

**PROPOSAL FOR शोध SUPPORT FOR STUDENTS**

*(Under the SHODH program for research)*

1. **SUMMARY SHEET:**

**Project proposal submitted under (tick mark the शोध scheme)**

**□ RISE (Research & Innovation for Science and Engineering)**

* **RISoCS (Research & Innovation for Students of Computer Science)**

**□ RISoM (Research & Innovation for Students of Management)**

**□ RISoL (Research & Innovation for Students of Law)**

**□ RISoD (Research & Innovation for Students of Design)**

**□ RISoHS (Research & Innovation for Students of School Health Sciences and Technology)**

**□ RISoMM (Research & Innovation for Students of School for Modern Media)**

**□ RISoLS (Research & Innovation for Students of School for Liberal Studies)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. Title: Strand: Synthetic Cybersecurity DNA | | | | **OFFICE PURPOSE**  DATE RECEIVED (in R&D Office):  PROPOSAL No. |
|  | Duration  (Months)  10 | | Amount |
| 2. Name and Department of applicants with contact details (email and phone): | | | |
| \*Applicant(s) (Name/Course/Department/SAP ID) & Signature | | Mentor(s) (Name/Department) & Signature | | |
| 1. Sonali Bhadra | B. Tech CSE | | | Dr. Akashdeep Bhardwaj | | |
| 1. Piyush Kumar | B. Tech CSE | | | Dr. Akashdeep Bhardwaj | | |
| 1. Dhruv Tandon | B. Tech CSE | | | Dr. Akashdeep Bhardwaj | | |
| (iv) | |  | | |
| (v) | |  | | |

\* A SHODH team will have minimum 2 students and a maximum of 5 students. SHODH team can have a maximum of 2 mentors (For SoE, there is no limit on number of mentors)

# Do not put any identifying information in Section (B)

(**This page intentionally left blank**)

**(B) DETAILS OF PROPOSAL:**

|  |  |
| --- | --- |
|  | **OFFICE PURPOSE**  DATE RECEIVED (in R&D Office):  PROPOSAL No. |

|  |
| --- |
| 1. Title (Title should be concise & specific)   **Strand: Synthetic Cybersecurity DNA** |
| 1. Objectives of the proposal demonstrating contribution to excellence at national level (List pointwise) # 2. **Cybersecurity Resilience Improvement-**Develop a breakthrough cybersecurity framework based on synthetic DNA authentication to protect the national digital security ecosystem. 3. **Digitization of identity protection-**Digital DNAs be explored as a means of identity theft prevention and preventing unauthorised access. Developing a trustworthy national cybersecurity architecture. 4. **Advances in AI-Powered Threat Detection -** Employ artificial intelligence and machine learning to perform real-time behavioural triage and anomaly detection to address new threats in cyberspace. 5. **Security, Scalability, and Adaptability -** Secure, scalable, and adaptive authentication scheme for government, defence and critical infrastructure applications needed. 6. **Innovation in Behavioural Cybersecurity -** Develop new methods integrating synthetic DNA and behavioural biometrics to establish new national benchmarks for cybersecurity researchers. 7. **To support national digital transformation -** Bring a cutting-edge security framework to banking, e-governance and smart city programs. 8. **Public and private sector security hardening -** Design a large, flexible cybersecurity environment that can be utilized by public intelligence bodies, banks and enterprise organisations. 9. **Encouraging Research and Development -** Encourage cybersecurity research in the indigenous space so as to facilitate innovation and technology development which are in sync with national requirements. 10. **Cybersecurity Policymaking Support -** Offer practical recommendations and ideas to policymakers in order to enhance better cybersecurity laws and policy. |
| 1. Expected deliverables of the Proposal (Products/Publications/Patents/ New concept/Spinoff etc.) #   **Products**   * A fully functional **Digital DNA-based authentication system** for secure identity verification. * **AI-driven behavioral cybersecurity framework** for real-time anomaly detection.   **Publications**   * Research papers in **high-impact cybersecurity and AI journals/conferences**. * Whitepapers on **synthetic DNA-based authentication and behavioural cybersecurity**.   **Patents**   * **Digital DNA** authentication model. * AI-based **behavioural anomaly** detection techniques.   **New Concepts**   * Introduction of the **Synthetic Cyber Security DNA** as a new type of Authentication Technique. * Development of a **Behavioural Diffusion** of Digital DNA Security.   **Spinoffs & Commercialization**   * **Potential** for a **new startup** or industry to collaborate on real world deployment. * **Licensing opportunities** have been made available for government agencies, defense entities and financial institutions.   **Contributions to National Cybersecurity Frameworks**   * Recommendations for **national security policies**. * Providing insights for **cybersecurity regulations and best practices**. |
| 1. Importance/highlights (3-5 bullet points) # 2. **Next-Generation Cybersecurity** - Introduces a synthetic DNA based authentication mechanism which expands the security offered significantly beyond the traditional password and biometrics. 3. **AI-Driven Threat Detection** - AI technologies that are able to perform threat detection uses machine learning and behavioral analytics for performing real time anomaly detection and to adapt the security level over time. 4. **Continuous Behavioral Monitoring** - limits the current user to real-time analysis of their behavior patterns, showing anomaly detection as well as showing prevention of cyber-attacks in real-time. 5. **Scalable and Versatile** - Applicable Across Government, Defense, Banking and critical infrastructure for national cybersecurity enhancement. |
| 1. Literature Review and advancement: Demonstrate knowledge of (with references (IEEE format) and contribution to the national state-of-the-art in the relevant area#   Cybersecurity threats and requirements continue to develop rapidly, thus demanding highly sophisticated security mechanisms beyond conventional authentication methods. Recently conducted studies in biometric security, behavioral analytics, and artificial DNA encoding have formed the base for the new approach being proposed by STRAND.    1. Conventional Authentication and Its Pitfalls    Conventional authentication modes that either included passwords or two-factor authentication (2FA) all had one thing in common, i.e., they suffered exploitation by phishing, brute force attacks, or credential leak. Research work in biometric authentication, such as fingerprints and facial recognition, claims improved security. However, they are still vulnerable to spoofing attacks and privacy concerns.    2. Behavioral Biometrics in Cybersecurity    Keeptroke dynamics and mouse movement analysis fall into the signature of behavioral biometrics and have brought some part of continuous authentication to the scene with greater reductions of risk in unauthorized access. Studies have indicated the successful performance of machine learning models to detect anomalies for real-time security monitoring. Still, the research looks into incorporating behavioral biometrics with a DNA-based synthetic-security model.    3. Synthetic DNA for Secure Data Encoding    DNA computing and data storage have proven capacity to store high-density and very long longevity of data. Synthetic DNA cryptography research promises its usage in hypersecure authentication based on bio-inspired sequence encoding of digital information [4]. STRAND extends this by embedding unique cybersecurity attributes into synthetic DNA to provide a unique identifier for users.    Advancement Over Existing Solutions    STRAND has introduced Synthetic DNA-Based Authentication, which goes beyond biometrics and conventional cryptography to secure enhancement. Thus, it contributes to the true national state of the art in the cybersecurity framework. |
| 1. Alignment to School specific priorities (State specifically the expected impacts at Cluster and School levels)#   It resonates with the School of Computer Science (SoCS) and its priorities in terms of research and innovation, as well as enhancement of national cybersecurity. The expected impacts at the Cluster and School levels are as follows.    Cluster Level Impact (Cybersecurity & AI Cluster)    Advancement of Cybersecurity Research: Fortifies and also advances the school's position as a leader in cybersecurity innovation through training and work on behavioral analysis and synthetic DNA authentication.    Integrative AI & Blockchain: Leverages knowledge in the AI way of mechanisms for security, with an additional focus on blockchain for integrity in authentication, thus supporting ongoing research under the cybersecurity and AI header.    Industry Partnerships: Opens avenues for partnerships with government, defense, and private cybersecurity organizations for application in the real world and avenues for funding.    Student & Faculty Development- Hands-on practical experience in cyber security, AI, and blockchain, with benefits to the students and researchers in the cluster.    National & International Recognition- Position as a center of excellence in cybersecurity, including high-impact publications, patents, and participation in global security forums.    Impact at School Level (School of Computer Science, UPES)    Enabling Cutting-edge Curriculum- Infusing some of the top-notch techniques in cybersecurity into academic curriculum thus creating an environment for innovational education.    Proliferation of Research Outputs- This possible development would include many high-impact publications and patents that would indeed make the research visibility of the school more of a coverage factor.    Developing Industry-Based Skills: Improve employability through imparting practical learning to students training them in cyber security, AI, and blockchain. |
| 1. Methodology#   The implementation of Strand follows a structured methodology to validate its effectiveness in cybersecurity applications. The methodology is divided into the following key stages:   1. Data Collection and Encoding   Behavioral Attribute Capture: Behavioral characteristics with each user, including typing speed, mouse movements, and interaction logs, are recorded.  Synthetic DNA Encoding: These behavioral characteristics are stored in a discriminative synthetic DNA sequence, i.e., they provide a unique digital identity achieving the highest information security and unique traits.  Data Preprocessing: The acquired data is noise reduced and normalized in order to increase authentication accuracy.   1. Experimental Setup and Implementation   Prototype Development: A prototype working STRAND is constructed by combining synthetic DNA based authentication and anomaly detection systems.  AI-Driven Behavioral Analysis: Machine learning models are used to continuously interact with user behavioin, increasing the accuracy of authentication.  Blockchain Integration: A tamper-proof record-keeping system, built on a blockchain, is integrated into the system for data integrity purposes.   1. Performance Evaluation   Authentication Accuracy Testing: The system is tested through an extensive analysis to quantify the performance of synthetic DNA-based authentication.  Security Resilience Assessment: The system is tested against cyber threats such as phishing, brute force attacks, and behavioral spoofing to assess its resilience.  Comparative Analysis: STRAND's effectiveness and security are contrasted with common authentication techniques to demonstrate its effectiveness.   1. Security and Threat Analysis   Penetration Testing: The security systems are subjected to penetration testing in order to discover the potential vulnerabilities and to strenghten security.  Data Encryption Mechanisms: Cipher techniques are applied to encrypt the stored synthetic DNA sequence and authentication information.  Threat Mitigation Strategies: Real-time measures of threat detection and mitigation are taken to counter security intrusions.   1. Results and Discussion   Evaluation of Digital DNA Authentication: The effectiveness of synthetic DNA-based authentication to deter unauthorized access is discussed.  Impact on Cybersecurity Enhancement: Consider the contribution of STRAND's continuous behavioral monitoring to the enhancement of cybersecurity is evaluated.  User Experience and Adaptability: Usability and versatility of the system for different applications such as government and finance industries are discussed.   1. Conclusion and Future Work   Key Findings Summary: Contributions made by STRAND to cybersecurity are summarized with the key results and takeaways.  Future Improvements: Potential enhancements, such as integrating additional biometric factors and refining AI models, are suggested.  Real-World Deployment Strategies: The uses of STRAND in the real world (i.e., collaborations with industry and government) are described. The STRAND implementation adopts a methodical approach to assure its proper use for cybersecurity applications. |
| 1. Gantt chart of the activities# |
| 1. Budget with justification:  |  |  |  |  | | --- | --- | --- | --- | | **Proposed expenditure** | Quantity | Value | **Total** | | **OPEX Items** | | | | | Consumables |  |  |  | | Characterization |  |  |  | | Any Other (Please specify) |  |  |  | | **CAPEX Items** | | | | | Equipment |  |  |  | | **Total Budget** |  |  |  |   Justification item wise: |
| 1. Additional information (as per requirement) |

Note: 1) Please attach one-page CVs of Mentors.

**#**If required, annexures may be used for items 2-8.