Project proposal submission to C3iHub:

‘Vulnerability discovery and liveness detection for improving the security in biometric authentication systems’

**1. Project title:** Vulnerability discovery and liveness detection for improving the security in biometric authentication systems

**2.** **Name of PI:**   
 Dr. Tushar Sandhan  
 Assistant Professor, Electrical Engineering,  
 IIT Kanpur

**3. Type of Proposal:** 3 years

**4. Executive summary:**

The spoofing or presentation attacks on identity authentication systems have become a major concern for the cyber physical systems. Biometric authentication systems such as fingerprint recognition, face and iris recognition are used in multitudes of applications including finance, KYC authentication, Indian UID, passport verification and in numerous security systems. Recently it has been revealed that fingerprint based UID aadhaar verification has been misused or easily forged by intruder for stealing ration distributed at various government centres in villages. It has also been spoofed for mobile SIM card distributions. To increase the security of these cyber authentication systems, the most important criteria is to detect the liveness of the input data. That means checking whether the biometric data which is being captured is coming from actually live person or not.

Extra security is provided by combining the identity authentication software with a liveness detection system, which may be implemented in hardware or software. Here we are proposing hardware and ML algorithm software based combined robust anti-spoofing system. We will design the hardware considering variables like type of illumination source, its optimal wavelength, condenser, lens focusing element to acquire sub-epithelial layer details of the finger skin. Investigation will also be conducted for optimal imaging device assembly arrangement, automatic illumination control and security level adjustment. After imaging the appropriate finger patterns, the distinguishable features for live vs spoof input data need to be extracted. As state-of-the-art anti-spoofing methods use deep learning-based ML models, we propose to design novel CNN, ML models to improve upon their performance keeping latency within acceptable limit for real time performance. In the process we will also review in detail about all kinds of spoofing attacks, their severity thereby discovering the vulnerability of biometric security systems. The overall research focuses on design and development of hardware, ML algorithm for CNN based classification of the acquired data for spoofing detection and thereby improving the security of cyber physical identity authentication systems.

The proposed study's main innovation is the creation of a task-specific, efficient hardware module that can be easily retrofitted into existing authentication scanners. The innovation then lies in creating a highly secure identity authenticating cyber physical system that is resistant to presentation and spoofing attacks using a scalable AI based intelligent system.

Deliverables clearly include designed hardware and workable product and accompanying AI based software for liveness detection and vulnerability discovery in the biometric identity authentication systems. We plan to file minimum 2 patents (hardware design and ML software), 3 international conference and journal publications. Along with hardware and programming codes we will also deliver the vast amount of live and spoof dataset that will be captured over the investigation period for further research and validation of new AI models.

POC of the final product including GUI will be presented to UIDAI for aadhaar biometric security improvement and collaboration will be sought after from the Indian industries like Actatek, Pentagon engineers, Dheeram Innovations, Signzy, SecurAX and Matrix Comsec which work in biometric authentication but yet to produce security solution of liveness detection and anti-spoofing for identity authentication cyber physical systems.

**5. Proposal Body:**

**a.** **Origin of the proposal**

Biometric authentication systems like fingerprint, face and iris recognition become ubiquitous in all types of smart phones, SIM card verification, government grocery ration distribution, inside airports and even as an attendance system in schools [1]. Face, iris, fingerprint, palm, veins, ear pattern, gait etc. are the types of different biometric modes. Unimodal biometric means the authentication system based solely on one type of biometric mode. These unimodal systems completely rely on the perfect working of that biometric mode. However, there is high probability of failure of the single biometric mode or damaged or insufficient input data. For example, performance (True Accept Rate: TAR) of the fingerprint-based authentication system degrades when the user’s finger is wet due to water, oil or sweat etc. Simply the environment changes like cold conditions make fingers very dry, sometimes finger skin get damaged due to physical work and thereby causing problems in fingerprint recognition. These issues increase the false reject rate (FRR). High FRR causes inconvenience for user authentication and hinders its practical public usage. Thus, to alleviate these problems the biometric authentication systems are designed in a broader sense in order to incorporate all fingerprint quality variations. That also makes it easier to intrude or spoof the authentication system by unauthorized user. Nowadays spoofing or presentation attacks on identity authentication systems have become a major concern in cyber physical systems.

Aadhaar based biometric authentication (Unique Identification: UID) is being used in India for variety of purposes, including ITR filing, SIM registration, financial services and KYC compliances. There have been numerous cases where UID is being stolen due to fake or spoofed fingerprints created by fraudsters. In later 2017, UP police busted aadhaar racket which was using fake fingerprints made via polymer resin [2]. Fingerprints were cloned to perform online bank fraud in June, 2021, via printing the stolen fingerprints on butter paper, then obtaining the inverted pattern via light-sensitive photopolymer and casting the finger pattern on usual office rubber stamp. That spoofing attempts accuracy of successful intrusion reported whopping 70% [3]. Hacking of personal accounts via fake fingerprints have been reported in Hyderabad up recently in June 2022 by Times of India [4]. Thus security of cyber physical systems are getting compromised as they inevitably use identity authentication as one of their primary modules. Discoveries of these kinds of vulnerabilities and efficient artificial intelligence based anti-spoofing mechanisms are highly necessary for improving the security in biometric authentication systems. It is important to detect whether the fingerprint being captured is coming from actual live person or not; that is liveness detection of the biometric data. So we are proposing to investigate and design a new modular hardware which can be plugged in the existing systems, analyse the various types of spoofing attacks and develop ML algorithm based liveness detection system for improving the cyber security.

**b. Formulation of the problem in scientific terms**

This project will investigate all possible spoofing attacks over fingerprint identity authentication system, analyse spoofing images for finding peculiar patterns and signals indicating their non-liveness nature. Then investigation will develop imaging hardware including specific illuminating source for fingerprint imaging which can amplify non-liveness patterns. On the algorithmic forefront, AI based robust risk score prediction model for vulnerability discovery and machine learning (convolutional neural networks-CNN) based anti-spoofing computational framework will be developed. It includes predicting the vulnerability scores, confidence scores for liveness, hardware module and GUI based user interaction module.

Consider the biometric image data obtained via fingerprint scanner be having inside LEDs for illumination given as and the reflectance of finger patterns of ridges and valleys be given as where are spatial coordinates of the image pixel. Illumination is further decomposed into – lumens per lamp (lumen), – coefficient of utilization, – area per lamp (meter square), – loss factor of the light and which are related as,

, and image formation model as

It gives us the control over and we propose to exploit that by designing the appropriate light source hardware having specific frequencies of illumination, intensity and micro-lens assembly inside the existing biometric scanner. Wavelength of the illuminating source also plays a vital role in terms of emphasizing specific patterns in the image , this can be observed from the monochrome camera without any optical filters which produces enhanced vision at night if infrared is being used as the illuminating source. Thus, varying the frequency or using multiple LEDs with rotary mechanism will device a way to capture hidden patterns of the finger which otherwise will be invisible to current biometric scanning system. For finding the optimal wavelength or combination of wavelengths for detecting presence of various spoofing materials, a vast number of experiments, frequency sweeping and image capturing need to be performed. These detailed experiments for modular compact hardware design which can be incorporated in the existing fingerprint scanners are the part of proposed project.

The reflectance is dependent on the type of material e.g. actual live finger skin, glue casts, gelatin flexible mould, rubber stamp, electrically charged ink over normal paper, acetic paper sheet etc. Equation (1) can be considered in the additive terms as Thus the captured image will contain the micro scale properties of the reflecting material which includes live as well as spoofing or presentation attacks. The minute variations are like a noise and unobservable via naked eyes but computationally these patterns can be detected. First we will investigate the images and their characteristics for all possible types of spoofing attacks and then by incorporating AI we will distinguish between them. New ML model architecture need to be developed to solve this problem and then we will train these newly developed ML models (convolutional neural networks – CNN) for predicting the vulnerability scores and confidence scores for liveness detection.

**c. Novelty of the proposed work**

Main novelty of the proposed investigation is in the design of the task specific efficient hardware module which is flexible enough to be installed on existing biometric authentication scanners. Then novelty is in the development of scalable AI based intelligent system for making the identity authenticating cyber physical systems highly secure over presentation and spoofing attacks. Existing AI models are not sufficient to handle critical intricacies of spoofing attacks. So the research and development of new AI/ML model for vulnerability discovery in these authentication systems, risk prediction and blocking the presentation or spoofing attacks via robust liveness detection is very essential. The system will be designed to achieve high performance (accurate blocking of spoofing attacks over 99% accuracy for print, charge ink prints and 98% accuracy for gelatin skin like materials, while maintaining low false reject rate – FRR of the valid live user) for targeted population i.e. subjects from India. Thus, the proposed investigation has the significant novelty for improving the security of cyber physical systems tailored for identity authentication with the help of AI. The main purpose of the project is to invent the complete product (hardware and AI/ML modules) for the real-world application.

**d. Significance of problem solution in current context**

**I. current status of R&D works at national level**

The demand for precise and convenient identification and authentication has prompted a massive global deployment of biometric systems. These advancements have been fuelled by a heightened public profile, significant gains in precision, the availability of a comprehensive product line, and declining costs for sensors, IP cameras, and software. With the onset of digital India mission and mass adoption of cyber technologies even by villagers in India, led to massive utilization of cyber physical systems and thereby need for their robust security. The Aadhaar biometric identification system consolidates the biometric and demographic information of over 1.3 billion Indian citizens [6]. It is the most comprehensive biometric identification system ever created and is linked to bank accounts, social security numbers, etc. Due to the dependence of governing structures on biometrics, it is necessary to develop a system for protecting assets that rely on biometrics for storage and authentication. Centrally over the clouds these identification systems combine various user information like a photograph and biographical documents (name, date, and vicinity of birth). This central information accessible via fingerprint authentication is a boon not only for access and travel (self-service kiosks and automated gates), but also for civil identification, eKYC systems, online user registration and authentication, and more. It is also essential for critical infrastructures such as border control, immigration and regulation enforcement, health and subsidies, population and voter registration. Failure to safeguard these fingerprints may also result in severe consequences. Up until recently June 2022, numerous cases of aadhaar based fingerprint forging and spoofing have been reported by news media [2, 3, 4]. These reports show that even simple glue based minor presentation attacks are sufficient to intrude aadhaar based biometric identity authentication systems. The Aadhaar process presents a warning to emphasise the security aspect of the biometric system in order to protect the privacy and security of millions of people's biometric characteristics [13].

Earlier work on fingerprint anti-spoofing using Ridgelet transform, haptic feedbacks [7] and ensemble classifiers was able to block doh and gummy spoofs of about 92% accuracy on limited (less than 200 testing) samples. As per the prior work reviews in [8], periodicity of sweat glands and sweat diffusion patterns were utilized for anti-spoofing in [9]. Latest survey paper [10] shows the deep learning based promising techniques for improving the effectiveness of anti-spoofing and can block the presentation attacks from eco flex, gelatine, latex, silgum and wood glue. However non-cooperative spoofing accuracy only reached upto 83% and increased till 90% with user’s cooperation (i.e. indirectly more inconvenience to user).

Indian start-ups like Matrix Comsec, SecurAX, Technowin Solutions and Dheeram Innovations provide fingerprint based biometric solutions for attendance, access control, RFID and payroll management. However, they do not tackle anti-spoofing issues. Signzy Pvt. Ltd. deals with digital contract management and forgery detection systems enabled by biometrics and aadhaar, but does not directly deal with liveness detection in those biometric systems.

**II. current state-of-the-art R&D at international level**

The dangers posed by fraudsters for cyber physical systems are significant. To spoof the fingerprints, they have access to advanced technology such as 25-micron resolution resin 3D printers and casting various flexible skin-like materials. Fingerprint spoof attacks (also known as PA - Presentation Attacks) have been carried out utilising imitations crafted from readily available materials such as glue, wax, plasticine, and silicone [12]. The first instance of fingerprint reader spoofing was reported by NETWORK computing in 1998 [11]. In recent decades, these attacks have been the subject of numerous tests, and the international community's interest in anti-spoofing has grown substantially. Since 2009, the LivDet - liveness detection competitions have been held every other year [12]. The proposed investigation also planned to take advantage of these competitions and their dataset to train initial ML models and discover various vulnerabilities, which in turn will help in development of final robust anti-spoofing system as output of the project.

For liveness detection, hardware-based methods acquire vital signs such as fingertip temperature, pulse, blood pressure, and pulse oximetry using hardware including semi-consensual printed circuit boards [15]. Because fingerprints are extremely susceptible to interference from the external environment, solely hardware-based detection methods are not suitable for use in harsh environments. In addition, other factors, such as breaks, stains and dryness on the fingers, can hinder the ability to identify liveness. On the basis of image processing, a software-based method is utilised to cut costs and improve performance. State of the art methods use deep learning methods for improving the accuracy of liveness detection. Using texture properties such as clarity, continuity, and ridge strength, it is possible to distinguish real fingerprints from imitations [14]. It also makes use of CNN with image scale equalization to obtain fixed dimensional latent space mapping. [16] proposed the square regression error technique for each receptive fields of the CNN layers, [17] used the residual block based light weight CNN called slim ResCNN, [18] proposed the two-tier method where fingerprint recognition and anti-spoofing tasks were solved simultaneously. Template probe convolutional neural network and additionally restricted Boltzmann machine (RBM) were used for liveness detection [19]. [20] proposed the universal material translator (UMT) for creating new spoof images from only fewer samples which translates the style of fake fingerprint image to the live one. Our investigation will thoroughly study these state-of-the-art deep learning methods for proposing new robust liveness detection algorithm.

It is a significant challenge for the industry to design a biometric system that protects against current and future spoof attacks. FindBiometrics reported that FPC a global identity management company designed T-shape sensor module for biometric cards which met the mastercard’s anti-spoofing specifications. Feitian is also in review for featuring FPC’s T-shape sensor in new biometric cards in Japan [5]. These sensors are not yet integrated to generic biometric fingerprint scanner which are used in massively in public cyber physical systems.

**e. Work plan:**

**I. Organization of work elements**

Robust liveness detection needs hardware as well as ML algorithm based fusion methods. So to discover vulnerabilities and liveness detection, we propose to take multistep investigation.

Step1: (Hardware design) – RGB imaging is ubiquitous in nature and easily available even on hand-held devices. But it can only visualize upper most part of the epithelial. Along with RGB, we propose to investigate the responsive frequency spectra for the illuminating sources for narrow band imaging (NBI), blue and narrow infrared wavelengths to visualize the underneath partial capillary structures up to 10 to 100 micrometres. Overview of the proposed hardware and software based combined system is shown in Fig.1. So the imaging hardware pipeline submodules and the frequency of illumination can be controlled (as given in equation (1)) to effectively image the different types of skin across variety of Indian population.

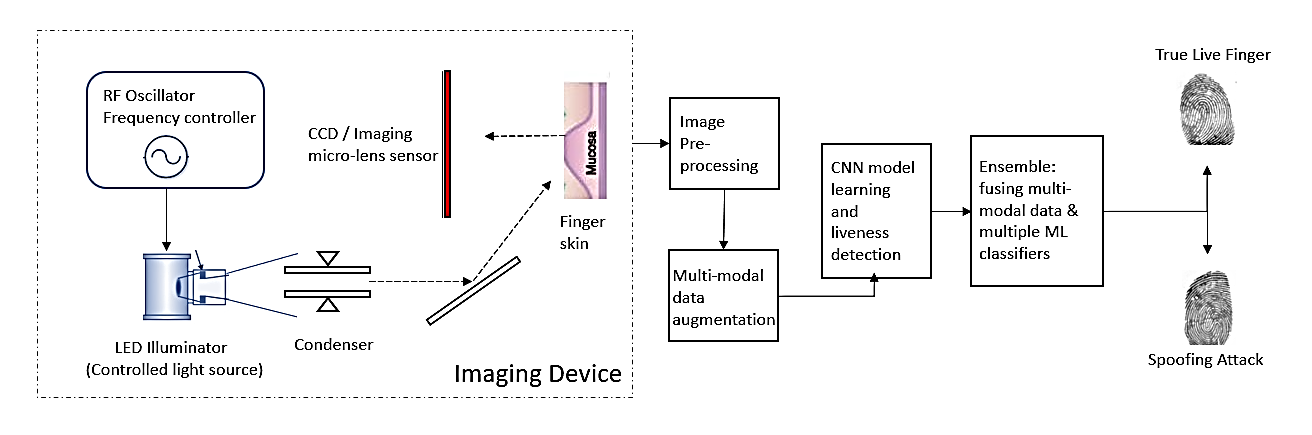


Fig. 1: Block diagram of the proposed investigation, which includes R&D for imaging device design and deep learning (ML) based algorithm for live vs spoof detection of the fingerprints.

Step2: (Efficient targeted data pre-processing) –The captured image data are pre-processed because that are usually contaminated with various artifacts like specular reflections, skin moisture lustures, apparatus noise, loss of details due to camera defocus, color saturation, occlusions due to skin cracks or mole, spurious allergic spots and contrast variations due to skin pigmentation. We will explore the state-of-the-art deep learning methods for these artifacts removal like multimodal image-to-image translation (MUNIT) [21], artifact disentanglement network [22] and diverse image-to-image translation (DRIT) [23]. For keeping the latency in check, the image optimization based methods like trilateral weighted sparse coding (TWSC) [24] for real-world image denoising will be incorporated.

Step3: (Training with limited data) – To handle the limited & imbalanced spoofing vs live data problem for training computationally heavy neural networks, a model-based framework from the medical domain for classifying global patterns [25] will be employed. It uses finite symmetric conditional Markov model in color space and the computed parameters of the Markov chain are treated as features. Then a hierarchical layered classification model using color, texture and sub-regions categories will be used for modelling the wide range of spoofing attacks. Then transfer-leaning based methods will be explored where the CNN will be trained on publicly available large dataset (LivDet competition datasets [10,11,12]). The newly acquired data will be amplified by the use of ML data augmentation methods. The multimodal data will be segmented using CNN models like HR-Net and U-Net for ROI extraction [26]. This ROI will then only be combined with Markov chain feature parameters. Final fused data will be used for vulnerability discovery and robust liveness detection.

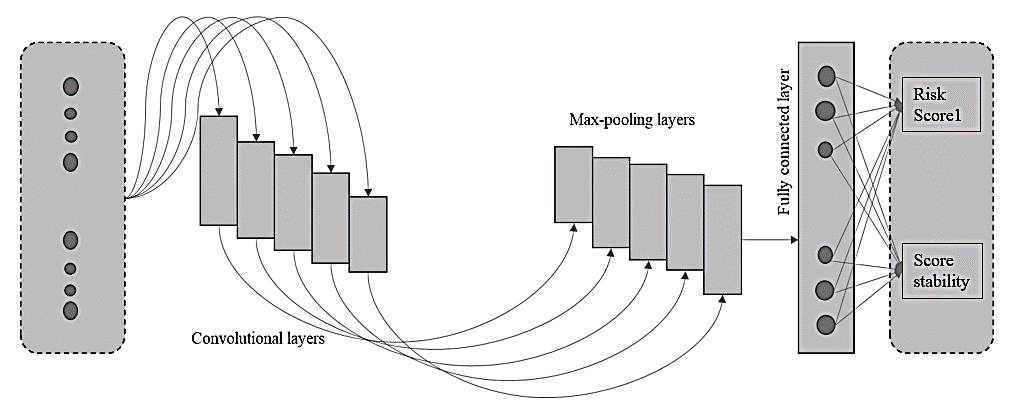


Fig. 2: Basic architecture of convolutional neural network (CNN) for vulnerability discovery (score stability) and liveness detection (risk score1) for identity authentication systems.

**II. Our evaluation metrics**

We will be considering comprehensive performance evaluation metrices for thorough evaluation of the proposed ML based framework. We include the below metrics:

* FRRLive: The rate at which the model misclassified the live fingerprints
* FRRFake:  The rate at which the model misclassified the fake fingerprints
* Average Classification Error (ACE): The average of the FRRLive and FRRFake rates
* Equal Error Rate (EER): The rate at which FRRLive and FRRFake are equal
* DET (Detection Error Tradeoff): Plot of the false rejection vs the false acceptance rates
* Accuracy: rate of correct classification of the live and fake fingerprints at a 0.5 threshold

**f. Schedule of activities, milestones and timeline via BAR diagram**

All 36 months detail activities and timelines are succinctly mentioned as below

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Milestones and Activities** | **Months for 3 years** | | | | | | | | | | | |
| **3** | **6** | **9** | **12** | **15** | **18** | **21** | **24** | **27** | **30** | **33** | **36** |
| A comprehensive study of various digital biometric parameters (skin types, dryness measure, moisture content and its response on fingerprint sensor) |  |  |  |  |  |  |  |  |  |  |  |  |
| Analysis of the public biometric live and spoof data and simultaneous collection of provided real world data – part I |  |  |  |  |  |  |  |  |  |  |  |  |
| Evaluation of AI models/methods for data pre-processing (finding principal features) |  |  |  |  |  |  |  |  |  |  |  |  |
| Design and R&D for imaging hardware, proposing new risk scores and liveness detection for fingerprint authentication |  |  |  |  |  |  |  |  |  |  |  |  |
| Latency and memory optimization of the AI/ML model |  |  |  |  |  |  |  |  |  |  |  |  |
| Improved real world data collection after incorporating new hardware – part II |  |  |  |  |  |  |  |  |  |  |  |  |
| Experimental setup for security analysis and privacy preservation in real world |  |  |  |  |  |  |  |  |  |  |  |  |
| Experimental setup configuration for the real time spoof detection and GUI display |  |  |  |  |  |  |  |  |  |  |  |  |
| IP generation, demonstration on real world anti-spoofing and validation |  |  |  |  |  |  |  |  |  |  |  |  |

**g. Summary of past works of PI justifying in tackling the proposed problem**

PI has worked in the industry for 7 years (Samsung Electronics HQ South Korea 2014~2021) where in last 3 years he has worked on multimodal biometric and anti-spoofing systems. He has also designed and developed the fingerprint security algorithms using multi-fusion of CNN networks. The invented methods were successfully commercialized for Samsung smart phones having inbuilt fingerprint scanners like Galaxy S series and Note series phones. Over the period he was inventor and co-inventor of the several patents for identity authentication in cyber physical systems as given below

* [Appl. No. US16/793567] (Country: USA) “Electronic apparatus for authenticating biometric information and operating method thereof”, 2020
* [Appl. No. 20759703.0] (Country: Europe region) “Biometric information operating method and device thereof”, Doc ID GM-201901-148-1-EP0, 2020
* [Appl. No. US16/975106] (Country: USA) “Method for performing authentication based on display”, Doc ID GM-201801-031-1-US0, Product classification PA010102, 2019
* [Appl. No. P20180022263] (Country: South Korea) “A method for fingerprint authentication and electronic device thereof”, Tech classification TA01011906, 2019
* [Appl. No. 18907245.7] (Country: Europe region) “Method for performing authentication according to display of object”, Doc ID GM-201801-031-1-EP0, 2019
* [Appl. No. P20180022275] (Country: South Korea) “Multiple camera multimodal system for biometric authentication”, Tech classification TA01011906, 2019
* [Appl. No. 19756969.2] (Country: Europe region) “Method of biometric authentication using plurality of camera with different field of view”, Doc ID GM-201801-030-1-EP0, 2019
* [Appl. No. P20180024891] (Country: South Korea) “Spoofing detection in biometric data for portable devices”, Doc ID 201712-009-1-KR1, Tech classification TA01011907, 2018
* [Appl. No. US16/268792] (Country: USA) “Method and apparatus with liveness verification”, IPC G06K-009/62, Registered No. US11023757, 2019
* [Appl. No. PCT/KR2018/015048] (Country: China) “Under display image sensor and fingerprint verification method”, Pub. No. WO2019124811, IPC G06F-021/32, 2018
* [Appl. No. US16/473899] (Country: USA) “Method and apparatus for processing of fingerprint image”, IPC G06T- 005/50, Registered No. US11093776, 2018
* [Appl. No. US16/477736] (Country: USA) “Electronic device for controlling the biometric data of fingerprints”, Doc ID GM-201609-032-1-US0, 2017

**h. Suggested plan of action for utilization of research outcome expected from the project**

The project will produce the workable prototype, an imaging system and computing device, which will show the input/output results via intuitively designed GUI. The proposed compact system can easily be installed or integrated with existing aadhaar based authentication modules. The project will help to establish strong academic and industrial collaboration as project mostly tailored towards product development. This partnership is very essential for collecting and analysing real-world biomedical data (across diverse population) for the robust AI model deployment for the anti-spoofing. The final product of anti-spoofing will be demonstrated with POC to UIDAI for the possible commercialization and improvement for the large-scale security improvement of aadhaar based authentication systems.

**i. How the solution is useful in cyber security practice and interested industries**

The proposal is solving the identity authentication problem in cyber physical systems by patching the loopholes of spoofing. The proposed liveness detection module is very essential for cyber security as variety of cyber transactions, systems, services rely on secured and genuine identity authentication protocols. The framework will increase the security of aadhaar based biometric authentication as well.

Interested industries in India would be: Actatek (founder W. Pamai), Pentagon engineers (founder S. Mudaliar), Dheeram Innovations (founder D. Pandi), Signzy, SecurAX (founder P Kotha, DN Belavadi, PG Reddy) and Matrix Comsec (founder G. Jeevni).

**j. References**

[1] D. Bhattacharyya, R. Ranjan, F. Alisherov, and C. Minkyu. Biometric authentication: A review. 2, 09 2009

[2] IT Next media news - sept 2017, https://www.itnext.in/article/2017/09/11/aadhaar-racket-using-fake-fingerprints-busted

[3] Biometric updates, June 2021, https://www.biometricupdate.com/202106/indian-police-nab-biometric-spoofing-gang

[4] Times of India, 2022, https://timesofindia.indiatimes.com/city/hyderabad/gang-clones-fingerprints-to-hack-a/cs-through-aadhaar-based-pay/articleshow/92269356.cms

[5] FPC T-shape sensor for anti-spoofing, https://findbiometrics.com/fpc-t-shape-meets-mastercard-biometric-anti-spoofing-specifications-501101/

[6] Unique Identification Autority of India (UIDAI), https://uidai.gov.in/en/, 2022   
[7] SB Nikam, S. Agarwal, "Fingerprint Anti-Spoofing Using Ridgelet Transform", IEEE International conf BTAS, 2008  
[8] Anita Kori et al., "Antispoofing Methods for Authenticating Live Users in Biometric System", Int. Journal of Sci and research, 2012  
[9] Javier Galbally, Julian Fierrez, and Javier OrtegaGarcia, Vulnerabilities in Biometric Systems: Attacks and Recent Advances in Liveness Detection, ATVS  
[10] D. Sharma and A. Selwal, "FinPAD: State-of-the-art of fingerprint presentation attack detection mechanisms, taxonomy and future perspectives", Pattern recognition letters, 2021  
[11] L Kavisankar et al., "Against Spoofing Attacks in Network Layer", 2016  
[12] LG David A.Y Valerio et al., "Review of the Fingerprint Liveness Detection (LivDet) competition series: 2009 to 2015  
[13] Mahesh Joshi, Bodhisatwa Mazumdar, Somnath Dey, "Security Vulnerabilities Against Fingerprint Biometric System", 2019  
[14] C. Yuan et al., "Fingerprint Liveness Detection Using an Improved CNN With Image Scale Equalization", IEEE access 2019  
[15] Bozhao Tan and Stephanie Schuckers, "A New Approach for Liveness Detection in Fingerprint Scanners Based on Valley Noise Analysis", Journal of electronic imaging  
[16] R.F. Nogueira, R.D.A. Lotufo, R.C. Machado, Fingerprint liveness detection using convolutional neural networks, IEEE Trans. Inf. Forensics Secur 2016  
[17] Y. Zhang, D. Shi, X. Zhan, D. Cao, K. Zhu, Z. Li, Slim-ResCNN : a deep residual convolutional neural network for fingerprint liveness detection, IEEE Access 2019.  
[18] M. Sajjad, et al., CNN-based anti-spoofing two-tier multi-factor authentication system muhammad, Pattern Recognit. Lett. 2018  
[19] D.M. Uliyan, S. Sadeghi, H.A. Jalab, Anti-spoofing method for fingerprint recognition using patch based deep learning machine, Eng. Sci. Technol. An Int. J. 2019  
[20] R. Gajawada, A. Popli, T. Chugh, A. Namboodiri, A.K. Jain, Universal material translator towards spoof fingerprint generalization, IEEE 2019  
[21] H. Liao, W. Lin, S. K. Zhou, and J. Luo. Adn: Artifact disentanglement network for unsupervised  
metal artifact reduction. IEEE Transactions on Medical Imaging, 2019  
[22] Xun Huang et al. “Multimodal unsupervised image-toimage translation”, In ECCV, 2018  
[23] Hsin-Ying Lee, Hung-Yu Tseng, Jia-Bin Huang, Maneesh Kumar Singh, and Ming-Hsuan Yang.  
Diverse imageto-image translation via disentangled representations. In ECCV, 2018  
[24] Jun Xu, Lei Zhang, and David Zhang. “A trilateral weighted sparse coding scheme for real-world image denoising”. ECCV, 2018.  
[25] A. Saez, C. Serrano, and B. Acha, “Model-based classification methods of global patterns in  
dermoscopic images,” IEEE TMI, vol. 33, pp. 1137–1147  
[26] Olaf Ronneberger, Philipp Fischer, Thomas Brox, “U-Net: Convolutional Networks for Biomedical Image Segmentation”, MICCAI, 2015.