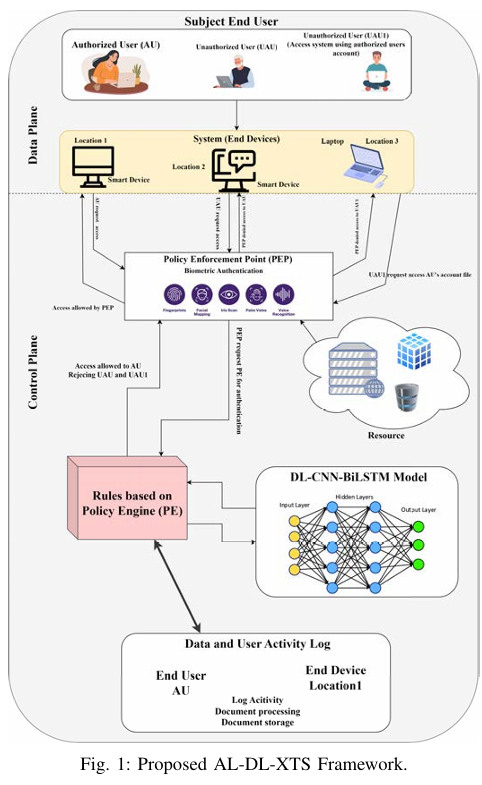
Deep CNN-BiLSTM network

Bayes Theorm 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.

AI-enabled deep learning model based zero trust security (AI-DL-XTS) framework for verification and authentication for devices, users, and applica tions for every access request.



Deepy = Softmax(Sdatax;Θ)

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

. Concf = ReLU(Wcf ∗x+bcf)

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.

Concf = ReLU(Wcf ∗x+bcf)

output state of the BiCNN LSTM network, and mathematically, it is expressed in (5).

BiLSTMho=tanh(Who∗[BiLSTMhfd ⊕BiLSTMhbk ]+bho) (5)

Where,[BiLSTMhfd ⊕ BiLSTMhbk ] represents the con catenated hidden state output of the forward and backward BiCNN-LSTM, Who is the weight matrix, bho 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 DeepFCO, and can be expressed mathematically as per (6).

DeepFCO = WFC ∗BiLSTMho+bFC (6)

Where, WFC and bFC are weight matrix and bias term applied at fully connected layer, and BiLSTMho is the f inal hidden output state of the BiCNN-LSTM network

. The softmax classifier is used for user authentication classification and is expressed in (7)

. Deepy = Softmax(DeepFCO)

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

Loss=− Deepyi∗log(Deep′ yi )−(1−Deepyi)∗log(Deep′ yi ) (8)

Where, Deepyi is the ground truth label of the sensor input data (”authenticate” or ”unauthenticated”), Deep′ yi is the predicted probability

Bayes theorem-based trust score (Bayes-TSC) Process:

Trust Score=P(Req|UID,DID,NetLoc,IPAdd,times) =ω1∗P(UID|Req)+ω2∗P(DID|Req)+ω3∗P(NetLoc|Req) +ω4∗P(IPAdd|Req)+ω5∗P(times|Req) (9)

Where, Req is the access request, UID is the user identity, DID is the device identity, NetLoc is the network location, IPAdd is the IP address, and times is the time of the access request. To calculate the probability of granting access (Req), given the user identity (UID), device identity (DID), network location (NetLoc), IP Address (IPAdd), and time (times),

we need to consider conditional probability P(En|Req) is given in (10).

P(En|Req) = P(Req|En)∗P(En)/P(Req) (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); EntityEn = {useridentity(B),deviceidentity(C),networklocation(D)}, {Ipaddress(E),timeoftheaccessrequest(F)}. The pseudo code for proposed model is depicted in algorithm 1.

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= FAV FAV +TRV (11)

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

FRER= FRV FRV +TAV . (12)

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

Accuracy=((TAV+TRV))/((TAV+TRV+FAV+FRV))

SR= NSA TNAA ∗100

Where, SR is the sucess rate, NSA is the Number of Successful Authentication, and TNAA is the Total Number of Authenti cation Attempts.

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%.

AT = TTAU Number of Users ms

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

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.