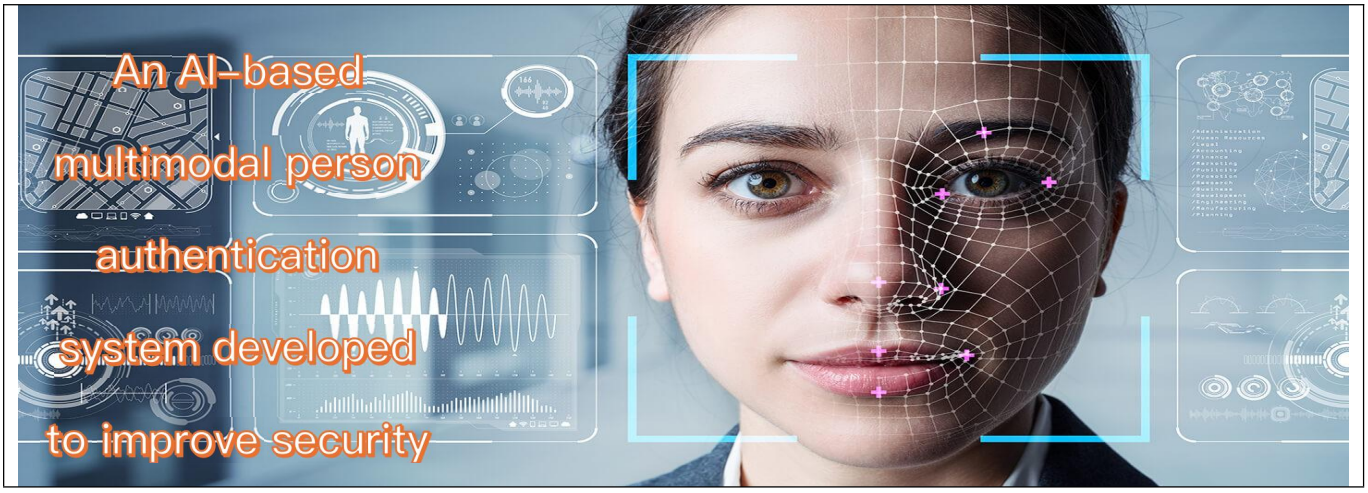
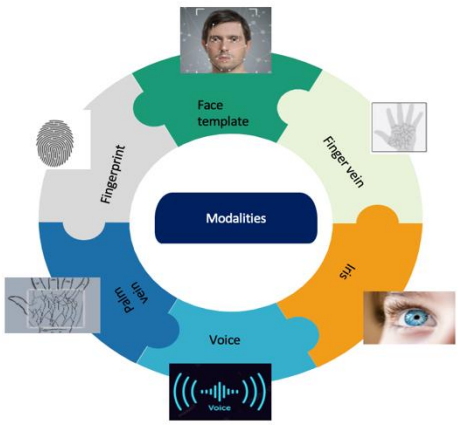


To meet the requirement of data and network security of an organisation having remotely located employees, Nexucon developed a unique multi-modal person authentication system based on AI and machine learning. It also ensures attendance and accountability on the part of the employees and helps to track a remote worker's readiness and alertness level.



Multimodal Biometrics

Multimodal biometric authentication refers to a security approach that combines two or more biometric characteristics such as fingerprints, facial features, iris patterns, voiceprints, or behavioural characteristics (like typing rhythm) for identity verification. At times of the unfortunate COVID-19 pandemic, as part of government policy corporate workers started working remotely. The trend of people working remotely has been on the rise since those times and many corporates have accepted it as part of their normal norms.

With remote work becoming more prevalent, ensuring secure access to sensitive data and server systems and also company's private network is crucial. The usual practice to login in to company's server involves authentication with passwords and keys. However, in case of password or key compromise, there is high risk of

unauthorized people getting access to the system. There could also be a risk of proxies securing access to the system in place of the actual employees. Most organizations, otherwise, have strict regulatory requirements regarding data security and access control. Nexucon's unique solution helps to provide such organizations with a secure employee login system so as to comply with these regulations. In addition to that, our system provides insights from the login data about readiness and alertness level even in remote work settings.

Nexucon combines the strength of face recognition and voice recognition along with measures to counter spoofing attempts to add an additional layer of security for the company's data and network systems. In particular, we create a multimodal deep learning architecture to develop the system.

Overview:

Client: IT & ITeS Companies, Academic Organisations, Utility & Manufacturing Companies, Security Companies

Region: India, Singapore, Malaysia, UK

Industry: Utility , Manufacturing, Education, Security, IT & ITeS

Client challenge: Clients were searching for remote login to company's network with improved data security and secured authorization. Also, it gets difficult to ascertain the readiness and alertness levels of its employees..

Solution: Our multimodal biometric system helps to ensure secure access and it goes much beyond that to provide valuable insights into the employee's behavioural patterns and composure throughout the day. The system can continue to provide access and security even if some of the modalities fail. In that case, just one modality for authentication may be used subject to prior settings.

Benefits:

- High levels of authentication accuracy are achieved by Nexucon's multimodal biometric authentication, which incorporates several biometric identification technologies, such as face and voice recognition, and is user-friendly (*3).
- Duplicate and proxy attempts for access were eliminated with the use of Nexucon's multimodal authentication system.
- By combining the outcomes of voice, and facial recognition, Nexucon's developed system allows for

authentication with negligible false acceptance rate.

Building a customized solution:

Throughout the world, Nexucon has deployed several biometric authentication systems in different nations and areas. These systems' exceptional precision, user-friendliness, and security make them suitable for dependable deployment as a crucial component of the social infrastructure that upholds the security and safety of day-to-day activities, from business applications to leisure and pleasure.

We present a multimodal biometric approach in this work that integrates voice biometric and face biometry modalities. For the multimodal biometric approach, we provide a state-of-the art end-to-end deep learning model.

Increasing the usefulness of multimodal biometrics:

When implementing multimodal authentication, an organization's present tech stack must be integrated with and a number of variables, including security requirements, must be evaluated. Nexucon considered different important factors like, security considerations, backend infrastructure, and user enrolment procedures. Also, it includes the technical complexity of integrating several modalities as well as concerns about standards, interoperability, scalability, and cost.

Nexucon's Multimodal authentication system can be used by financial services companies to protect transactions, lower fraud, and improve client satisfaction. Tighter security measures streamline procedures and enhance patient privacy and identification accuracy in the healthcare industry.

With the successful completion of this initiative, Nexucon is now at the forefront of industry innovation. The business will keep refining the method by which it assists clients internationally as the service is expanded globally.