


Please cite the Published Version

Nagarajan, Senthil Murugan, Devarajan, Ganesh Gopal, M, Suresh Thangakrishnan, T V, Ramana, Bashir, Ali Kashif  and AlZubi, Ahmad Ali (2024) Artificial Intelligence Based Zero Trust Security Approach for Consumer Industry. IEEE Transactions on Consumer Electronics. ISSN 0098-3063

DOI: <https://doi.org/10.1109/TCE.2024.3412772>

Publisher: Institute of Electrical and Electronics Engineers (IEEE)

Version: Accepted Version

Downloaded from: <https://e-space.mmu.ac.uk/635863/>

Usage rights:  In Copyright

Additional Information: © 2024 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works

Enquiries:

If you have questions about this document, contact openresearch@mmu.ac.uk. Please include the URL of the record in e-space. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from <https://www.mmu.ac.uk/library/using-the-library/policies-and-guidelines>)

Artificial Intelligence based Zero Trust Security Approach for Consumer Industry

Senthil Murugan Nagarajan, *Member, IEEE*, Ganesh Gopal Devarajan, *Senior Member, IEEE*, Suresh Thangakrishnan M, Ramana T V, Ali Kashif Bashir, *Senior Member, IEEE*, and Ahmad Ali AlZubi

Abstract—Development in internet technology made consumer electronics growth to another extent where several consumers from all over the world utilize various essentials through recent development. However, consumer electronics based devices could be vulnerable to cyber attacks if it is not appropriately secured. In this research work, we proposed AI-enabled deep learning model based zero trust security (AIDL-XTS) framework for verification and authentication for devices, users, and applications for every access request. We use smartphone sensor data for user authentication using Deep CNN-BiLSTM network. Furthermore, we proposed Bayes theorem based trust score to evaluate the zero trust security. This proposed framework assumes all users, devices, and applications are un-trusted which requires verification and authentication for every access request, regardless of the user's location or device. To evaluate the trust score in the zero trust security model, Bayes theorem-based trust score (Bayes-TSC) model is proposed. The performance of model is analyzed over three datasets: WISDM-HARB, HMOG, and UCI-HAR, using four metric measures: accuracy, equal error rate, success rate, and authentication time. From the results, the performance of proposed framework outperforms when compared with traditional benchmark deep learning models for user authentication while protecting against unauthorized access in minimal authentication time.

Index Terms—Artificial Intelligence, Consumer Industry, Deep Learning, Security, Zero Trust.

I. INTRODUCTION

RECENT advancements in technologies have made world to become victims of connectivity with digitization. Because of increasing connection between devices and trending tools such as Internet of Things (IoT), cloud computing, and sensors within the network which exchanges information or

data across various places which results in need and importance of network security requirements [1], [2]. In today's modern world, various security concepts used in the network is based on separation between external and internal networks. The internal networks are isolated using Network Access Controls (NACs), Virtual Private Networks (VPNs), and Firewalls [3]. Different services, devices, users are trustworthy when they are inside the protected internal network. However, other devices and users who are outside will be treated as intruders. This is where the realm of trustworthy protocol or zero trust security is playing an important role that should be practiced in various consumer environment [4], [5].

These challenges were adversely promoted by zero-trust concept that is growing in recent days. In this methodology, the main idea behind this is develop no trustworthy in which each and every request or information must be validated and approved before transferring through the network. Several organizations are still depend on perimeter-based model despite of the potential ability towards zero-trust solutions for secure networking [6], [7]. However, there is a multifaceted and complex process in investing for new security approaches. This becomes more important for customers, employees, and business process to take informed decisions for their consumer based industries. Various research has focused on technical aspects of zero trust security and business oriented questions were neglected [8], [9].

The paradigm of cyber-security is known to be zero trust where it is mainly focused on protection of resources in which continuous evaluation is must before implicitly granting trust. Trustworthiness is the degree that viewed coarsely for the people who has confidence for the product or service that behaved as promised, intended, and advertised [10]. In the environment of Zero-trust, continuous authorization and verification are required for users while they access to the resources of enterprise. The Zero Trust Architecture (ZTA) helps in improving analytics and viability across various enterprise network. An Ericom software survey has detailed that 83% out of 1300 risk and security specialists have responded and thus the zero trust is agreed and implemented the solutions for their enterprise [11]–[13].

Transition towards ZTA will be an questionable task and also challenging to understand and long journey to have proper use. The migration to Zero Trust ecosystem is an challenging and have several barriers for the enterprise industries [14]. It is due to lack of concrete frameworks and industry standards that can efficiently implement this methodology in different enterprises. The requirements for infrastructure must be un-

Senthil Murugan Nagarajan is with Department of Mathematics, Université du Luxembourg, Maison du Nombre 6, Avenue de la Fonte, L-4365 Esch-Sur-Alzette, Luxembourg (e-mail: senthil.nagarajan@uni.lu)

* (Corresponding Author) Ganesh Gopal Devarajan is with Department of Computer Science and Engineering, Faculty of Engineering and Technology, SRM Institute of Science and Technology, Delhi - NCR Campus, Delhi - Meerut Road, Modinagar, Ghaziabad, Uttar Pradesh - 201204, India (e-mail: dganeshgopal@gmail.com)

Suresh Thangakrishnan M is with Department of Computer Science and Engineering, Einstein college of Engineering, Tirunelveli, Tamil Nadu 627012, India (e-mail: suresh.nellai@gmail.com)

Ramana T V is with Department of Computer Science and Engineering, Jain University, Bangalore, Karnataka, India (e-mail: Venkataramana.t@gmail.com)

Ali Kashif Bashir is with Department of Computing and Mathematics, Manchester Metropolitan University, UK, and with Woxsen School of Business, Woxsen University, India, and with Department of Computer Science and Mathematics, Lebanese American University, Beirut, Lebanon (email: dr.alikashif.b@ieee.org)

Ahmad Ali AlZubi is with Computer Science Department, Community College, King Saud University, P.O. Box 28095, Riyadh 11437, Saudi Arabia (email: aalzubi@ksu.edu.sa)

derstood clearly before migrating to ZTA as various standards of Artificial Intelligence (AI) and IT system interoperability and compatibility is different. More applicability towards AI and zero trust security is integrated to develop an reliable architecture to improve trust in enterprise industries [12], [15]. The main contributions of this research is summarized below:

- User authentication is analyzed using DeepCNN BiLSTM network based on smartphone sensor data.
- Furthermore, the trust-score of zero trust security solution is evaluated using Bayes theorem.

In this research, we proposed AI-enabled deep learning model based zero trust security (AI-DL-XTS) framework for verification and authentication for devices, users, and applications for every access request. We use smartphone sensor data for user authentication using Deep-CNN-BiLSTM network. Furthermore, we proposed Bayes theorem based trust score to evaluate the zero trust security.

II. RELATED WORKS

Organizational operations have been changed these days with increase in work from home popularity where devices and users need dynamic access to various applications and data from the outside to connect with internal network of certain consumer based industries, organizations, and much more [1]. Syed et al. [16] presented a extensive survey about zero trust and critical infrastructure risk management. Authors described the role of access control and authentication of zero trust architectures in different scenarios. Authors also discussed the various challenges associated with access control schemes, software-defined perimeter, contemporary authentication schemes, micro-segmentation approaches, and risk computation techniques which affect the zero trust implementation.

Eidle et al. [17] presented Observe, Orient, Decide, Act (OODA) framework implementation based on experimental test-bed results of plane feedback with automatic control. In their model, automated threat response with identity management and combined with packet-based authentication of trust levels towards eight distinct network. Poppo et al. [18] presented two main frameworks for supply chain management on zero trust security. First one authors mentioned as calculative trust in which economics transaction cost is associated closely and second is relational-trust in which sociological theories were closely aligned. Sedjelmaci et al. [19] proposed hybrid model for security framework which combined of machine learning and security experts for protecting the edge computing network from unknown and known attacks by minimizing false alarm rate.

Grzonkowski and Corcoran [20] proposed authentication framework by user centric approach for home networks. Authors used zero knowledge proof authentication scheme into the cloud infrastructure by allowing users to transfer their service temporarily within a trusted environment. Furthermore, sophisticated services and sharing of personal content is enabled over convenient TCP/IP protocol by using this approach. Wan et al. [21] presented zero knowledge proof with high efficiency for data authentication by extending the previous zk-SNARK scheme. Authors developed off-chain data based on

zero-knowledge authenticated and zk-AuthFeed for achieving both authenticity and privacy for blockchain enabled DApps.

Ran [22] presented deep Content Disarm and Reconstruction (CDR) methodology based on zero-trust in which the validation is first executed using the CDR and prevention rate with effect of disarming were presented and measured. Authors used well-know dataset for analyzing the performance of DeepCDR model where they proved that reconstruction file is functional and usable. Baozhan et al. [23] proposed a protection and security awareness system for 5G-based healthcare platform using zero-trust architecture. Four key dimensions were considers in 5G-based healthcare such as terminals, users, and much more for constructing trust-able dynamic access control models.

Zhang et al. [24] realized the intelligent emergency analysis, management and trustworthy using emergent semantic based information centric-fog system. They designed efficient dissemination network for emergency information and aggregating. Furthermore, authors filtered fake contents using semantic based trustworthy routing scheme. Abou-Nassar et al. [25] come up with the solution where semantic gaps is reduced by the Indirect Trust Inference System (ITIS) and budget authentication by smart contract and enhanced estimation of Trustworthy Factor (TF) using network edges and node with the help of proposed Blockchain Decentralized Interoperable Trust framework (DIT) for IoT zones.

Hosney et al. [26] proposed an alternative solution based on machine learning algorithms for saving time and increase efficiency for maintaining security posture with less human intervention. In this mode, configured policies and information about security feeds are enforced and maintain zero-trust network policies. Kant and Johannsen [27] used AI based security features in small and medium sized companies (SMEs) and concluded the potential impact of security level is surveyed. Saleem et al. [28] proposed zero-trust security framework based on rich model for verification of trust by involving federated learning in the cloud environments.

Tiwari et al. [29] demonstrated secure data aggregation without using bi-linear groups with the support of verifiable federated learning method to address malicious third-party aggregation. Patil et al. [30] proposed a scheme based on member reputation and member list chain based association (MLC-R b A) for changing the type of authenticated data. Authors also proposed two necessary functions for root authentication without using external trust for hierarchical trust model in which revoked members were controlled without causing inconvenience to user. Kumar et al. [31] introduced authentication and key key agreement (AKA) and AI based Intrusion Detection System (IDS) for analyzing computation cost. However, authors proposed explainable AI based on blockchain for securing consumer applications in smart cities. Shunji et al. [32] computed situation values by integrating three factors such as IoT-threat, IoT-attack, and IoT-attack probabilities. Then authors applied proposed model to decompose sequences with the help of variational mode decomposition (VMD) and developed CNN-BiLSTM model for predicting sub-sequences.

III. PROPOSED METHODOLOGY

The growth of recent technologies made consumer electronics to reach millions of people and increased in usage for daily life style. Such consumer electronic devices like smart phones, banking transactions, smart environment, and much more made ease of usage and routine work life balance which also lead consumers to obtain different advantages. However, this flexibility also leads to severe cyber attacks as these devices are not always protected from firewall devices. To enable security against internet-enabled consumer electronics, we proposed an AI-based deep-learning enabled zero-trust security (AI-DL-XTS) model that use deep-learning techniques for biometric authentication to detect authorized smartphone user. Smartphones are equipped with various sensors that sense user touch during a different activities like reading, writing, eating, sitting, walking, etc. based on the sensor data, the proposed deep learning model detects user authentication. The zero trust security model uses DL method outcomes and other networking activities to allow or deny the user request. Fig. 1 represents the proposed AL-DL-XTS model architecture for detecting cyber attacks in consumer electronics.

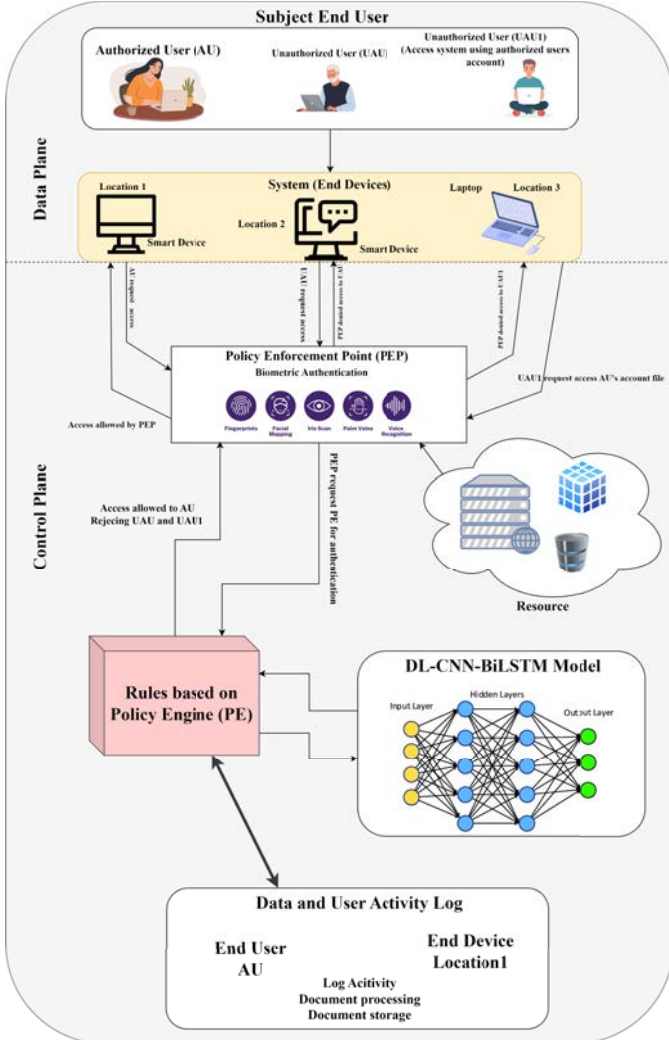


Fig. 1: Proposed AL-DL-XTS Framework.

Zero Trust Security model: Here, it assumes by default that no user, device, or network is trusted and all resources must be secured and continuously authenticated. In the context of consumer electronics, such as smartphones and laptops, implementing a Zero Trust security model requires several components working together, including a policy enforcement point, policy engine, data store, and deep learning-based trust engine for user authentication using various factors such as smartphone, IP address, device, and location.

Policy Enforcement Point (PEP): It is the component that enforces the security policies in the Zero Trust model. It sits at the point of access to resources and ensures that only authenticated and authorized users can access them.

Policy Engine: It defines the security policies that the PEP enforces. It determines the criteria for granting or denying access to resources based on the user's location, device, IP address, and behavior patterns.

Data Storage: The data store contains information about the users, devices, and resources in the system. The trust engine uses it to build user profiles, establish baselines for normal behavior, and store authentication data.

DL-CNN BiLSTM Model: We proposed a deep learning-based CNN-BiLSTM (Deep-CNN-BiLSTM) model for user authentication that uses smartphone-based sensor data for typical user patterns and behavior. The proposed Deep-CNN-BiLSTM consists of deep learning-based Convolutional Neural Networks (Deep-CNN), which helps in the extraction of features and Bidirectional Long Short-Term Memory (BiLSTM) network that is used for extracting temporal dynamic elements from the input data. The trust engine is a deep learning-based system that continuously evaluates user behavior and makes authentication decisions based on multiple factors. It analyzes patterns and behavior over time to build a user profile and establish a baseline of "normal" behavior for that user.

The proposed model in Fig. 1 outlines a scenario where an authenticated user (AU) is accessing her account file using her smartphone device, and a deep learning-enabled Zero Trust model is used to verify her location, internet connection, and behavior patterns to authenticate her. The model also checks her authorization to access the specific account file and grants her access if authorized. When an unauthorized user (UAU) gains access to Alice's device and tries to access the account file, the model detects a deviation from Alice's typical behavior patterns and blocks Bob's access. Similarly, when an unauthorized user (UAU1) tries to access the account file from a different location and internet address using an other device, the model analyzes the context of the access request and blocks John's access as his behavior patterns do not match Alice's typical behavior. The proposed model combines authentication, authorization, threat detection, and contextual analysis to enhance user authentication security measures.

Let $Sdata_x$ be input to the Deep-CNN-BiLSTM model that gathers from smartphone sensor reading, Θ the learning parameter, and $Deep_y$ be the target output. Equation 1 represents the formula for Deep-CNN-BiLSTM model.

$$Deep_y = Softmax(Sdata_x; \Theta) \quad (1)$$

The softmax function is used classifier that uses features extracted from CNN and Bi-CNN-LSTM network. The Deep-CNN component applies a series of convolutional filters to the smartphone sensor input data to extract relevant features. Equation 2 represents the mathematical expression for feature extraction.

$$Con_{cf} = ReLU(W_{cf} * x + b_{cf}) \quad (2)$$

Where, W_{cf} and b_{cf} represents the convolutional weighted filter and bias term, and ReLU is the rectilinear activation function and is expressed as $ReLU(x)=\max(0,x)$. The output Con_{cf} of the CNN component represent a set of feature maps.

To extract temporal characteristics of smartphone sensor data, we apply the BiCNN-LSTM network over a convolutional feature set Con_{cf} . BiCNN-LSTM network is a bidirectional CNN-LSTM network that extracts features from two networks in two directions: forward network in the forward direction with learning parameter Θ_{lstm}^{FD} and backward network in the backward direction with model learning parameter Θ_{lstm}^{BK} . The output of forward and backward CNN-LSTM networks are given in (3) and (4).

Let $BiLSTM_{h_{fd}}$ and $BiLSTM_{h_{bk}}$ be the output of forward and backward CNN-LSTM networks, respectively.

$$BiLSTM_{h_{fd}} = BiLSTM_{h_{fd}}(Con_{cf}; \Theta_{lstm}^{FD}) \quad (3)$$

$$BiLSTM_{h_{bk}} = BiLSTM_{h_{bk}}(Con_{cf}; \Theta_{lstm}^{BK}) \quad (4)$$

Where, $BiLSTM_{h_{fd}}$ and $BiLSTM_{h_{bk}}$ are the functions implemented by the BiCNN-LSTM network in the forward and backward directions. The output of the forward network $BiLSTM_{h_{fd}}$ and backward network $BiLSTM_{h_{bk}}$ is concatenated to produce the final hidden output state of the BiCNN-LSTM network, and mathematically, it is expressed in (5).

$$BiLSTM_{h_o} = \tanh(W_{h_o} * [BiLSTM_{h_{fd}} \oplus BiLSTM_{h_{bk}}] + b_{h_o}) \quad (5)$$

Where, $[BiLSTM_{h_{fd}} \oplus BiLSTM_{h_{bk}}]$ represents the concatenated hidden state output of the forward and backward BiCNN-LSTM, W_{h_o} is the weight matrix, b_{h_o} is the bias term, and \tanh is the tangent activation function.

The concatenated output of the final hidden output state of the BiCNN-LSTM network then passes through a fully connected layer that generates output $Deep_{FCO}$, and can be expressed mathematically as per (6).

$$Deep_{FCO} = W_{FC} * BiLSTM_{h_o} + b_{FC} \quad (6)$$

Where, W_{FC} and b_{FC} are weight matrix and bias term applied at fully connected layer, and $BiLSTM_{h_o}$ is the final hidden output state of the BiCNN-LSTM network. The softmax classifier is used for user authentication classification and is expressed in (7).

$$Deep_y = Softmax(Deep_{FCO}) \quad (7)$$

During the training phase, the model parameters (weights and biases) are learned by minimizing the loss function using

an optimization algorithm such as Stochastic Gradient Descent (SGD) or Adam. The loss function can be represented as per (8).

$$Loss = - \sum Deep_{y_i} * \log(Deep'_{y_i}) - (1 - Deep_{y_i}) * \log(Deep'_{y_i}) \quad (8)$$

Where, $Deep_{y_i}$ is the ground truth label of the sensor input data ("authenticate" or "unauthenticated"), $Deep'_{y_i}$ is the predicted probability of the sensor input data belonging to the authenticated user, and a log is the natural logarithm. Main goal of this optimization algorithm is to minimize the loss function loss value by updating the model parameters iteratively.

Bayes theorem-based trust score (Bayes-TSC) Process: The Zero Trust security model uses a trust score to determine whether a device, user, or network should be granted access to a resource or not. The trust score is calculated using a mathematical equation based on Bayes' theorem. The decision to grant or deny access can be made based on a threshold probability. For example, if the threshold probability is set to 0.7, access will be granted if Trust score > 0.7 , and denied if Trust score < 0.7 . The equation can be expressed as per (9).

$$\begin{aligned} Trust\ Score &= P(Req|U_{ID}, D_{ID}, Net_{Loc}, IP_{Add}, time_s) \\ &= \omega_1 * P(U_{ID}|Req) + \omega_2 * P(D_{ID}|Req) + \omega_3 * P(Net_{Loc}|Req) \\ &\quad + \omega_4 * P(IP_{Add}|Req) + \omega_5 * P(time_s|Req) \end{aligned} \quad (9)$$

Where, Req is the access request, U_{ID} is the user identity, D_{ID} is the device identity, Net_{Loc} is the network location, IP_{Add} is the IP address, and $time_s$ is the time of the access request. To calculate the probability of granting access (Req), given the user identity (U_{ID}), device identity (D_{ID}), network location (Net_{Loc}), IP Address (IP_{Add}), and time ($time_s$), we need to consider conditional probability $P(En|Req)$ is given in (10).

$$P(En|Req) = P(Req|En) * P(En) / P(Req) \quad (10)$$

Where, $P(En|Req)$ is the probability of the Entity (En) being valid given the access request (Req), $P(Req|En)$ is the probability of observing the access request (Req) given that the entity (En) is valid, $P(En)$ is the prior probability of the Entity (En) being valid. $P(Req)$ is the probability of observing the access request (A); $Entity\ En = \{useridentity(B), deviceidentity(C), networkklocation(D)\}, \{Ippaddress(E), timeoftheaccessrequest(F)\}$. The pseudo-code for proposed model is depicted in algorithm 1.

IV. RESULTS AND DISCUSSION

This section typically describes the experiments conducted to evaluate the performance of the proposed deep learning-based zero trust security (DL-XTS) model. Furthermore, we proposed a Deep-CNN-BiLSTM model for continuous user authentication using smartphone sensing data. Our experiments were conducted on three benchmark datasets: WISDM-HARB, HMOG, and UCI-HAR. To evaluate the performance of the proposed Deep-CNN-BiLSTM model, we used three

Algorithm 1 Proposed DL-TE Algorithm

Input: Smartphone sensor reading, Θ is the learning parameter, $Sdata_x$ is the input data

Output: $Deep_y$ is target output

Apply convolution filter for $Sdata_x$ using $Conf_f = ReLU(W_{cf} * x + b_{cf})$

if device type=smartphone **then**

$Y_l = Deep - CNN - BiLSTM(Sdata, \Theta)$

Compute $P(En|A) = P(En|Req) = P(Req|En) * P(En)/P(Req)$ //for each Entity

Compute Trust Score = $P(Req|UID, DID, NetLoc, IPAdd, time_s) = \omega_1 * P(UID|Req) + \omega_2 * P(DID|Req) + \omega_3 * P(NetLoc|Req) + \omega_4 * P(IPAdd|Req) + \omega_5 * P(time_s|Req)$

else

Compute $P(En|A) = P(En|Req) = P(Req|En) * P(En)/P(Req)$ //foreach Entity

Compute Trust Score = $P(Req|DID, NetLoc, IPAdd, time_s) = \omega_1 * P(DID|Req) + \omega_2 * P(NetLoc|Req) + \omega_3 * P(IPAdd|Req) + \omega_4 * P(time_s|Req)$

end if

if trust score ≥ 0.7 **then**

UserAut=Authenticated

else

UserAut=Unauthenticated

end if

Return UserAut

authentication metrics: confusion matrix, accuracy, and Equal Error Rate (EER). To assess the effectiveness of the proposed DL-XTS model, we used success rate as a metric measure.

The proposed user authentication Deep-CNN-BiLSTM model is evaluated using error rate-based metrics, such as false rejection error rate (FRER) and false acceptance error rate (FAER). FRER and FAER increase and decrease, respectively, as sensitivity rises. The equal error rate (EER) represents the sensitivity point where FRR and FAR are equal. Metrics such as FAER, FRER, accuracy, and EER are calculated using formulas to determine authentication failures. Additionally, accuracy and confusion matrices are used to evaluate the classification performance of the authentication scheme.

FAER represents the probability of categorizing a pattern as "Authenticate" if it does not belong to it and mathematically it is expressed as (11).

$$FAER = \frac{FAV}{FAV + TRV} \quad (11)$$

FRER represents the probability of not classifying a pattern as "Authenticate" if it does and is expressed mathematically as per (12).

$$FRER = \frac{FRV}{FRV + TAV} \quad (12)$$

Accuracy measures the likelihood of a pattern classifying correctly and is expressed mathematically as (13).

$$Accuracy = ((TAV + TRV)) / ((TAV + TRV + FAV + FRV)) \quad (13)$$

EER is the error rate obtained by equalizing FAER and FRER using the system's detection threshold. The EER is calculated using the formula: $EER = \frac{FAER + FRER}{2}$, where $|FAER + FRER|$ is the smallest value.

A. Dataset Description

The UCI-HAR dataset [33], also known as the "UCI Human Activity Recognition Using Smartphones Dataset," is a dataset collected from smartphone sensors that can be used to recognize human activities such as walking, standing, and sitting. The dataset contains 10,299 instances of 561 features extracted from accelerometer and gyroscope signals collected from 30 subjects while performing six activities. The dataset is commonly used for machine learning, data mining, and activity recognition research.

The WISDM-HAR dataset [34], also known as the "Wireless Sensor Data Mining for Human Activity Recognition dataset," is a dataset collected from an Android phone's accelerometer and gyroscope sensors that can be used to recognize human activities such as walking, jogging, and sitting. The dataset contains 1,098,207 instances of three features (x, y, and z acceleration) collected from 29 subjects while they performed six activities. The dataset is commonly used for research in machine learning, data mining, and activity recognition.

The HMOG dataset [35], also known as the "Human Motion Database," is a dataset collected from an inertial measurement unit (IMU) that can be used to recognize human activities such as walking, running, and jumping. The dataset contains data collected from 11 subjects while they performed various activities. The dataset includes a total of 12,960 instances of 10 features extracted from the IMU sensors. The dataset is commonly used for machine learning, data mining, and activity recognition research.

V. EXPERIMENTAL RESULTS

This study evaluated the proposed Deep-CNN-BiLSTM authentication framework against basic deep learning algorithms using three public datasets: UCI-HAR, WISDM-HARB, and HMOG. The following subsections provide the experimental observations of these deep learning methods trained on mobile sensing data on various datasets.

A. UCI-HAR Dataset:

Figure 2 demonstrates the authentication performance comparison of proposed work with different models such as Convolutional Neural Network (CNN), CNN-LSTM, Long Short Term Memory (LSTM), Deep Neural Network (DNN), ensemble based deep federated learning (E-DFL), and cascaded federated deep learning (C-FDL) using UCI HAR dataset. For performance evaluation for this work, we considered the UCI HAR dataset comprises smartphone sensor data collected from 35 volunteers. The accuracy and EER (Equal Error Rate) are the metrics assessed. As shown in Fig. 2, the Deep-CNN-BiLSTM based PEP model outperforms existing models such as CNN, CNN-LSTM, LSTM, DNN, E-DFL, and C-FDL in

terms of accuracy and EER across all six activities (walking, walking upstairs, walking downstairs, sitting, standing, and laying). The Deep-CNN-BiLSTM model achieves an average accuracy of 94.4% ($\pm 8.432\%$) and an average EER of 5.16% ($\pm 8.532\%$). On the other hand, the CNN model obtains an average accuracy of 96.20% ($\pm 4.603\%$) and an average EER of 5.27% ($\pm 7.034\%$). In comparison, the CNN-LSTM model achieves an average accuracy of 88.60% ($\pm 11.593\%$) and an average EER of 10.41% ($\pm 14.874\%$). However, E-DFL and C-FDL performs better and close to proposed method. Consequently, the Deep-CNN-BiLSTM model performs better than the CNN and CNN-LSTM models for the given dataset. Proposed Deep-CNN-BiLSTM model in Fig. 2 outperforms current baseline deep learning models in average accuracy and EER across all activity patterns using the UCI-HAR dataset, which involves sensor data from 30 volunteers engaging in six activities.

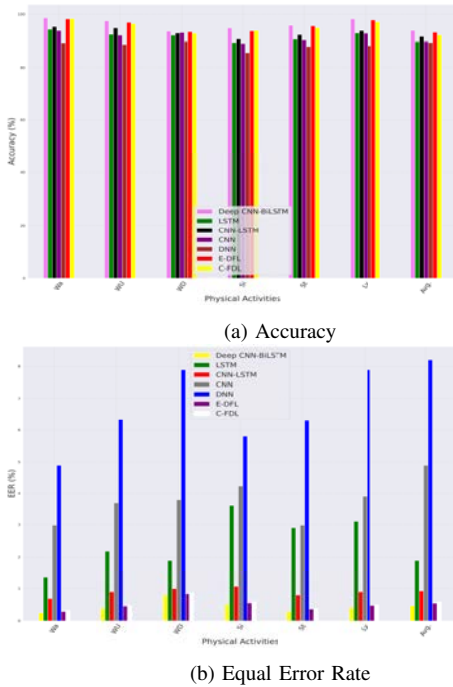


Fig. 2: Result Analysis for Different Physical Activities on UCI-HAR Dataset

B. WISDM-HARB Dataset

For WISDM-HARB dataset, 44 individuals that encompasses mobile sensor data performing 18 physical activities are considered. The dataset was evaluated using three deep learning models: CNN, CNN-LSTM, and Deep-CNN-BiLSTM. The authentication performance metrics for each of the 18 physical activities were computed, including Accuracy and Equal Error Rate (EER). Based on Fig. 3, the Deep-CNN-BiLSTM model exhibited the highest accuracy of 99.81% ($\pm 0.529\%$) for sitting, while the lowest EER of 0.19% ($\pm 1.714\%$) was obtained for clapping by the same model. Results indicate that the proposed model outperforms the other models for most physical activities, followed by E-DFL, C-FDL, and CNN-LSTM model, and then the CNN model.

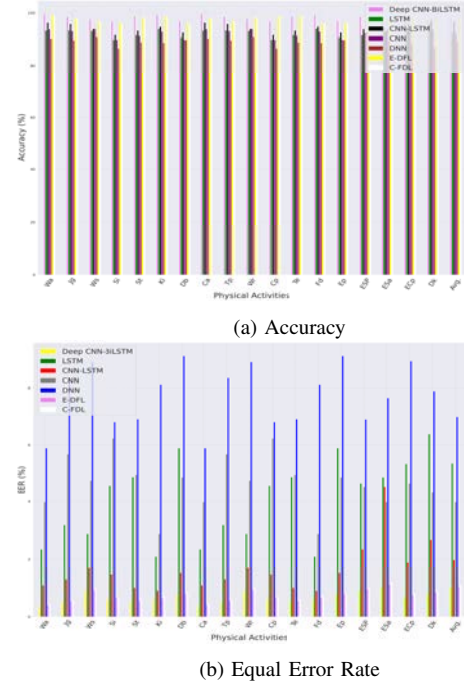


Fig. 3: Result Analysis for Different Physical Activities on WISDM-HARB Dataset

C. HMOG Dataset

Fig. 4 depicts the authentication performance metrics of CNN, CNN-LSTM, Deep-CNN-BiLSTM, and Deep-CNN-BiLSTM models for the HMOG dataset, which consists of sensor data collected from 100 smartphones for six different activities. Accuracy and equal error rate (EER) are the reported metrics. For reading, while sitting, all three models achieved accuracy above 99.45%, with Deep-CNN-BiLSTM having the highest accuracy of 99.64% and the lowest EER of 0.46%. Similarly, all three models showed an accuracy above 99.50% for reading while walking, with Deep-CNN-BiLSTM again having the highest accuracy of 99.62% and the lowest EER of 0.38%. For writing, while sitting, all models achieved very high accuracy, with Deep-CNN-BiLSTM having the highest accuracy of 99.99% and the lowest EER of 0.01%. However, for writing while walking, the accuracy of all models was slightly lower, with Deep-CNN-BiLSTM having the highest accuracy of 99.34% and the lowest EER of 1.02%. For the activity of using a map while sitting, all models obtained high accuracy above 98.77%, with Deep-CNN-BiLSTM having the highest accuracy of 99.99% and the lowest EER of 0.01%. For using a map while walking, all models achieved accuracy above 99.08%, with Deep-CNN-BiLSTM having the highest accuracy of 99.55% and the lowest EER of 0.73%. Overall, the results suggest that Deep-CNN-BiLSTM outperformed the other models regarding accuracy and EER for most activities in the HMOG dataset.

D. Success Rate

Success rate states how the proposed model correctly recognizes the authenticated user and allows access permission to request files and is mathematically expressed in Eqn. 14:

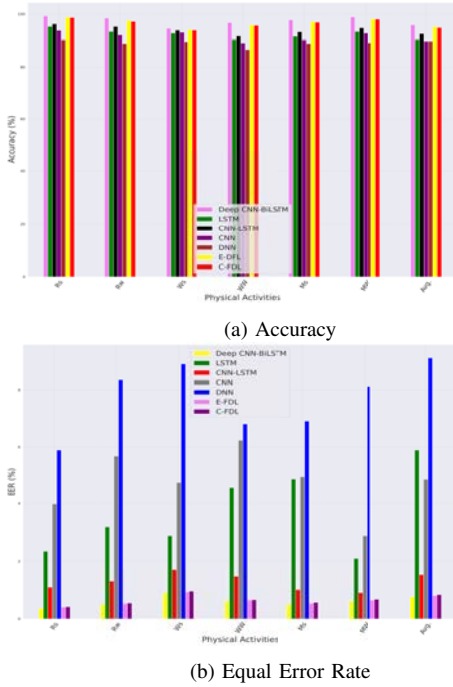


Fig. 4: Result Analysis for Different Physical Activities on HMOG Dataset

$$SR = \left(\frac{NSA}{TNA} \right) * 100 \quad (14)$$

Where, SR is the success rate, NSA is the Number of Successful Authentication, and TNA is the Total Number of Authentication Attempts.

Figure 5(a) represents the success rate for the proposed AI-DL-XTS and non-AI-DL-XTS models. The result showed that the proposed AI-DL-XTS model has a higher success rate than the non-AI-DL-XTS model (MEC without ZTS). The success rates for the AI-DL-XTS model were 78.5% to 81.5% for different user node configurations, while the success rates for the non-AI-DL-XTS model were 39% to 61%. This indicates that the AI-DL-XTS model is more effective at accurately authenticating users.

Authentication time is the time taken by the model to authenticate a user and is expressed in Eqn. 15:

$$AT = \left(\frac{TTAU}{Number\ of\ Users} \right) ms \quad (15)$$

Where, AT is the authentication time and TTAU is the Total Time Taken to Authenticate All Users.

Figure 5 (b) shows the outcome of authentication time. It is observed that in terms of authentication time, the proposed AI-DL-XTS model also performs better. The proposed AI-DL-XTS model authenticates all the user nodes between 10 to 100 in 80ms to 81 ms, while the non-AI-DL-XTS model takes 90.5 to 91.5 ms. From the result, it was suggested that the AI-DL-XTS model is faster at authenticating users than the non-AI-DL-XTS model.

The proposed zero-trust security solution not only stands out in terms of technical innovation but, more importantly, offers

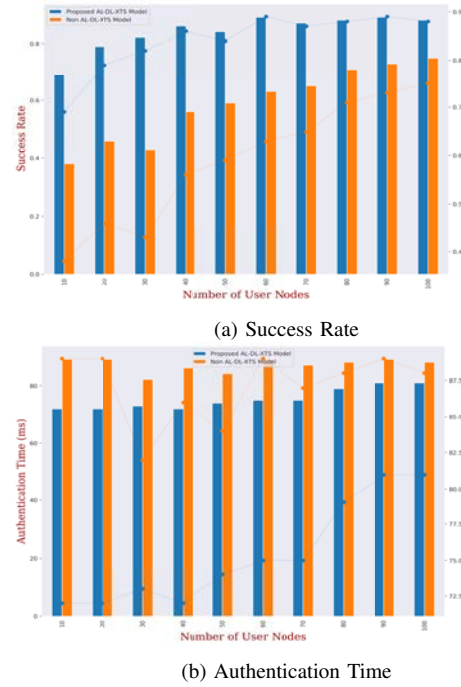


Fig. 5: Success Rate and Authentication Time-based Analysis for Proposed Model

tangible benefits for end-users. Unlike traditional approaches, our framework prioritizes user-centric security by reduced false positives and increased accuracy. This work focused in ensuring a seamless and secure digital experience for consumers. In the realm of cyber-security, the user experience is paramount. This work distinguishes itself by placing a strong emphasis on enhancing the overall user experience. By minimal authentication hassles and adaptive security which ensures that consumers can stay secure. Furthermore, leverages threat intelligence data to proactively update security policies and block access to known malicious entities. The proposed algorithm can classify and monitor sensitive data, ensuring that proper access controls are in place and sensitive information is not compromised.

VI. CONCLUSION

With the increasing use of consumer electronics, including smartphones and laptops, in our daily lives, the threat of cyber-attacks is also increasing. In this regard, we have proposed an AI-based deep learning-enabled zero-trust security (AI-DL-XTS) model that uses deep learning techniques Deep-CNN-BiLSTM for secure authentication to detect authorized smartphone users. We presented the Bayes-TSC method for trust score calculation in the zero trust security model. The proposed Deep-CNN-BiLSTM model for continuous user authentication using smartphone sensing data has been evaluated on three benchmark datasets: WISDM-HARB, HMOG, and UCI-HAR. Our experiments demonstrate that the Dee-CNN-BiLSTM model outperforms other deep learning models, namely CNN-LSTM, LSTM, DNN, E-DFL, and C-DFL in terms of accuracy and equal error rate for all six activities. The proposed AI-DL-XTS model has also shown high success

rates, providing a robust and secure solution against cyber-attacks. Future enhancements to this model can further improve its performance and extend its capabilities to various other scenarios. Furthermore, analysis based on cloud native environments for zero trust security.

VII. ACKNOWLEDGMENT

The authors thank King Saud University for funding this work through the Researchers Supporting Project number (RSP2024R395). King Saud University, Riyadh, Saudi Arabia.

REFERENCES

- [1] Y. Chen, H.-c. Hu, and G.-z. Cheng, "Design and implementation of a novel enterprise network defense system by maneuvering multi-dimensional network properties," *Frontiers of Information Technology & Electronic Engineering*, vol. 20, no. 2, pp. 238–252, 2019.
- [2] M. Wazid, A. Kumar Das, and S. Shetty, "Bsfr-sh: Blockchain-enabled security framework against ransomware attacks for smart healthcare," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 1, pp. 18–28, 2023.
- [3] J. Y. V. M. Kumar, A. K. Swain, K. Mahapatra, and S. P. M. verify, "Fortified-noc: A robust approach for trojan-resilient network-on-chips to fortify multicore-based consumer electronics," *IEEE Transactions on Consumer Electronics*, vol. 68, no. 1, pp. 57–68, 2022.
- [4] B.-C. Chifor, S.-C. Arseni, I. Matei, and I. Bica, "Security-oriented framework for internet of things smart-home applications," in *2019 22nd International Conference on Control Systems and Computer Science (CSCS)*. IEEE, 2019, pp. 146–153.
- [5] A. Moubayed, A. Refaey, and A. Shami, "Software-defined perimeter (sdp): State of the art secure solution for modern networks," *IEEE network*, vol. 33, no. 5, pp. 226–233, 2019.
- [6] X. Yan and H. Wang, "Survey on zero-trust network security," in *Artificial Intelligence and Security: 6th International Conference, ICAIS 2020, Hohhot, China, July 17–20, 2020, Proceedings, Part 16*. Springer, 2020, pp. 50–60.
- [7] C. Buck, C. Olenberger, A. Schweizer, F. Völter, and T. Eymann, "Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust," *Computers & Security*, vol. 110, p. 102436, 2021.
- [8] E. Weishäupl, E. Yasasin, and G. Schryen, "Information security investments: An exploratory multiple case study on decision-making, evaluation and learning," *Computers & Security*, vol. 77, pp. 807–823, 2018.
- [9] D. Xu, C. Peng, W. Wang, H. Liu, S. A. Shaikh, and Y. Tian, "Privacy-preserving dynamic multi-keyword ranked search scheme in multi-user settings," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 4, pp. 890–901, 2023.
- [10] P. Laplante and J. Voas, "Zero-trust artificial intelligence?" *Computer*, vol. 55, no. 02, pp. 10–12, 2022.
- [11] M. Campbell, "Beyond zero trust: Trust is a vulnerability," *Computer*, vol. 53, no. 10, pp. 110–113, 2020.
- [12] P. Phiayura and S. Teerakanok, "A comprehensive framework for migrating to zero trust architecture," *IEEE Access*, vol. 11, pp. 19487–19511, 2023.
- [13] N. Vashistha, M. M. Hossain, M. R. Shahriar, F. Farahmandi, F. Rahman, and M. M. Tehranipoor, "echain: A blockchain-enabled ecosystem for electronic device authenticity verification," *IEEE Transactions on Consumer Electronics*, vol. 68, no. 1, pp. 23–37, 2022.
- [14] J. Chen, J. Wu, H. Liang, S. Mumtaz, J. Li, K. Konstantin, A. K. Bashir, and R. Nawaz, "Collaborative trust blockchain based unbiased control transfer mechanism for industrial automation," *IEEE Transactions on Industry Applications*, vol. 56, no. 4, pp. 4478–4488, 2020.
- [15] Z. A. Collier and J. Sarkis, "The zero trust supply chain: Managing supply chain risk in the absence of trust," *International Journal of Production Research*, vol. 59, no. 11, pp. 3430–3445, 2021.
- [16] N. F. Syed, S. W. Shah, A. Shaghghi, A. Anwar, Z. Baig, and R. Doss, "Zero trust architecture (zta): A comprehensive survey," *IEEE Access*, vol. 10, pp. 57143–57179, 2022.
- [17] D. Eidle, S. Y. Ni, C. DeCusatis, and A. Sager, "Autonomic security for zero trust networks," in *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, 2017, pp. 288–293.
- [18] L. Poppo, K. Z. Zhou, and J. J. Li, "When can you trust "trust"? calculative trust, relational trust, and supplier performance," *Strategic management journal*, vol. 37, no. 4, pp. 724–741, 2016.
- [19] H. Sedjelmaci, S.-M. Senouci, N. Ansari, and A. Boualouache, "A trusted hybrid learning approach to secure edge computing," *IEEE Consumer Electronics Magazine*, vol. 11, no. 3, pp. 30–37, 2022.
- [20] S. Grzonkowski and P. M. Corcoran, "Sharing cloud services: user authentication for social enhancement of home networking," *IEEE Transactions on Consumer Electronics*, vol. 57, no. 3, pp. 1424–1432, 2011.
- [21] Z. Wan, Y. Zhou, and K. Ren, "zk-authfeed: Protecting data feed to smart contracts with authenticated zero knowledge proof," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 2, pp. 1335–1347, 2023.
- [22] R. Dubin, "Content disarm and reconstruction of rtf files a zero file trust methodology," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 1461–1472, 2023.
- [23] B. Chen, S. Qiao, J. Zhao, D. Liu, X. Shi, M. Lyu, H. Chen, H. Lu, and Y. Zhai, "A security awareness and protection system for 5g smart healthcare based on zero-trust architecture," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10248–10263, 2021.
- [24] Q. Zhang, J. Wu, M. Zanella, W. Yang, A. K. Bashir, and W. Fornaciari, "Sema-iiovt: Emergent semantic-based trustworthy information-centric fog system and testbed for intelligent internet of vehicles," *IEEE Consumer Electronics Magazine*, vol. 12, no. 1, pp. 70–79, 2023.
- [25] E. M. Abou-Nassar, A. M. Iliyasa, P. M. El-Kafrawy, O.-Y. Song, A. K. Bashir, and A. A. A. El-Latif, "Distrust chain: Towards blockchain-based trust models for sustainable healthcare iot systems," *IEEE Access*, vol. 8, pp. 111223–111238, 2020.
- [26] E. S. Hosney, I. T. A. Halim, and A. H. Yousef, "An artificial intelligence approach for deploying zero trust architecture (zta)," in *2022 5th International Conference on Computing and Informatics (ICCI)*. IEEE, 2022, pp. 343–350.
- [27] D. Kant and A. Johannsen, "Evaluation of ai-based use cases for enhancing the cyber security defense of small and medium-sized companies (smes)," *Electronic Imaging*, vol. 34, no. 3, p. 387, 2022.
- [28] M. Saleem, M. Warsi, and S. Islam, "Secure information processing for multimedia forensics using zero-trust security model for large scale data analytics in saas cloud computing environment," *Journal of Information Security and Applications*, vol. 72, p. 103389, 2023.
- [29] P. Tiwari, A. Lakhan, R. H. Jhaveri, and T.-M. Grønli, "Consumer-centric internet of medical things for cyborg applications based on federated reinforcement learning," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 4, pp. 756–764, 2023.
- [30] V. C. Patil and S. Kundu, "Realizing robust, lightweight strong pufs for securing smart grids," *IEEE Transactions on Consumer Electronics*, vol. 68, no. 1, pp. 5–13, 2022.
- [31] A. Kumar, G. Rathee, C. A. Kerrache, M. Bilal, and T. R. Gadkallu, "A secure architectural model using blockchain and estimated trust mechanism in electronic consumers," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 4, pp. 996–1004, 2023.
- [32] S. Itani, S. Kita, and Y. Kajikawa, "Multimodal personal ear authentication using acoustic ear feature for smartphone security," *IEEE Transactions on Consumer Electronics*, vol. 68, no. 1, pp. 77–84, 2022.
- [33] J. Reyes-Ortiz, D. Anguita, A. Ghio, L. Oneto, and P. Xavier, "Human Activity Recognition Using Smartphones," *UCI Machine Learning Repository*, 2012, DOI: <https://doi.org/10.24432/C54S4K>.
- [34] G. M. Weiss, "Wisdm smartphone and smartwatch activity and biometrics dataset," *UCI Machine Learning Repository: WISDM Smartphone and Smartwatch Activity and Biometrics Dataset Data Set*, vol. 7, pp. 133190–133202, 2019.
- [35] Z. Šitová, J. Šeděnka, Q. Yang, G. Peng, G. Zhou, P. Gasti, and K. S. Balagani, "Hmog: New behavioral biometric features for continuous authentication of smartphone users," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 877–892, 2015.