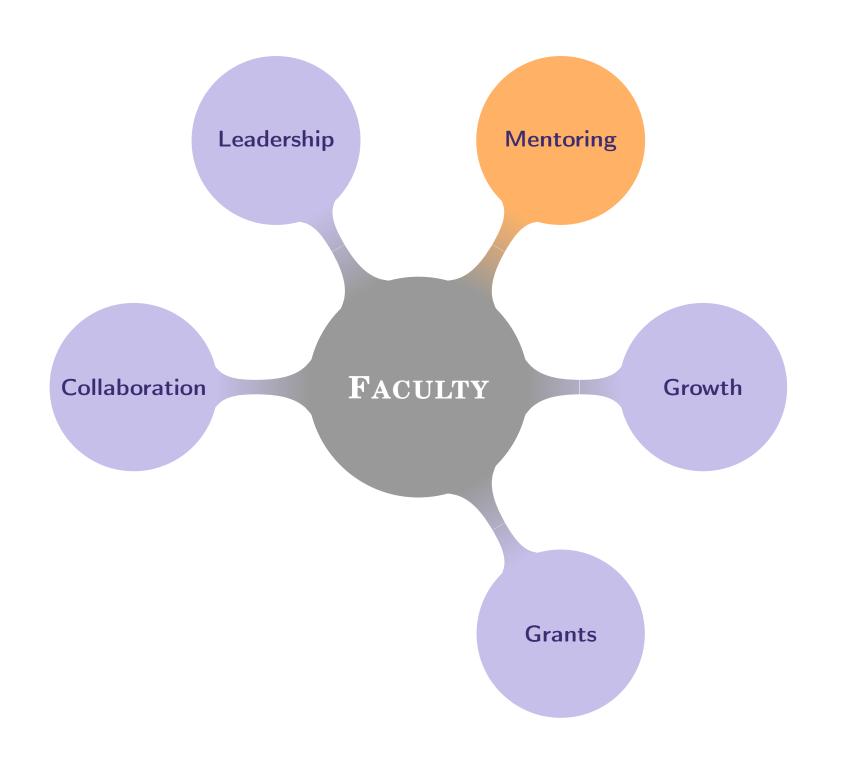
Opportunities for Faculty Members

Collaboration

Leadership

#### Mentoring

Growth Grants





- mentor students and junior researchers, imparting deep technical expertise in related domains.
- guide them on developing skills as well as research proficiencies like designing robust experiments and publishing at top venues.



### Faculty Opportunities Mentoring

Opportunities for Research Students

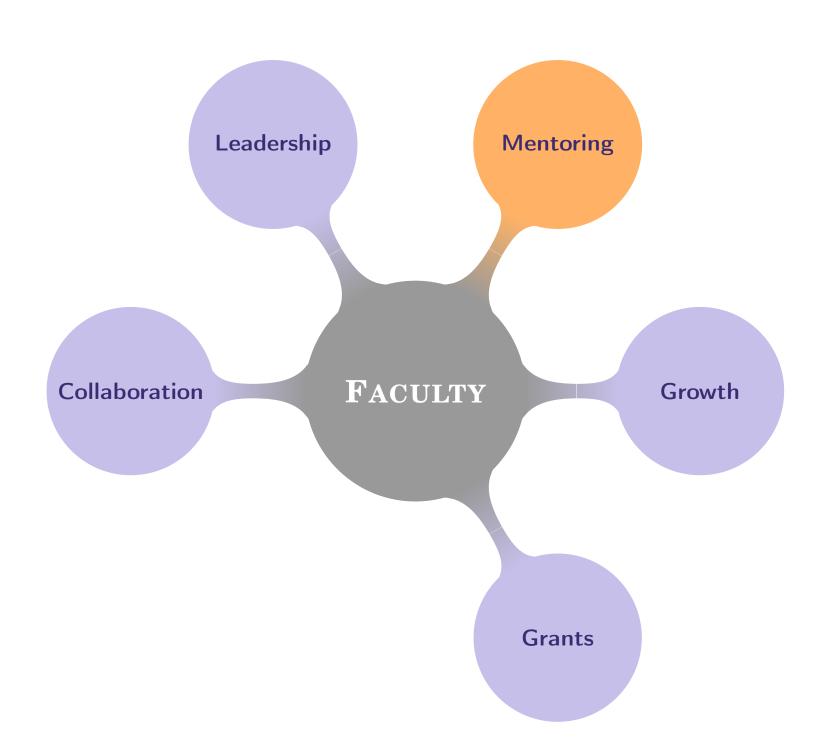
Opportunities for Faculty Members

Collaboration

Leadership

Mentoring

Growth Grants





- mentor students and junior researchers, imparting deep technical expertise in related domains.
- guide them on developing skills as well as research proficiencies like designing robust experiments and publishing at top venues.
- be an official external supervisor for PhD students in Deakin University





Opportunities for Research Students

Opportunities for Faculty Members

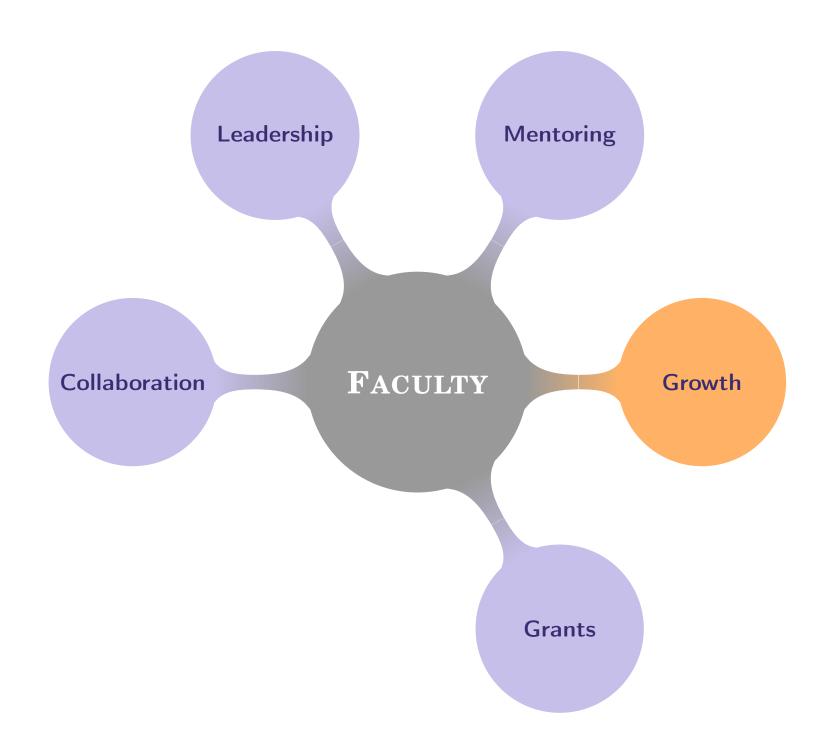
Collaboration

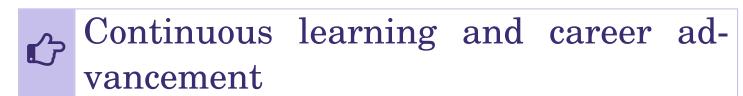
Leadership

Mentoring

Growth

Grants









Opportunities for Research Students

Opportunities for Faculty Members

Collaboration

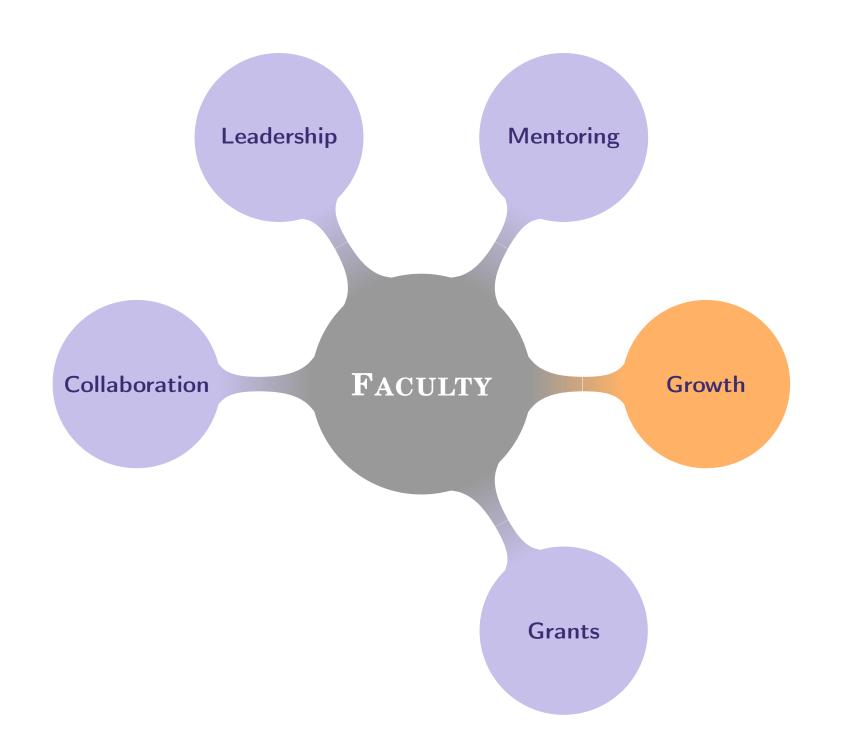
Leadership

Mentoring

Growth

Grants

Road to Success





attend conferences, workshops and certified training programs to stay ahead of the curve on rapidly progressing AI techniques, emerging threats, defensive technologies and research best practices.





Opportunities for Research Students

Opportunities for Faculty Members

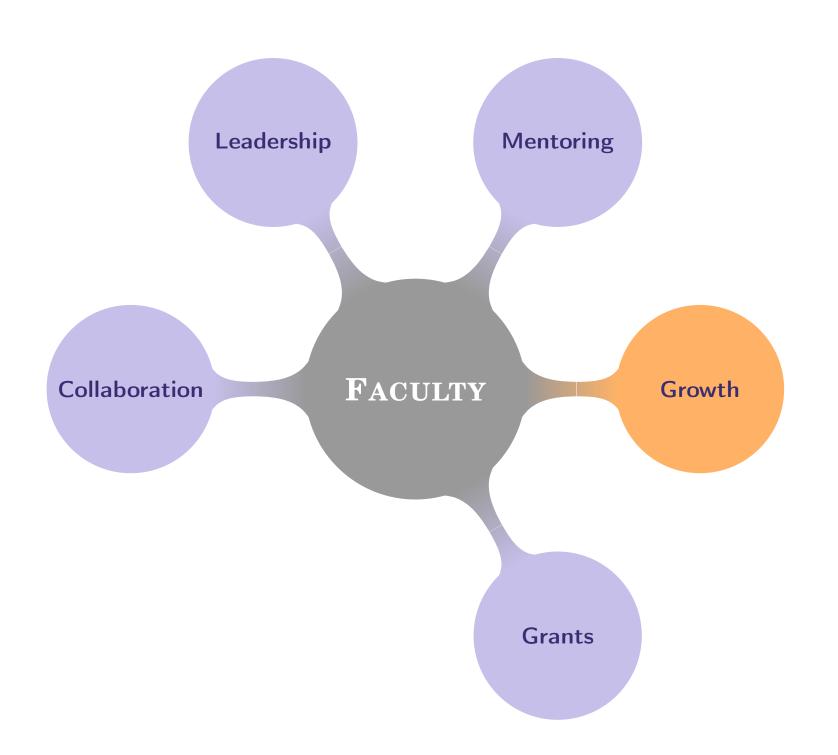
Collaboration

Leadership

Mentoring

Growth

Grants





- attend conferences, workshops and certified training programs to stay ahead of the curve on rapidly progressing AI techniques, emerging threats, defensive technologies and research best practices.
- develop skills in research, publishing, technology transition and take on project leadership roles for enriching professional growth.



Opportunities for Research Students

Opportunities for Faculty Members

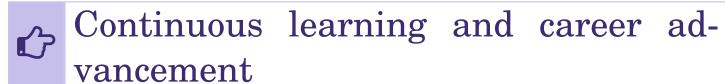
Collaboration

Leadership

Mentoring

Growth Grants





- attend conferences, workshops and certified training programs to stay ahead of the curve on rapidly progressing AI techniques, emerging threats, defensive technologies and research best practices.
- develop skills in research, publishing, technology transition and take on project leadership roles for enriching professional growth.
- IEEE Senior membership, etc.



Opportunities for Research Students

Opportunities for Faculty Members

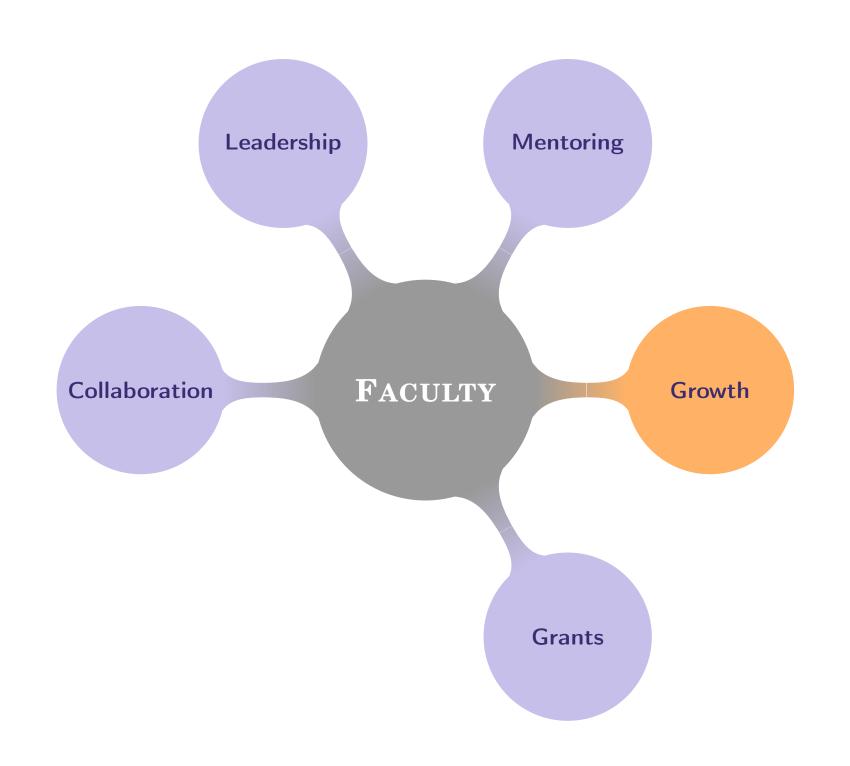
Collaboration

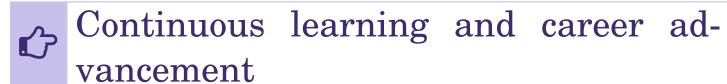
Leadership

Mentoring

Growth

Grants





- attend conferences, workshops and certified training programs to stay ahead of the curve on rapidly progressing AI techniques, emerging threats, defensive technologies and research best practices.
- develop skills in research, publishing, technology transition and take on project leadership roles for enriching professional growth.
- IEEE Senior membership, etc.
- organize or chair some International conferences:
  - **♦** KSEM Conference Series
  - **♦** ATIS Conference Series





### Conferences Chairing Opportunity with TULIP-LAB

Opportunities for Research Students

Opportunities for Faculty Members

Collaboration

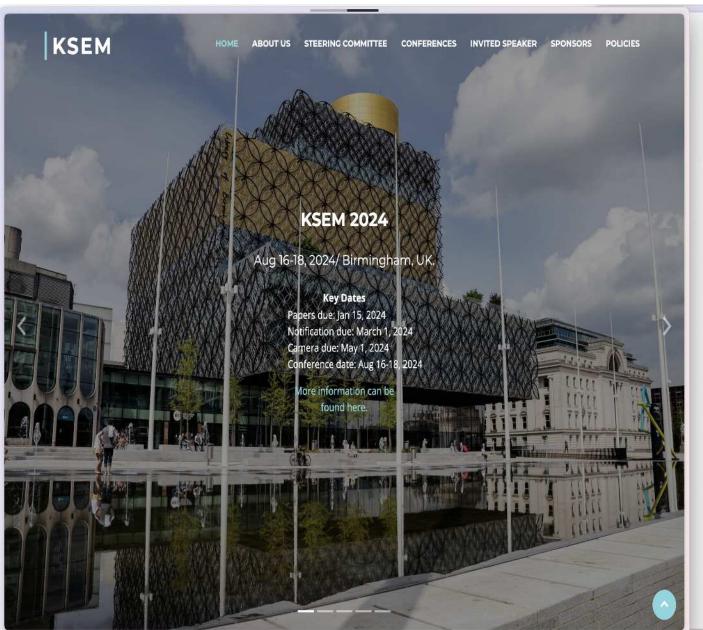
Leadership

Mentoring

Growth

Grants

Road to Success





#### **ATIS Conference Series**

The purpose of ATIS is to provide a forum for presentation and discussion of innovative ideas, research results, applications and experience from around the world as well as highlight activities in the related areas. The annual ATIS conference highlights new results in the design and analysis of digital security hardware and software implementations. ATIS provides a valuable connection between the theoretical and implementation communities and attracts participants from industry, academia, and government organizations.

#### The 14<sup>th</sup> International Conference on Applications and Techniques for Information Security

- ▶ Website: https://apps.sastra.edu/atis2024/
- ▶ Location and date: Tamil Nadu, India, November 22-24, 2024
- To be decided

### The 13<sup>th</sup> International Conference on Applications and Techniques for Information Security

- ▶ Website: http://www.atis.conferences.academy/
- Location and date: Manipal, India, December, 2022
- ATIS 2022 proceedings is published as "Applications and Techniques in Information Security" in CCIS, Springer

#### The 12<sup>th</sup> International Conference on Applications and Techniques for Information Security

#### **Steering Committee**

- ▶ Prof. Lynn Batten (Honorary Chair) Deakin University, Australia
- A/Prof. Gang Li (Chair)
   Deakin University, Melbourne,
   Australia
- Prof. Heejo Lee
- Korea University, Seoul, Korea

   Prof. Jiqiang Liu
- Beijing Jiaotong University, China

   Prof. Tsutomu Matsumoto
- Yokohama National University, Japan
- Prof. Wenjia Niu
- Beijing Jiaotong University, China

   Prof. Yuliang Zheng
  University of Alabama at
  Birmingham, USA
- Dr Shiva Pokhrel (Secretary)
   Deakin University, Melbourne,
   Australia

#### Sponsorship









Opportunities for Research Students

Opportunities for Faculty Members

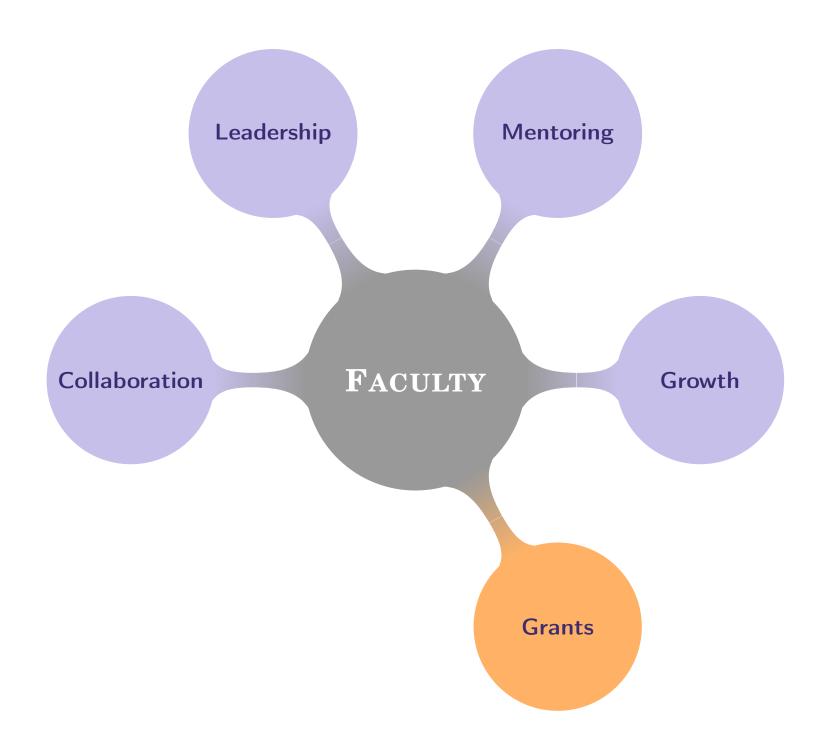
Collaboration

Leadership

Mentoring

Growth

Grants









Opportunities for Research Students

Opportunities for Faculty Members

Collaboration

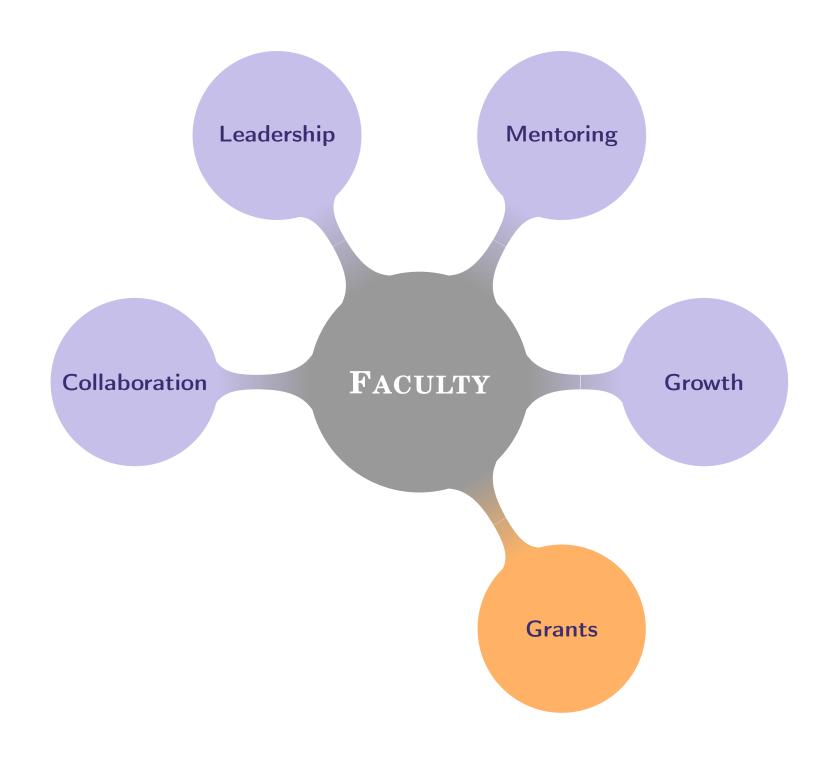
Leadership

Mentoring

Growth

Grants

Road to Success





 access to substantial internal and external funding sources to support the pioneering collaborative research





Opportunities for Research Students

Opportunities for Faculty Members

Collaboration

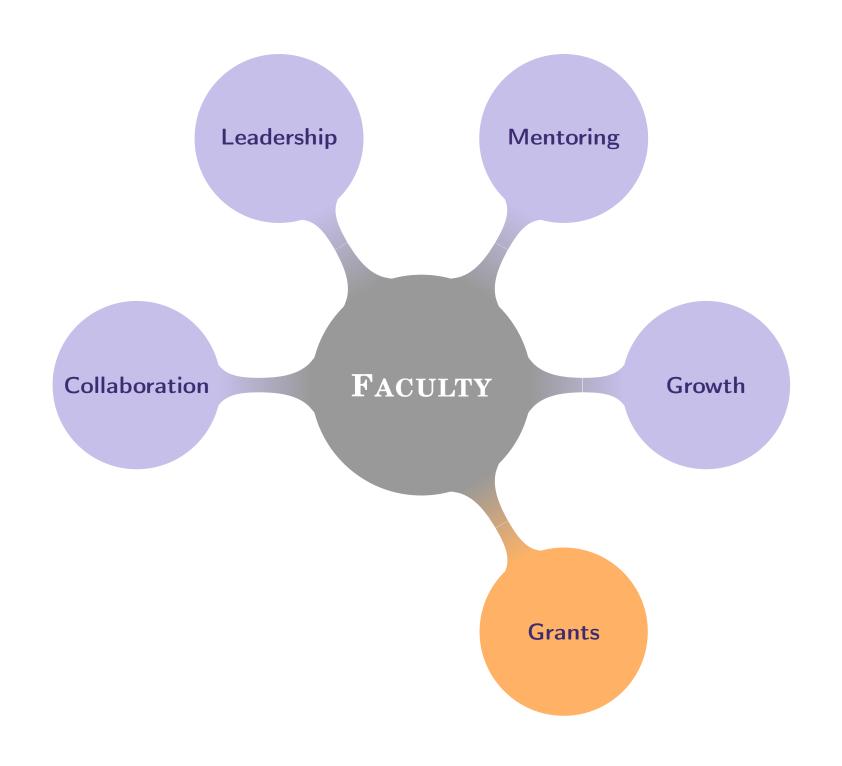
Leadership

Mentoring

Growth

Grants

Road to Success





 access to substantial internal and external funding sources to support the

pioneering collaborative research

Annual Australia-India grant, Australia-India Cyber and Critical Technology Partnership (AICCTP)





Opportunities for Research Students

Opportunities for Faculty Members

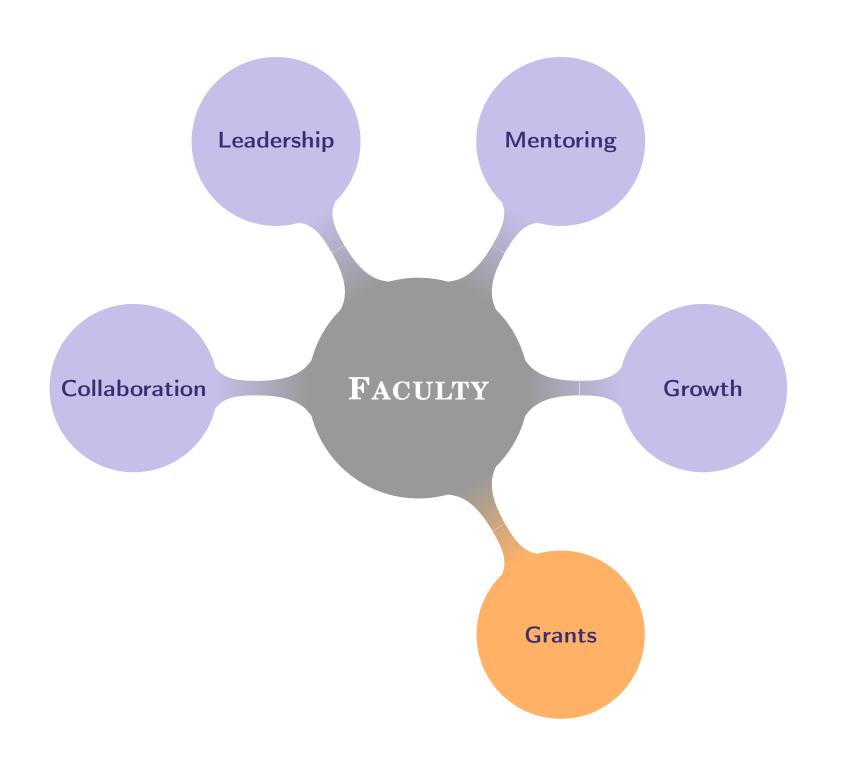
Collaboration

Leadership

Mentoring

Growth

Grants





- access to substantial internal and external funding sources to support the pioneering collaborative research
- Annual Australia-India grant, Australia-India Cyber and Critical Technology Partnership (AICCTP)
- India DST's Spark grant, etc.





Opportunities for Research Students

Opportunities for Faculty Members

Road to Success

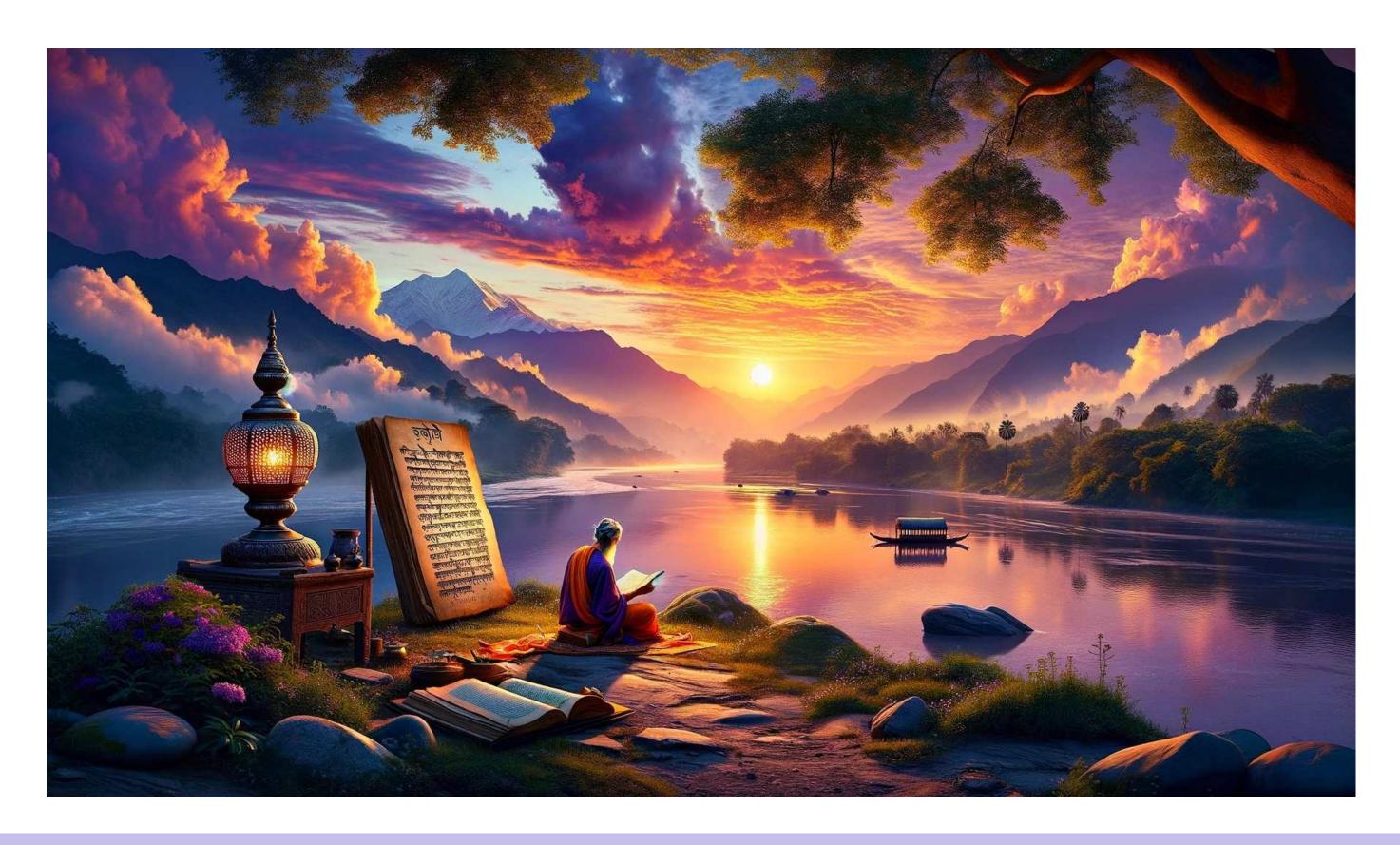




# **Enjoy the Journey**

Opportunities for Research Students

Opportunities for Faculty Members







# **Questions?**

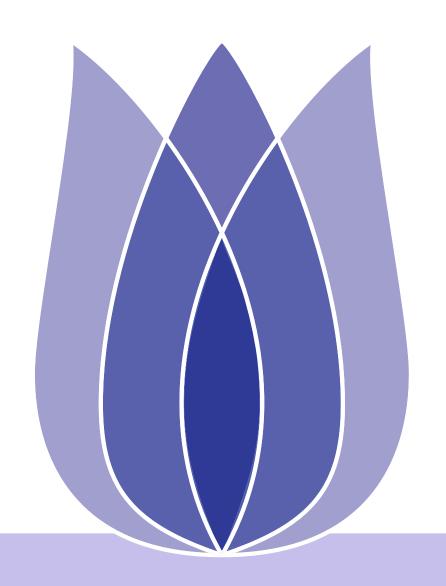
Opportunities for Research Students

Opportunities for Faculty Members





### **Contact Information**



Professor GANG LI
School of Information Technology
Deakin University
Burwood, Victoria 3125, Australia





GANGLI@DUCK.COM



OPEN RESOURCES FROM TULIP-LAB



TEAM FOR UNIVERSAL LEARNING AND INTELLIGENT PROCESSING, AUSTRALIA