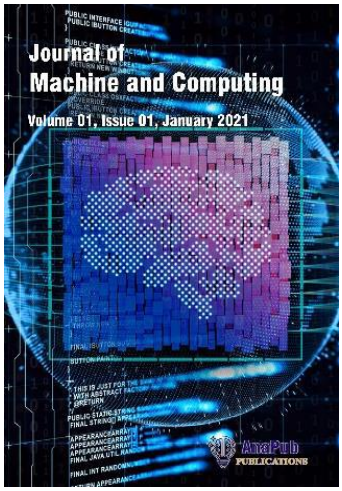
Journal Pre-proof

An Improvised Finger Vein Patterns Attribute Based Recommendation Technique for Remote (IoT) Authentication using Key-Value Distribution



Sujani G and Sreerama Reddy G M

DOI: 10.53759/7669/jmc202505166

Reference: JMC202505166

Journal: Journal of Machine and Computing.

Received 02 April 2025

Revised from 16 June 2025

Accepted 18 July 2025

Please cite this article as: Sujani G and Sreerama Reddy G M, "An Improvised Finger Vein Patterns Attribute Based Recommendation Technique for Remote (IoT) Authentication using Key-Value Distribution", Journal of Machine and Computing. (2025). Doi: https://doi.org/10.53759/7669/jmc202505166.

AnaPub PUBLICATIONS

An Improvised Finger Vein Patterns Attribute Based Recommendation Technique for remote (IoT) authentication using Key-Value Distribution

Sujani G[1], Sreerama Reddy GM[2]

[1]Department of Electronics and Communication Engineering., C Byre Gowda Institute of Technology, Kolar, VTU, Karnataka, India.

[2]Department of Electronics and Communication Engineering., Bangalore Technological Institute, VTU, Bengaluru, India

sujani13@gmail.com, sreeramareddy90@gmail.com

Abstract – Authentication and remote validation is a challenging task, the process of authentication via finger vein values is a challenging task for IoT values customization. In this paper, we have developed an improvised Attribute Based Recommendation (ABR) technique for extracting the finger vein attributes and processing via IoT administrator gateway for processing and mapping the key attributes of dynamically collected finger veins. Based on the recommendation, the attributes correlation is extracted and key value pattern is generated with synchronization from user backend via secure channel. The end user further extracts the attribute key values and encodes the authentication form access for remote authentication. The proposed technique has secured an accuracy of 97% under open channel IoT authentication and 94% in a closed channel communication.

Keywords – Remote IoT authentication, finger vein pattern extraction, IoT, Key value encoding, attribute recommendation.

I. INTRODUCTION

In the realm of Internet of Things (IoT) devices, where authentication and security play pivotal roles, the monitoring and processing of these devices are facilitated through either a computational server or a centralized administrator. This infrastructure is designed to ensure effective communication and data management. The communication paradigm within IoT devices is structured around a dedicated channel. However, a noteworthy limitation arises in the form of a lack of validation in the peer-to-peer channel between the end-user and the processing administrator. This can potentially introduce vulnerabilities and compromise the overall security of the IoT ecosystem. Adhering to established operational standards, the authentication process is specifically designed to reside on the computational end, with a focus on the server. The current state-of-the-art authentication methods predominantly rely on digital inputs such as PINs, passcodes or passwords. These inputs, typically comprising numerical or alphanumeric characters, form the bedrock of user verification in most IoT systems.

In response to the ever-evolving landscape of cybersecurity, there is an increasing demand for more robust and sophisticated authentication mechanisms within IoT devices. Biometric inputs, including fingerprints, finger-vein patterns, and retinal scanning, are gaining prominence as they offer a more secure and personalized means of authentication. However, the

integration of biometric authentication services brings about its set of challenges. One critical concern revolves around ensuring end-to-end communication integrity. The transmission of biometric data necessitates stringent measures to protect against interception or tampering. Additionally, preserving the originality and authenticity of the data throughout the authentication process is crucial to prevent unauthorized access and ensure the overall security of the IoT ecosystem. Efforts to address these challenges are paramount in establishing a resilient and secure foundation for the continued proliferation of IoT devices, safeguarding sensitive data and maintaining user trust in an interconnected world.

The proposed system is designed and developed to encounter the need and necessity of higher order authentication systems and technique is based on the data processing and computation of finger vein patterns for authentication. The approach is dependent on end-to-end channel for secure communication via third party service provider. The approach is developed for remote authentication purpose of users and integrated application. The objective of this approach is to develop a user-authentication framework free from the geographical parameters of the IoT devices. The presented system is meticulously crafted to address the demand for advanced authentication systems, focusing on a methodology grounded in the processing and computation of finger vein patterns for authentication purposes. This innovative approach relies on leveraging end-to-end channels for secure communication, facilitated through a third-party service provider. The system is specifically designed to cater to the requirements of remote authentication for users and integrated applications.

The primary goal is to establish a robust user-authentication framework that transcends geographical limitations associated with Internet of Things (IoT) devices. By centering the authentication process around the unique biometric trait of finger vein patterns, the system aims to enhance the overall security posture. Leveraging secure communication channels via a third-party service provider ensures a comprehensive and reliable authentication mechanism. This design choice not only bolsters the security of the authentication process but also streamlines the integration of the system with various applications. The overarching objective of this approach is to create a user-authentication framework that operates seamlessly across diverse geographical locations, contributing to the scalability and adaptability of IoT devices. By mitigating the constraints imposed by geographical parameters, the proposed system seeks to offer a versatile solution for secure and remote authentication within the expanding IoT landscape.

II. LITERATURE REVIEWS

The authentication and validation process within the Internet of Things (IoT) infrastructure is established on a rather straightforward approach involving the sharing of information and pattern matching through methods such as password searches, pin searches, and One Time Password (OTP) services. Despite their common usage, these approaches have inherent limitations, particularly when accessed or requested from remote geographical locations for authentication services. In the realm of IoT, specific protocols are dedicated to governing its operations, as elucidated in [1] [2] and the comprehensive survey documented in [3]. Of particular significance is the implementation of a two-factor authentication protocol, which assumes a pivotal role in tailoring and managing sensitive information in the face of potential threats from prominent attackers.

An illustrative study can be found in [4], where the authentication process for biomedical sensor information involves a two-phase approach utilizing either a real or random model. This nuanced methodology adds an extra layer of security to safeguard critical health-related data from unauthorized access or manipulation. Additionally, the Authentication and Key Agreement (AKA) protocol-based authentication for IoT applications on Long-Term Evolution (LTE) networks is explored in [5]. This discussion delves into the intricacies of how AKA protocols contribute to enhancing the security of IoT devices, particularly when operating within the framework of high-speed LTE networks. The authentication and validation mechanisms within IoT infrastructure go beyond mere information exchange and pattern matching, incorporating dedicated protocols and advanced methods such as two-factor authentication and AKA protocols to ensure robust security, especially in the context of remote access and diverse application scenarios.

Expanding on the Authentication and Key Agreement (AKA) protocol, its application extends into the realm of Industrial Internet of Things (IIoT) applications, as detailed in [6]. This expansion specifically addresses two critical dimensions: complexity and communication cost. In tackling the complexity dimension, the AKA approach is further strengthened and tailored through the implementation of a key generation technique that utilizes Elliptic Curve Cryptography (ECC). This enhancement ensures a robust and reliable key-sharing mechanism within IIoT applications, contributing to the overall effectiveness of authentication processes. In [7], researchers have presented a multi-stage approach aimed at fortifying authentication within an IoT infrastructure. This approach employs the Burrows-Abadi-Needham (BAN) logic, known for its reliability in achieving mutual authentication. The multi-stage design provides a comprehensive and layered security strategy, addressing various potential vulnerabilities and ensuring a more resilient authentication process.

Further, a notable development in authentication protocols is the Firmware Secure Multi-Factor Authentication (FSMFA) discussed in [8]. This protocol takes a unique approach by leveraging the device firmware and software feasibility to establish mutual authentication keys within the framework of BAN logic. By incorporating the device's firmware and software capabilities, FSMFA not only enhances security but also demonstrates adaptability to the evolving landscape of IoT security challenges. The AKA protocol's influence extends into the industrial IoT domain, where additional considerations of complexity and communication cost are addressed. Moreover, advancements such as the use of Elliptic Curve Cryptography (ECC), multi-stage authentication with BAN logic, and the innovative FSMFA protocol contribute to the continuous improvement of authentication processes within IoT and IIoT applications.

With the advancement of communication technologies, the abiding of 5G norms for communication and authentication is a challenging task. In this regard, the approach in [9] has discussed the Real or Random (ROR) model for customization of information bits transferred and optimized. The detailed survey on multi-factor of IoT authentication protocols [10] is conducted by a Systematic Literature Review (SLR) methodology to assure higher and impactful analysis in the survey drawn. The collective summary of this survey is to harness the need and demand for remote authentication in IoT applications such as finger vein pattern, retina pattern etc. these approaches are further required to be evaluated under a secure cloud and administered environment for computing and processing. Thus from this survey, we have streamlined the proposed technique on remote authentication and monitoring.

III. METHOD AND MATERIALS

The proposed technique is developed with a trivial dual-validation cum base user authentication schema. The objective of this technique is to fetch finger vein patterns from remove authentication and validate through IoT framework/channel. Typically, the input from the users are customized and validated as shown in Fig. 1. The computational unit of dual authentication is based on the internal validation of user samples stored with the corresponding samples collected dynamically while the process activation. Typically, the vein patterns are processed and customized via a dedicated attribute recommendation technique as proposed in this manuscript. The attribute recommendation and customization technique extracts the internal Region of Interest (RoI) for the operational computation and processing. In general the dynamic data samples of users finger-vein which is subjected to the authentication is extracted under RoI filters. The process further evaluates the customization as shown in Fig. 2 respectively via three distinct phases.

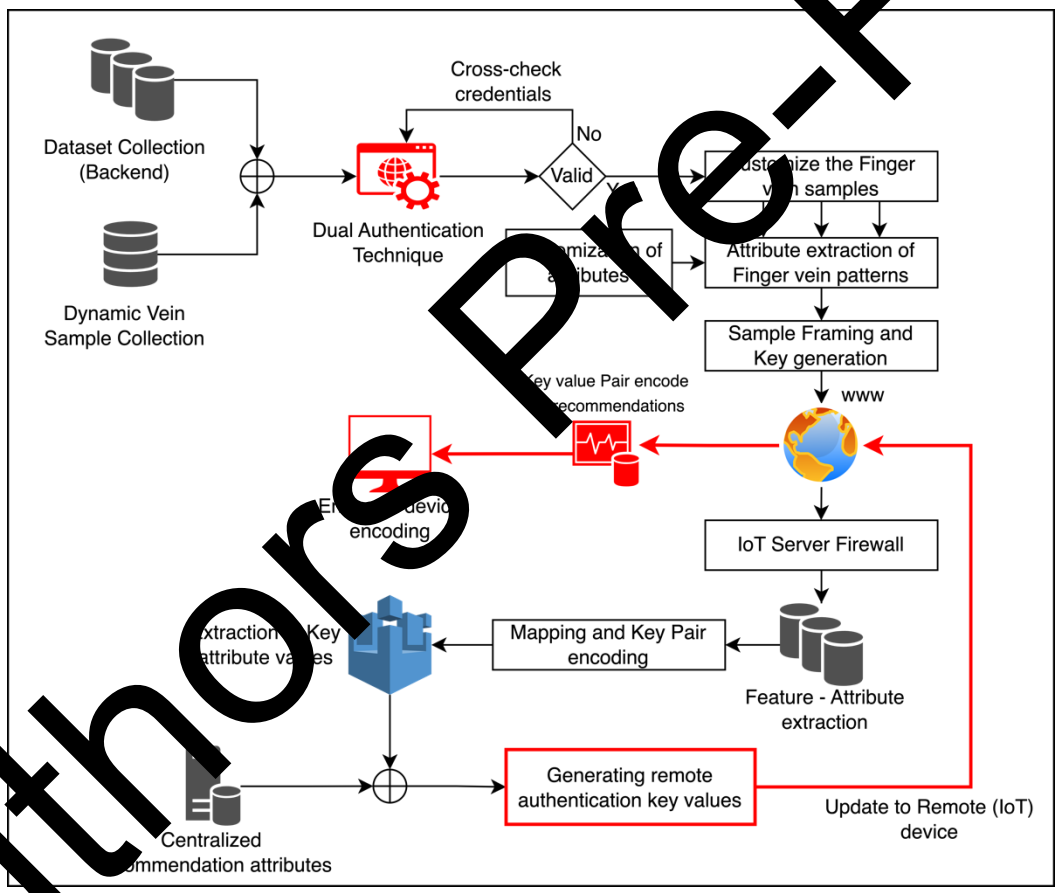


Fig. 1: Architecture diagram representation of proposed system

Data collection and pre-processing phase

This phase includes the primary collection of finger vein patterns and appending preprocessing technique such as the dual-authentication technique and attribute extraction from the subjected RoI of computation. The dataset authenticated via backend is subjected to be customized via user centric environment for validation (i.e.) the validation of attributes from dynamic schema and

stored schema is proposed under a single authentication platform or at the user-end. On consideration the subjected schema values of finger vein (dynamic) and backend (stored) patterns are validated via HTTP/RTSP protocol standards for secure channel communication, hence opening the services to the external environment of internet.

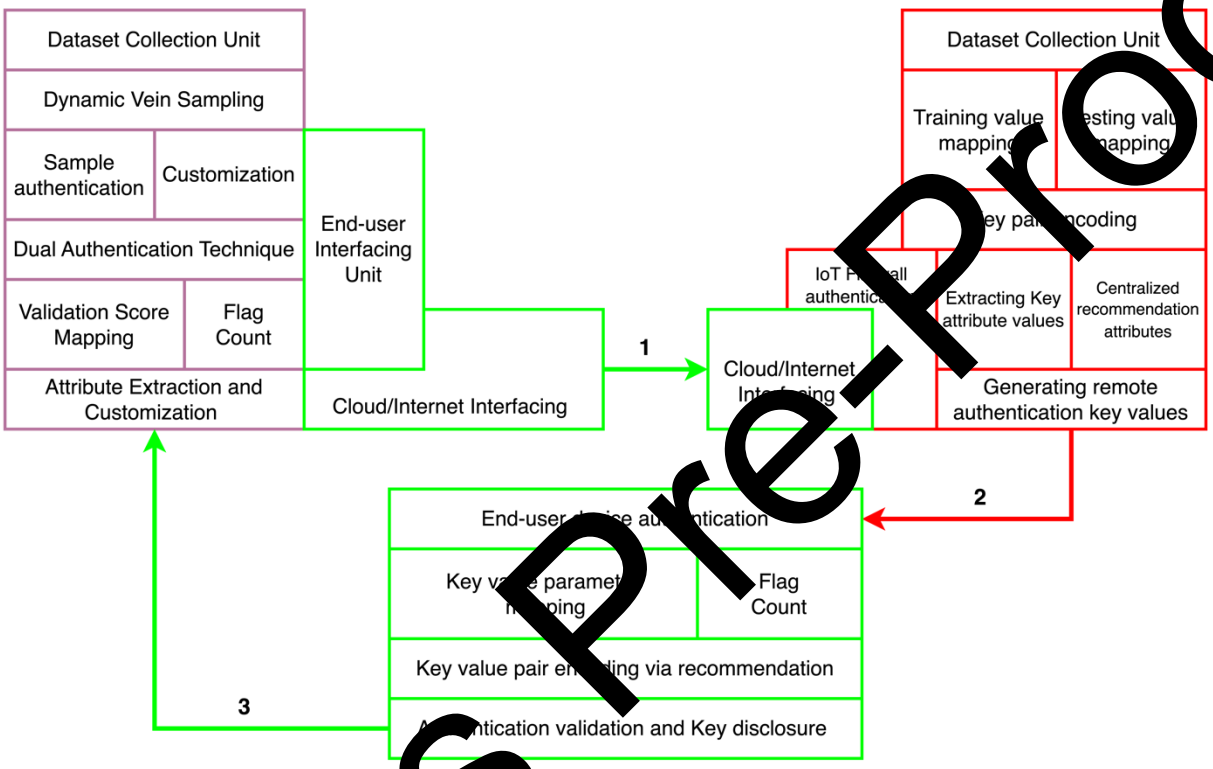


Fig. 2: Classification and flow control representation of user involvement modules and processing of remote authentication via IoT infrastructure

B. Feature extraction and attribute recommendation

This process is streamlined via internet (HTTP/RTSP) towards an IoT/cloud server services indexing. The feature and attributes from the primary and dynamic data samples are packed and transferred to the remote validation server for approval generation. Typically, the attribute customization and processing involves a recommendation technique for relevant attribute extraction. This includes the feature set and attribute set values for higher order computation. The attributes extracted are based on RoI influences and hence the parametric quotient of extraction is evaluated. The similarity scores and potential of attribute training is computed in this phase. The outcome of attributes recommendation generates a unique "Remote Authentication Key Values (RAKV)". The RAKV is a one-time authentication unit value generated from the services of key-values and elements. According to the objective of remote authentication the RAKV is digitalized and segmented via HTTP/RTSP channel for communication via user authentication using IoT channel.

C. End-user Remote device authentication

In this step, the RAKV is received and validated via the functional approach of secondary key-values and elements associated with it. The functional representation of end-users is associated with a one-time authentication pass values. The values are customized and communicated via HTTP/RTSP to the base (remote) user for validation. The remote users further exchange the authenticated key operation for access authentication and validation. The overall three phases assures the remote authentication and processing of finger vein pattern via IoT application.

IV. MATHEMATICAL REPRESENTATION

Consider the process of pre-trained datasets (P_X) with each value of authentication as $(\sum P_X) \Rightarrow \{P_{X1}, P_{X2}, P_{X3}....\}$ such that $(\forall P_{Xi} \in \mathrm{P})$ where (P) is the preserved/backend dataset attributes for expected finger vein patterns and backend storage. The value of $\left[(\mathrm{P}_X) \rightarrow \sum^{\infty}(P_i)\right]$ at every changing interval of data storage and collection. Let the (F_X) be the record of failed interval of time such that $(\forall F_X \subseteq \mathrm{P} \in P_i) \Rightarrow (0 \rightarrow t)$ where the time bound (t) is fixed for extraction. The extraction parameters are governed under a fixed interval of computation. If the regular clock on failure is altered, the computation flag is set to freeze at given time (t_z) interval of time such that $(t_z \le t_i)$ where (t_i) is the minimal looping time for computation. Technically, if $(\sum P_i < t_z < t_i)$ then the preprocessing phase is initialized for computation.

The preprocessing phase includes a customizable computation channel for regular operation management such as background validation and dual mode authentication as represented in Fig. 1. This includes a series of cross validation such as custom flag (F_C) setup, counter updating (C_U) and under validation (U_V) for a given time interval (t_j) such that $(j \subseteq i)$ and $(t_j \le t_i)$ with minimal waiting time is bounded with operational delay and hence standard customization is referred for the further evaluation. The consideration values $(F_C \in C_U(autten))$ until the rational user associated with the backend database (P_X) is validated such that $(\forall C_U \subseteq P_X)$ and $(C_U \Rightarrow U_V \bigcap P_X)$ at the time validation and the state of $(U_V = ACTIVE)$. This process indicates the validation is successful at the primary end of data and hence results in secondary customization for remote authentication.

The remote authentication process is developed within a series of time interval (t) such that $(\forall t \Rightarrow \{t_1, t_3 ... t_i ... t_j ... t_n\})$ and the authentication is restricted with a time interval (t_n) such that $(\forall t_n < \infty)$ where (∞) is the time bound required for authentication with $(t_x \cong t_n)$ and $(x \le n)$ for a given time frame values. Hence the situation process of validation can be represented in Eq. 1 for ease in consideration with (t_x) series.

$$t = \sum^{\infty}\left(\frac{\delta(t_i)}{\delta t_1} \oplus \frac{\delta(t_{i+1})}{\delta t_2} \oplus \frac{\delta(t_{i+2})}{\delta t_3} \oplus .....\frac{\delta(t_n)}{\delta t_n}\right)_{\mathrm{P}}^{n<\infty} \quad (1)$$

$$\therefore \sum(t) = \log_t (n)_0^{\infty} \cup \left[\sum_{i=1}^{n} \frac{\delta(t_i)}{\delta t} \right] \quad (2)$$

With a continues split of information variable $(\sum t)$ can be further adopted with (F_C) count values as shown in Eq. 3.

$$\therefore \sum(t) = \log_t (n)_0^{\infty} \cup \left[\sum_{i=1}^{n} \frac{\delta(F_C) \oplus \sum_{j=j+1}^{n} (C_U)}{\delta t} \right] \quad (3)$$

$$\therefore \sum(t) = \log_t (n)_0^{\infty} \cup \left[\lim_{n \to \infty} \left\{ \frac{\Delta(F_C)_0^3 \oplus \Delta(C_U)_j}{\Delta t} \right\} \right] \quad (4)$$

$$\therefore \sum(t) = \log_t (n)_0^{\infty} \cup \left[\frac{1}{t} \left(\lim_{n \to \infty} \left\{ \Delta(F_C)_0^3 \oplus \Delta(C_U)_j \right\} \right) \right] \quad (5)$$

Thus, according to the Eq. 3, the representation index of $\Delta(F_C)_0 \oplus \Delta(C_U)_j$ is jointly associated with structural values of time (t_i) such that, $(F_C \geq C_U \leq C_{max})$ and $(\forall U_V \subseteq P_X)$ i.e. the functional dataset of background verification model. The model further assures the count of successful attempts occurrence with failure ratio is (3) such that $(\Delta F_C \leq 3)$ for successful processing and computation of vein pattern within the user defined environment. Technically, the potential review analyses of existing (ΔF_C) value are bound to be operational within the count_flag (C_U) range such that ambiguous extraction is processed. The representation of time interval authentication under local use is shown in Eq. 4 and Eq. 5 respectively. The customized value attributes associated in Eq. 5 extracts the time (t_i) and assures the computation process is validated.

The process of time bound computation is resultant on Eq. 5 and is further aligned with attribute extraction process. The attributes (A) in the manuscript is derived from the existing representation values of finger vein patterns as $(A = A_1, A_2, A_3 .... A_n)$ such that, $(\forall A_X \in P_X)$ and $(A_X \Rightarrow (F_C)_0^3)$ and $(U_V = ACTIVE)$. Segmented variables associated in this order of attributes are further evaluated as $\forall A_X \Rightarrow (\sum A_i \subseteq \sum A_j)$ where, (A_i) is the current or primary extraction values, whereas (A_j) is the secondary associated values of extraction. This includes the $(A_i \in A_j)$ such that, all the existing (A_i) values are associated with (A_j) at a given time (t). Thus, on generalized the costumed variables (C_V) is further associated with (A_i) such that,

$\left(\forall A_j \subseteq A_i \Rightarrow \left(\forall C_V \oplus A_j\right)\right)$ at a given time representation. The generalized vein attributes $\left(A_j\right)$ are extracted as shown in Eq. 6.

$$A_j \Rightarrow \left\{\left\|\log\left(A_j\right)_j^n\right\| \oplus \log_k\left[\frac{\Delta A_j \bigcup \Delta C_V}{\Delta t_i}\right]\right\} \tag{6}$$

Thus according to Eq. 6, the attributes $\left(A_j\right)$ are dependent on $\left(\Delta t_i\right)$ time interval and hence while extracting $\left(A_i\right)$ the range of data interpretations should be evaluated as shown in Eq. 7 and Eq. 8 respectively.

$$A_i \Rightarrow \left\{\frac{\delta\left(A_j\right)}{\delta t_i} \oplus \left[\left\|\log\left(A_i\right)_{P+1}^n\right\| \oplus \log_P\left(\frac{\left[\Delta A_i \oplus \Delta A_j\right] \bigcup \left[\Delta C_V\right]}{\Delta t_{i+1}}\right)\right]\right\} \tag{7}$$

$$\therefore A_i \Rightarrow \frac{1}{\sum\left(\Delta t_{i+1}\right)}\left\{\left(\Delta A_j\right)_{t_i} \oplus \left\{\Delta\left(A_i\right)_{t+1}\right\}\right\} \tag{8}$$

$$\therefore A_i \Rightarrow \frac{1}{\sum\left(\Delta t_{i+1}\right)}\left\{\int_0^n \left(\Delta A_j\right)_{t_i} \cap \int_j^n \left(\Delta A_i\right)_{t_{i+1}}\right\} \tag{9}$$

Thus, according to Eq. 9, the customizable attributes of variables $\left(A_i\right)$ and its associated instance $\left(A_j\right)$ is validated at a given time instance $\left(\Delta t_{i+1}\right)$ where $\left(i+1\right)$ is the second instance of time frame referred with single shot data dynamically collected and processed. Hence, the streamlined parameters of attribute values are customized into a generative model for attribute extraction and evaluation $\left(C_Z\right)$ as shown in Eq. 10.

$$C_Z \Rightarrow \left[\frac{\Delta A_i \oplus P_X \oplus C_V}{\Delta t_{i+1}}\right] \cap \left[\Delta A_j\right] \tag{10}$$

According to Eq. 10, the customization variables of attributes are associated and fragmented into regional core attributes $\left(A_i\right)$ such that $\left(\forall A_i \subseteq A_j\right)$ and $\left(A_j\right)$ is processed with time frame $\left(t\right)$ and hence $\left(t > t_{i+1}\right)$ with each attribute $\left(A_j\right)$ extracted prior to secondary attribute extraction process. The $\left(C_Z\right)$ variables are further expanded for remote server authentication as shown in Eq. 11. On reaching the IoT firewall, the authentication remote server categorizes the input stream as priority customization variables $\left(C_{ZP}\right)$ for ease in processing and validation.

$$C_{ZP} \Rightarrow \log_n\left\{\left\|C_Z\right\|_{t+1}\right\} \oplus \left(\Delta U_{V(ACTIVE)}\right) \tag{11}$$

Thus, the rational representation of $\left(\Delta U_{V(ACTIVE)}\right)$ and associated $\left(C_Z\right)$ is decoded via third party channel operational technique included via HTTP or RTSP./ the features $\left(F_Z\right)$ and attributes are extracted as shown in Eq. 12 for mapping and validation.

$$F_Z \Rightarrow \log_n \left[\left\|C_Z\right\|_P\right]_{t+1} \Rightarrow \left[\frac{\delta\left(\left\|C_Z\right\|_{t+1}\right)}{\delta t} \oplus \frac{Ext\left(A_i \oplus A_j \oplus P_X\right)}{Ext\left(C_V\right)}\right] \tag{12}$$

The extracted feature set $\left(F_Z\right)$ is further evaluated to optimize the process of key-generation. The key-generation $\left(K_Z\right)$ is a one-time pass key value generated for resultant connection based authentication. Typically, the key generated is bound with the connected HTTP/RTSP IP address of local user and its corresponding properties. The key generated $\left(K_Z\right)$ is shown in Eq. 13.

$$K_Z \Rightarrow \int_0^n \frac{\delta\left(F_Z\right) \oplus \left[\lim_{n\to\infty}\left(F_Z\right) \otimes \left\|A_i \oplus P_X\right\|\right]}{\delta t} \tag{13}$$

$$K_Z \Rightarrow \frac{1}{t} \times \left\{\Delta F_Z \oplus \left[\lim_{n\to\infty}\left(\Delta F_Z\right) \otimes \left\|A_i \oplus P_X\right\|\right]\right\} \tag{14}$$

With the key generated $\left(K_Z\right)$ the values of attribution and functional expansion is computed via the activated channel in the IoT framework application domain. Typically, the bounding key value with an associated time to live (TTL) is embedded for secure communication and authentication. The process is further communicated to the application seeking a remote authentication. The receiving end user acquires, the TTL computed is within the acceptable range of authentication standards to avoid unprecedented events.

V. RESULTS AND DISCUSSIONS

The proposed approach for remote authentication via finger vein pattern on IoT applications is a novel and first of its kind for the larger applications. The process of deployment is dependent on the dataset creation, training and validation. The inputs of primary dataset are bound with respect to the user driven samples and hence requires minimal training on annotating the data units. The datasets are further associated with user indexing to avoid cross training and sample cloning. The validation of finger vein patterns are further evaluated and customized with reference to the sample size and customization ratio [11]. The detailed representation of authenticating sample at the user-end is shown in Table. 1. Thus according to size of vein pattern in user stage, it is made constant with 237 bytes and the communication channel is optimized accordingly. The phase of user authentication is based on user type and the privilege given.

Table. 1: Observations of detailed customization of user principles and evaluation time

User_Type	Privilage_Type	Finger Vein Pattern Size (B)	Evaluating time (ms)	Rational differences (ms)
ADMIN	ADMIN	237	2.783	0.0721

STANDARD	ADMIN	237	2.817	0.0832
STANDARD	STANDARD	237	3.172	0.0873

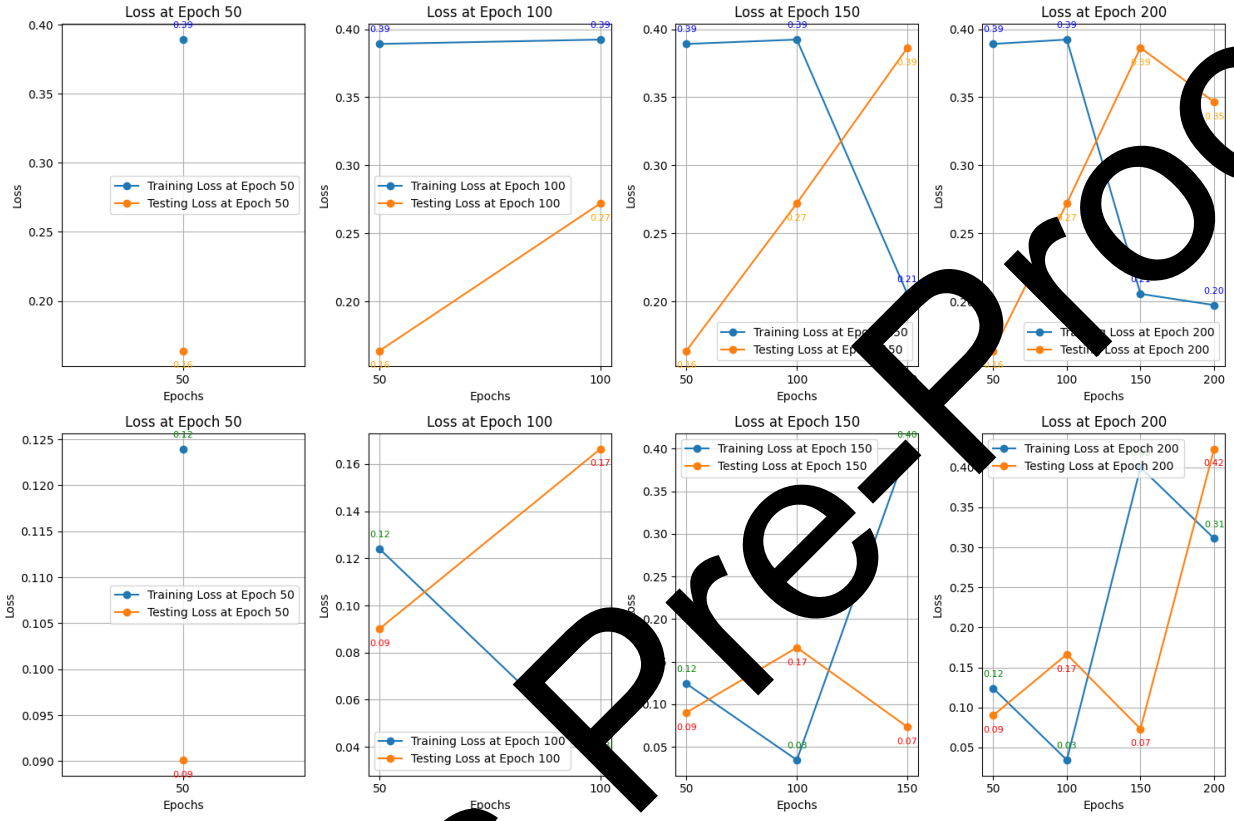


Fig. 3: Representation of training and testing losses on various epochs for finger vein pattern datasets

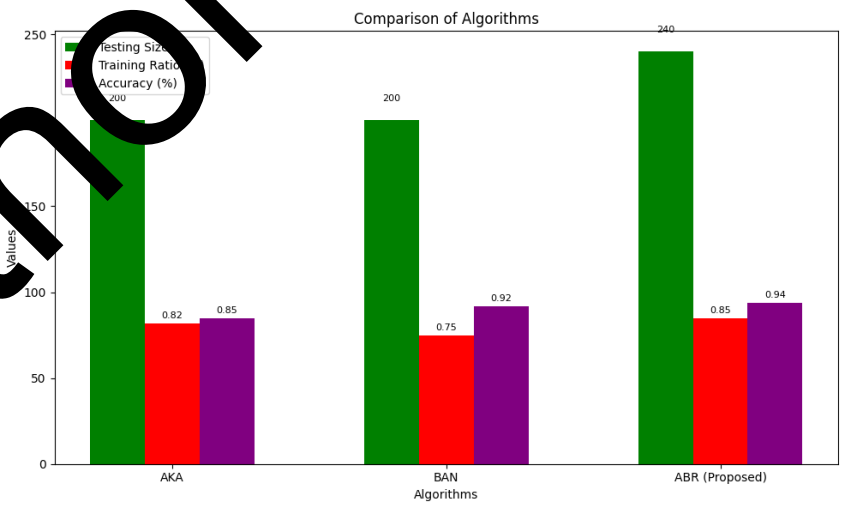


Fig. 4: Computation of accuracy with reference to training and testing data_size [11]

The finger_vein datasets from GAN model [11] is computed to evaluate and customize the authentication protocol. In Fig. 3, a detailed representation is shown with respect to the changing epoch intervals. The training and testing losses are computed to assure minimal losses and maximum relaiblity in remote authentication phases. Typically, the losses are minimal in initial epochs (50, 100, and 150), whereas a consistency in losses is attained with respect to 150 and beyond. Further, the process of training size and testing size is computed and accuracy is developed as shown in Fig. 4. In the proposed ABR technique, the testing size of data is constant and higher compared to the training size as the initial data-input from the user is limited to 7 turns max with 5 minimal turns, hence the training size is optimized and minimal.

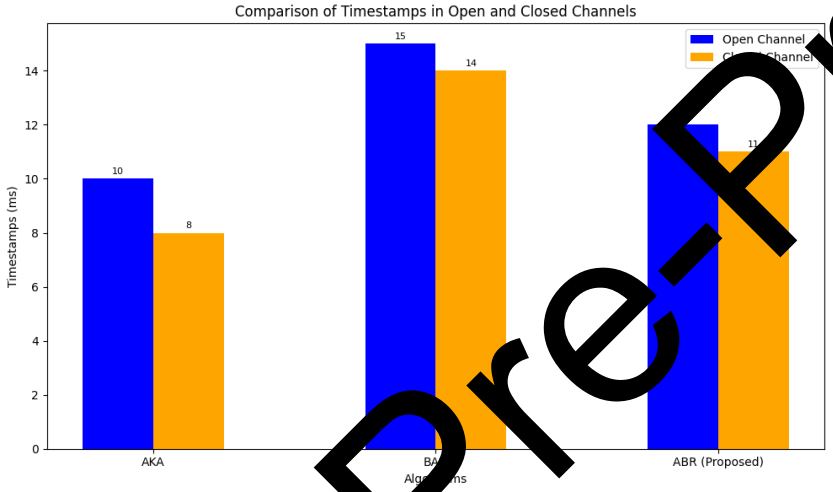


Fig. 5: Comparison of Timestamps in Open and Closed IoT application channel for remote authentication.

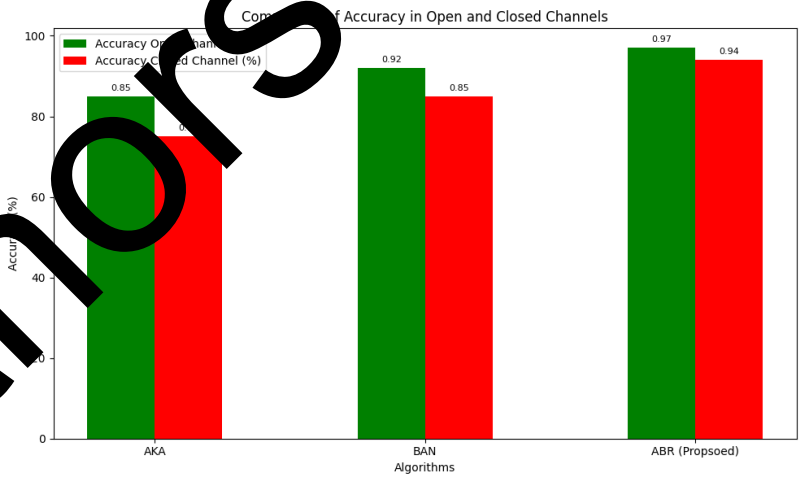


Fig. 6: Accuracy comparison in open and closed channel of IoT application for remote authentication.

According to Fig. 5 and Fig. 6, the computation of open channel and closed channel timestamps are evaluated. The open channel of IoT application is under public domain of operations via third party service providers. The users under this domain operate on minimal and

standard privileges of the communication channel, whereas the closed channel is the dedicated line of communication for a given application and hence the process is monitored via an authentication protocol. The proposed technique (ABR) is compared with AKA and BAN logic approach for authentication and time stamp computation. The proposed ABR technique has achieved an accuracy of 97% under 12ms timestamp on an open channel and 94% accuracy under 11ms timestamp for a closed channel. This improves the key sharing principle and operating ratios as shown in Table. 1 with respect to the user privileges.

VI. CONCLUSION

The proposed technique is designed and validated with the customization approach of finger vein pattern authentication via remote application. The technique has extracted relevant and subjected attributes via feature recommendation technique. Typically, the extracted features are further evaluated with dynamic patterns and stored patterns of finger-vein using dual-mode authentication technique and generate a recommended pattern for evaluation. The process further generates an instance one-time key variable for processing and customization on remote authentication. The scenario of remote authentication is governed via HTTP/RTSP protocol channel for secure communication. The technique has successfully demonstrated the remote authentication via finger vein patterns and key distribution by an accuracy of 97% in an open IoT channel. In future, the proposed technique can be interfaced with real-time face and synchronized security applications for improving the reliability of the technique

Reference

1. Azrour, M., Mabrouki, J., Guezzaz, A., & Farhaoui, Y. (2021). New enhanced authentication protocol for internet of things. *Big Data Mining and Analytics*, *4*(1), 1-9.
2. Porambage, P., Schmitt, C., Kumar, P., Gurtov, A., & Ylianttila, M. (2014, April). Two-phase authentication protocol for wireless sensor networks in distributed IoT applications. In *2014 IEEE Wireless Communications and Networking Conference (WCNC)* (pp. 2728-2733). Ieee.
3. Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., & Shu, L. (2017). Authentication protocols for internet of things: a comprehensive survey. *Security and Communication Networks*, *2017*.
4. Agrahari, A. K., Sharma, S., & Venkatesan, S. (2023). Two factor authentication protocol for IoT based healthcare monitoring system. *Journal of Ambient Intelligence and Humanized Computing*, *14*(12), 16081-16098.
5. Mo[illegible]rha[illegible], M. [illegible], & [illegible]amah, M. (2023). REPS-AKA5: A robust group-based authentication protocol for IoT applications in LTE system. *Internet of Things*, 100700.
6. [illegible]ith, [illegible] & Deborah, L. J. (2023). An efficient key agreement and authentication protocol for secure communication in industrial IoT applications. *Journal of Ambient Intelligence and Humanized Computing*, *14*(3), 1431-1443.
7. Alhusayni, K., Wazirali, R., AlAkhras, M., Almasri, M., & Alhazmi, S. (2023). A Multi-Stage Secure IoT Authentication Protocol. *Computer Systems Science & Engineering*, *45*(1).
8. Chen, Z., Cheng, Z., Luo, W., Ao, J., Liu, Y., Sheng, K., & Chen, L. (2023). FSMFA: Efficient firmware-secure multi-factor authentication protocol for IoT devices. *Internet of Things*, *21*, 100685.
9. Li, X., Liu, S., Kumari, S., & Chen, C. M. (2023). PSAP-WSN: a provably secure authentication protocol for 5g-based wireless sensor networks. *CMES-Computer Modeling in Engineering & Sciences*, *135*(1), 711.
10. Fneish, Z. A. A. M., El-Hajj, M., & Samrouth, K. (2023, May). Survey on IoT Multi-Factor Authentication Protocols: A Systematic Literature Review. In *2023 11th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-7). IEEE.

11. Yang, H., Fang, P., & Hao, Z. (2020, December). A gan-based method for generating finger vein dataset. In *Proceedings of the 2020 3rd International Conference on Algorithms, Computing and Artificial Intelligence* (pp. 1-6).