Data Fusion Dynamics

A collaborative UK–Saudi initiative in cybersecurity and artificial intelligence

- Big data, artificial intelligence (AI), and cybersecurity are increasingly important areas of research.
- As big data use increases and AI gets smarter, better and more innovative cybersecurity methods are needed to protect us from cybercriminals in the online environment.
- Researchers from Cardiff Metropolitan University, King Abdulaziz University and King Abdullah University of Science and Technology have joined forces in a UK–Saudi Research Partnership to collaboratively approach the global challenges faced in this field.
- Through joint enterprise, the 'Data fusion dynamics: A collaborative UK–Saudi initiative in cybersecurity and artificial intelligence' hopes to shape the future of digital tech.

This is a game of cat and mouse which is increasingly high on the agenda of world leaders as cybersecurity organisations struggle to stay ahead.

Big data, artificial intelligence (AI), and cybersecurity are part of our daily lives now in ways we couldn't have imagined even five years ago. They meet our needs in plain sight and in the background, both at home and at work.

Bigger and better

Hospitals and healthcare providers can use big data analysis to predict patient health trends or admissions while retailers might use it to tailor your online shopping experience so that you get personalised recommendations (and spend more!). Farmers can apply weather system big data to predict conditions and plan planting and harvest, and airlines can now forecast aeroplane component failures before they happen, allowing mechanics to fix them in advance. AI is also helping both groups and individuals streamline processes and workflows or improve outcomes. Carrying out a search online? You'll now get an answer from AI at the top of the results page compiled from sources all over the internet. Like to play computer games? AI will be adapting the environment and your opponents based on your game play to give you the best time possible. In many instances, big data and AI work in tandem. Some banks, for example, use AI to analyse big data to detect fraud or even predict market trends.

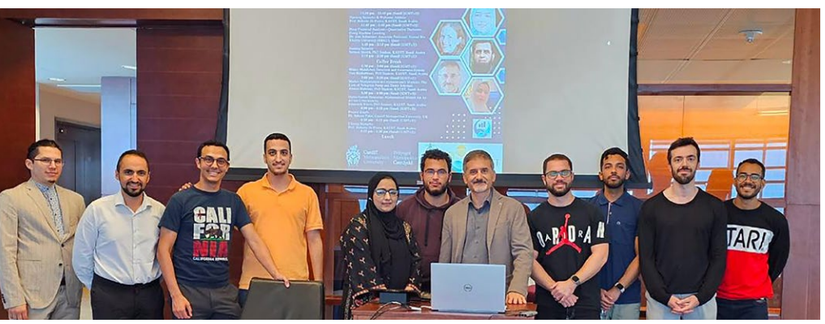
The cyber war

These relatively new digital environments are constantly under threat though, which is where cybersecurity comes into play. Healthcare providers, financial institutions, governments, and internet users like you need to know that their data is safe. The threat is massive; cybercriminals can bring an

UK–Saudi Challenge Fund 2024 British Council project partners.

Work by the Data Fusion Dynamics researchers is essential if we want to keep our data safe.

The project's research activities include joint research and collaborative publications.



international airport to a standstill, cause a political crisis with a data leak or clear your personal bank account in a few clicks. It has never been more important that cybersecurity is able to keep up with the ever more ingenious gangs and individuals looking to exploit the online world.

AI is a weapon used by both sides in this cyber warfare. Deep learning, machine learning, and natural language processing techniques are all getting better at the automated detection and prediction of cybercrimes. But while AI can be employed to protect data or detect threats and malware, it can also be used by criminals to carry out crimes faster and on a scale that has never been seen before. This is a game of cat and mouse which is increasingly high on the agenda of world leaders as cybersecurity organisations struggle to stay ahead of cyber threats.

The ambitious project is tackling critical global challenges, fostering innovation and strengthening academic and research partnerships to shape the future of digital technologies.

Data fusion dynamics

Luckily, important research and innovation is being carried out in this highly volatile field. An exciting new collaboration – 'Data Fusion Dynamics: A Collaborative UK–Saudi Initiative in Cybersecurity and Artificial Intelligence' – between the UK and Saudi Arabia has the aim of advancing big data, cybersecurity and AI. The ambitious project is tackling critical global challenges, fostering innovation and strengthening academic and research partnerships to shape the future of digital technologies. In this unique West to East partnership, academics from Cardiff Metropolitan University (UK), King Abdulaziz University (Saudi Arabia), and King Abdullah University of Science and Technology (Saudi Arabia) have acknowledged the significance of addressing challenges and opportunities in these domains through global collaboration.

Led by Dr Sabeen Tahir, a team of researchers — Dr Fiona Carroll, Dr Sheikh Tahir Bakhsh, Dr Reem Alotaibi, Dr Linda Mohaisen, and Dr Roberto Di Pietro — are launching a Research Exchange Programme to foster collaboration, drive innovation, and harness the expertise of researchers from institutions across Saudi Arabia. This initiative aims to break disciplinary barriers, encourage the exchange of cutting-edge ideas, and strengthen international research partnerships.
The project's research activities include joint research supervision, collaborative publications, joint workshops and training sessions, and research skills development workshops to create a robust environment that supports high-quality research. The formation of this UK–Saudi Research Partnership stems from a joint recognition of the transformative potential within the specified fields.

Funded by the British Council, work like that being done by the Data Fusion Dynamics researchers is essential if we want to keep our data safe. Fighting the threat from cybercriminals is like tackling the mythical Hydra – as soon as you cut off one head, two more grow in its place. Only through clever collaboration and the sharing of ideas it might be possible to keep pace with the newer and smarter cyber threats that face us every day.

Personal response

Could you tell us more about the specific research being undertaken by the researchers on the Data Fusion Dynamics project?

The **UK–Saudi Challenge Fund 2024 BC project** represents a significant international collaboration between the UK and Saudi Arabia, bringing together expertise in cybersecurity, AI, and data analytics. Researchers in this initiative are addressing some of the most pressing challenges in these fields by exploring innovative solutions for secure and efficient data management. One of the key research studies under this project focuses on the impact of mobility on wireless communication systems, particularly in dynamic environments such as defence operations. This research assesses optimal configurations for Long Range Wide Area Network efficiency by analysing variables such as mobility models, transmission intervals, altitude, and speed. The insights are particularly valuable for real-time health monitoring systems in military settings, ensuring reliable communication for medical interventions and emergency responses. Future studies aim to investigate more complex mobility patterns and environmental influences to further strengthen system resilience. Another researcher in the initiative has conducted an in-depth study on the role of **Emotional User Interfaces in cybersecurity awareness**. With cyber threats becoming increasingly sophisticated, understanding human factors in online security is crucial. This study analysed emotional responses to 25 different web interfaces through a survey of 1,922 participants from the UK and the US.

Why do you think UK and Saudi Arabian institutions make such a strong partnership to tackle the challenges in this field?

The partnership between UK and Saudi Arabian institutions offers a unique advantage in tackling cybersecurity challenges due to the complementary strengths of both nations. The UK has a long-standing reputation for pioneering cybersecurity research, regulatory frameworks, and industry best practices. Saudi Arabia, on the other hand, has been making rapid advancements in AI-driven security solutions and national cybersecurity infrastructure. This synergy enables the collaborative development of cutting-edge technologies that address both regional and global cybersecurity concerns. The establishment of joint PhD supervision programmes, such as those within the UK–Saudi Challenge Fund 2024 BC project, further strengthens this partnership by fostering academic exchange and innovation.

Do you think it's possible for cybersecurity to stay ahead of the cybercriminals?

The ever-evolving nature of cyber threats poses an ongoing challenge for cybersecurity professionals. While technological advancements such as AI-driven threat detection, quantum encryption, and behavioural analytics have significantly improved defence mechanisms, cybercriminals continue to adapt their tactics. A proactive approach is required — one that integrates real-time threat intelligence, user education, and ethical AI deployment. By leveraging interdisciplinary research and fostering international collaboration, cybersecurity can maintain an edge over emerging threats. However, achieving complete dominance over cybercriminals remains a continuous battle, requiring constant vigilance and innovation.

What does the future hold for Data Fusion Dynamics in terms of research and innovation?

Looking ahead, the **project** aims to expand its research scope, focusing on enhancing cybersecurity resilience through **machine learning-based threat detection, decentralised data security frameworks, and adaptive encryption methods**. Additionally, efforts will be directed towards developing **more sophisticated mobility models for IoT networks, particularly in high-risk environments such as healthcare, financial, defence, and critical infrastructure protection**.
To promote knowledge exchange and industry–academic collaboration, over the past year we have successfully organised six on-campus research seminars at Cardiff Metropolitan University, King Abdullah University, and King Abdulaziz University, featuring insightful guest lectures. We have successfully established a collaborative partnership between the three universities, fostering academic exchange and research innovation. As part of this collaboration, we have launched a joint PhD supervision programme and commenced the supervision of two PhD students. These initiatives foster dialogue among researchers, policymakers, and industry experts, ensuring that our findings translate into practical applications. As part of our research dissemination efforts, we have successfully published **three conference papers and one Q1 journal paper**, demonstrating the impact and quality of our work. These publications contribute to the broader academic and professional cybersecurity community, providing valuable insights and advancing knowledge in the field. The future of the project is poised for groundbreaking innovations, reinforcing the commitment of UK–Saudi partnerships to advancing cybersecurity and data intelligence for a safer digital world.

Details

Dr Sabeen Tahir

Dr Fiona Carrol

Prof Roberto

Dr Sheikh Tahir

Dr Linda Mohaisen

Dr Reem Alotaibi

e: stahir@cardiffmet.ac.uk
w: www.cardiffmet.ac.uk/technologies/staff-profiles/Pages/Sabeen-Tahir.aspx
www.linkedin.com/in/dr-sabeen-tahir-262b57185/
scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Sabeen+Tahir&btnG=&oq=sabeen+

Funding

This project, *Data Fusion Dynamics: A Collaborative UK–Saudi Initiative in Cybersecurity and Artificial Intelligence*, has been made possible with funding support from the British Council. We extend our gratitude to the British Council for their generous support. This collaboration brings together Cardiff Metropolitan University, King Abdulaziz University, and King Abdullah University of Science and Technology to advance innovation in cybersecurity and artificial intelligence.

Collaborators

Cardiff Metropolitan University, King Abdulaziz University Saudi Arabia, King Abdullah University of Science and Technology Saudi Arabia.

Bio

Dr Sabeen Tahir, Project Lead, Senior Lecturer at Cardiff School of Technologies, Cardiff Metropolitan University, UK.
Dr Sabeen is an experienced Higher Education professional with 15 years of teaching experience in undergraduate and postgraduate programmes. She played a key role in supervising postgraduate students and is an active researcher. Her research interests lie predominantly in wireless networks, cybersecurity, cloud computing, blockchain, and the internet of things.

Funded by
BRITISH COUNCIL
Cardiff Metropolitan University
Prifysgol Metropolitan Caerdydd
KAUST