Abstract:  
  
5G services have improved over 4G services in the following ways: higher data rates are specified, flexible network communications, support for very high traffic densities of Internet of Things devices, ultra reliability, and low latency. Authenticating a mobile subscriber or a sub-network with a main network in 5G mobile communications is an important criterion to check and minimize security threats and attacks. By implementing security intelligence and control on the base station situated at the networking edge, one can considerably reduce the amount of networking traffic and effects that an attacker can exploit. A neurofuzzy based mutual authentication system with three biometric entities and a hash signature-based AKA protocol is developed to mutually authenticate the user equipment to the 5G base station is proposed in this paper.   
  
Introduction/Problem Statement:  
  
The 3rd Generation Partnership Project (3GPP) has specified that the 5G network architecture consists of the same elements as the previous generations which are User Equipment (UE, a mobile station and a USIM), a Radio Access Network (NG-RAN), and a core network. The main entity of the NG-RAN is the gNB, where "g" stands for "5G" and "NB" for "Node B". The term "Node B" has been a part of the terminology since the 3G era, referring to the base station that connects mobile devices to the cellular network. In 5G networks, the gNB functions as the radio access node responsible for connecting user devices (such as smartphones, IoT devices, etc.) to the 5G network. It manages the radio communication between the user equipment and the core network, facilitating the exchange of data and enabling the high-speed, low-latency capabilities promised by 5G technology. The 5G network introduces several key new technologies such as network slicing, network function virtualization and edge computing. The incorporation of these new technologies introduces many security issues in 5G networks. Small cell densification implies frequent handovers and hence frequent authentications [2] which makes seamless and secure handovers a necessity [5]. Securing the link between the base station and the user equipment ensures seamless handovers. The 5G networks enable widespread connections among a large variety of devices, however, this open network and access method brings in many vulnerabilities. [3], [4]. Key agreement and user authentication have been identified in [7] as being crucial for secure packet exchanges over the 5G networks. Biometric authentication of a user when the user is trying to access the system at the base station in 5G mobile communications is a very effective way to check and minimize security threats and attacks [8]. Implementing biometric authentication at the network's farthest edge in the base station (the first hop from the user) provides the security benefits of edge computing (including faster threat mitigation and lower threat impact than implementing security control on the far core network). An advanced artificial intelligence (AI) based mutual authentication system with three biometric entities and a hash signature-based AKA protocol is developed to mutually authenticate the user equipment to the 5G base station is proposed in this paper.   
  
Biometric data, once compromised, cannot be easily changed, however integration of multiple biometric entities enables more reliable authentication. A person talking salutation or greeting words at different times usually consists of a very narrow range of frequencies (0.08 ~ 3.5 kHz) which vary in nature from person to person [6]. Thus, voice frequency matching of the salutation or the word selected by the user like hi, hello, good Morning, etc. with his/her stored voice frequency for the word is taken as the first entity. Then the second entity is taken as the analysis of the unique patterns of ridges and valleys on the user’s fingertip. The third entity is the face image matching of the user based on unique facial features, including the distance between eyes, nose shape, and overall facial structure. All three biometric modalities are non-intrusive, requiring minimal physical contact and user acceptance is generally high due to the convenience of these methods.   
  
System Model/ Algorithm being proposed  
  
The network verifies the user using the Neurofuzzy model before using elliptic curve cryptography to authenticate the User Equipment at the base station. The proposed technique has the following steps:

User Enrollment: When the user initially accesses the system for the first time, the system asks the user for his/her salutation or greeting word, the word and the voice frequency is taken as the first entity. Then he/she is asked for his or her fingerprint, then the unique patterns of ridges and valleys on the user’s fingertip is taken as the second entity. Finally, the unique facial feature of the user is taken as the final entity. These are stored on the system cloud network. To adhere to privacy protocols, the system asks for authorization before proceeding with the storage. The voice frequency is measured using MATLAB and is typically recorded in Hertz (Hz), which represents the number of cycles per second of the sound wave. The facial image and fingerprint of the user is taken by the camera and fingerprint scanner on the user’s device respectively.

Storage Structure: The system storage has 3 databases for storing the entities. The first database, DB1 stores the subscriber the most frequently (V1), more frequently (V2), and less frequently (V3) used voice frequencies for the user’s chosen salutation word and its corresponding relative grades. The second database (DB2) stores the fingerprint range of each user. Just like for the voice frequency, the DB2 also stores the most probable (F1), more probable(F2), and less probable(F3) fingerprints. While the third database(DB3) stores the face images of all users in the network. Before the 3 databases proceed with the storage, each entity is hashed using the Secure Hash Algorithm 256-bit (SHA-256). The resulting hash value is then sent alongside the biometric data to ensure that the data will not be altered during transmission or storage.

Matching Process: Upon receiving a connection request, the server hashes the user's newly provided biometric data and compares it with the stored data. The server then finds the matched frequency of the salutation word within the rows V1, V2, and V3 of DB1 and stores it as v1, if not match, v1 = 0. Then it matches the frequency of the fingerprint within the stored range F1, F2, F3 of DB2 as f1, if not match, f1 = 0. The server or the switch finds the matched subscriber face image percentage by comparing pixels within the rows of DB3. If the face image of the user is matched with the stored face image pixelwise, then it stores value, q1= Relative grade of matched location in the row; otherwise, q1 = 0. These features are then passed through the neurofuzzy model, which combines fuzzy inference with neural network processing to determine the likelihood of a match based on the provided biometric data. The neurofuzzy model outputs a decision score indicating the degree of similarity between the provided biometric data and the stored data for each modality (voice, fingerprint, facial). Based on the decision scores from the neurofuzzy model, the server makes a final decision on whether to proceed with authentication.

Authentication Challenge: If the neurofuzzy model matches the biometric data with the stored data, the server proceeds with user authentication. The UE sends a request containing its identity U and authentication information (biometric data) to the base station. Transport Layer Security(TLS) is implemented to encrypt the communication channels, upon receiving the request, the base station chooses a suitable elliptic curve Ep over a finite field Fp and then selects a generator point P on the curve. It then generates the base station's private key d and computes its corresponding public key Q = dP. The biometric data is then converted into a point on the elliptic curve using Hashing Algorithm (Eligator). Then the station computes the user's public key by multiplying the base point P by a nonce which is typically a random or pseudo-random number. If the computed public key matches the stored public key associated with the user, proceed with the authentication process. Otherwise, reject the request. If the user's public key matches the stored public key: Generate a challenge nonce(N), this nonce is typically a random or pseudo-random number chosen by the base station. Then compute an authentication parameter using hashing functions and the user's public key. Send the authentication challenge to the user. Upon receiving the challenge, the UE Computes a response using the challenge, user's private key which was derived from the biometric data and the hashing functions. It then sends the response back to the base station. The base station verifies the received response and proceeds to compute the expected response using the stored public key, received challenge, and hashing functions. If the computed response matches the received response, authentication succeeds. Otherwise, reject the request. If authentication is successful, grant access to the user. A. S. Khan et al. proposes a Multifactor Authentication Protocol (LEMAP) for miniaturized mobile devices in a multihop scenario, based on lightweight elliptic curve cryptography. OTP (biometrics, random number), timestamp, challenge, and password serve as the foundation for the multi-factor authentication. LEMAP utilizes ECC with Elgamal for achieving lightweight security protocol, confidentiality, integrity, and non-repudiation. Elgamal's smaller key size helps to lower communication costs and makes it suitable for use on small devices. This scheme has significantly lower computation cost, communication cost, and authentication overhead. The authors of 5 aim to create a remote voice user verification system for users of 5G-based IoT services. This system will allow users to be verified and registered in a variety of scenarios where it is necessary to perform mandatory user data provision and registration, as well as their identification and verification. It will also automatically register users who have legitimate access rights by voice through mobile devices (such as a tablet computer, cell phone, or communicator), automatically register user voices using a telephone channel or microphone, and provide real-time speech and voice recognition.

Contributions of the proposed model:

Introduction of a multi-modal biometric authentication system combining voice, fingerprint, and facial recognition technologies.

Implementation of privacy-preserving storage through hashing with SHA-256 to ensure that the biometric data will not be altered during transmission or storage.

Utilization of a neurofuzzy model for assessing the similarity between user provided biometric data and stored biometric data for a secure matching process.

Introduction of an authentication protocol based on elliptic curve cryptography at the base station for verifying the identity of users

Literature reviewed:

[9] proposed a light weight biometric-based anonymous authentication technique between the user and the application server in wireless body area networks which preserves the patient’s privacy as well as achieves mutual authentication. The proposed scheme has three phases— initialization phase, registration phase, and login and authentication phase. In [10] a 5G key management and handover protocol is developed. The proposed protocol uses ANN-FL technique to optimize the selection of the target cell prior to the actual handover, reducing handover delays. They introduced shared keys to secure the link between source 5G Node and target and the link between access and mobility management function and User Equipment respectively. They also encapsulated and encrypted the session keys used during handover to thwart eavesdropping and other associated attacks. The handover and key management protocol proposed in the paper is a multi-criteria one which employed received carrier power, power density, path loss, traffic intensity, call blocking probability and velocity as handover triggering parameters. The authors of [11] demonstrate a system that can distinguish between authentic, tampered, and fraudulent biometrics in 5G-based smart cities by detecting changes to biometric modalities. In particular, they employ convolutional neural network (CNN)-based deep learning models and a hybrid CNN+Convolutional long-short term memory (ConvLSTM) model to calculate a three-tier probability that a biometric has been tempered. A dataset of fingerprint images with three different kinds of alterations is used to test the suggested models. Adavoudi et al. proposed a three-factor authentication scheme for wireless sensor networks that combines the user's password and biometric with a non-tamper-resistant smart card. The system uses access control, which enables users from various groups to view the data from authorized sensors. A system architecture suitable for WSNs in 5G-integrated IoT was presented by Shin et al. They suggested an ECC-based three-factor authentication, authorization, and key agreement scheme based on this architecture. Compared to other non-ECC-based asymmetric key cryptography techniques, ECC is an asymmetric key cryptography method that offers comparable security measures with smaller key sizes. They demonstrated that in addition to offering the required security features, the suggested scheme is resistant to mobile device loss and offline password guessing attacks, privileged insider and stolen verifier attacks, impersonation attacks, user collusion attacks and desynchronization attacks. The authors of [13] aim to create a remote voice user verification system for users of 5G-based IoT services. This system will allow users to be verified and registered in a variety of scenarios where it is necessary to perform mandatory user data provision and registration, as well as their identification and verification. It will also automatically register users who have legitimate access rights by voice through mobile devices (such as a tablet computer, cell phone, or communicator), automatically register user voices using a telephone channel or microphone, and provide real-time speech and voice recognition. [14] suggested using a crypto-biometric method for online voting. The authors' proposed mechanism involves the use of a gabor filter with a threshold measure in two major crypto-biometric methods: the palm vein and the palmprint. Furthermore, the information is transmitted and then encrypted using a random key after being embedded in the biometric vector using a fuzzy commitment technique. By utilizing the new retrieval method to extract the encrypted key, the decryption process is completed. The crypto biometric system's accuracy and key retrieval are validated by the results.

References:

[1] Sang-Yoon Chang et al, “Base Station Gateway to Secure User Channel Access at the First Hop Edge”, in Computer Networks.  
[2] V.O. Nyangaresi, A.J. Rodrigues, and S.O. Abeka, “ANN-FL secure handover protocol for 5G and beyond networks,” in International Conference on e-Infrastructure and e-Services for Developing Countries, Springer, Eb`ene City, Mauritius, 99–118, 2020.  
[3] M. Chen, C. Tan, X. Zhu, and X. Zhang, “A Blockchain-Based Authentication and Service Provision Scheme for Internet of Things,” in 2020 IEEE Globecom Workshops (GC Wkshps), IEEE, 1-6, 2020.   
[4] V.O. Nyangaresi, A.J. Rodrigues, and S.O. Abeka, “Efficient Group Authentication Protocol for Secure 5G Enabled Vehicular Communications,” in 2020 16th International Computer Engineering Conference (ICENCO), IEEE, Cairo, Egypt, 25-30, 2020.  
[5]. Vincent Omollo Nyangaresi, Anthony Joachim Rodrigues, and Silvance Onyango Abeka “Neuro-Fuzzy Based Handover Authentication Protocol for Ultra Dense 5G Networks”, in 2020 2nd Global Power, Energy and Communication Conference (IEEE GPECOM2020), October 20-23, 2020, Online Conference  
[6]. IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 15, Issue 3, Ser. II (May - June 2020), Mutual Authentication Technique with Four Biometric Entities Applying Fuzzy Neural Network in 5G Mobile Communications Pijush Kanti Bhattacharjee  
[7] S. Shin, and T. Kwon, “A privacy-preserving authentication, authorization, and key agreement scheme for wireless sensor networks in 5G-integrated Internet of Things,” IEEE access, 8, 67555-67571, 2020  
[8] Pijush Kanti Bhattacharjee, “Mutual Authentication Technique with Four Biometric Entities Applying Fuzzy Neural Network in 5G Mobile Communications”, IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), 2020

[9]Gitanjali Behera, Saroj Kumar Panigrahy, and Ashok Kumar Turuk, “A Biometric based Anonymous User Authentication Technique in Wireless Body Area Networks,” in Proceedings of the International Conference on Communication, Computing and Internet of Things (IC3IoT 2018). IEEE, 2018, pp. 341-345.

[10] Adavoudi Jolfaei, Amirhosein & Ashouri-Talouki, Maede & Aghili, Farhad. (2019). “Lightweight and anonymous three-factor authentication and access control scheme for real-time applications in wireless sensor networks. Peer-to-Peer Networking and Applications.” 12. 43-59. 10.1007/s12083-017-0627-8.  
[11] Gitanjali Behera, Saroj Kumar Panigrahy, and Ashok Kumar Turuk, “A Biometric based Anonymous User Authentication Technique in Wireless Body Area Networks,” in Proceedings of the International Conference on Communication, Computing and Internet of Things (IC3IoT 2018). IEEE, 2018, pp. 341-345.

[12] A. S. Khan et al., "Lightweight Multifactor Authentication Scheme for NextGen Cellular Networks," in IEEE Access, vol. 10, pp. 31273-31288, 2022, doi: 10.1109/ACCESS.2022.3159686.

[13] O. Lavrynenko, A. Pinchuk, H. Martyniuk, A. Fesenko, S. Yarotsky and M. Aleksander, "Remote Voice User Verification System for Access to IoT Services Based on 5G Technologies," 2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Dortmund, Germany, 2023, pp. 1042-1048, doi: 10.1109/IDAACS58523.2023.10348955.

[14] A. Meraoumia, H. Bendjenna, M. Amroune and Y. Dris, "Towards a secure online E-voting protocol based on palmprint features", Proc. 3rd Int. Conf. Pattern Anal. Intell. Syst. (PAIS), pp. 1-6, Oct. 2018.