Research Proposal On

Permission Blockchain based Smart Contract utilizing Biometric Authentication as a Service

SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS OF THE DEGREE OF

DOCTOR OF PHYLOSOPHY (TECHNOLOGY)

IN

INFORMATION TECHNOLOGY

BY

MRS. GEETANJALI NILESH SAWANT

UNDER THE GUIDANCE OF

DR. VINAYAK ASHOK BHARADI

UNIVERSITY OF MUMBAI

DEPARTMENT OF INFORMATION TECHNOLOGY (PhD)

Hope Foundation's

Finolex Academy of Management and Technology

P60, P60-1, MIDC, Mirjole, Ratnagiri, Maharshtra, Pin 415639

www.famt.ac.in

Research proposal under PhD program of Mumbai University
Academic year 2019-20

1	**Faculty**	Information Technology
2	**Constituent College**	Finolex Academy of Management and Technology, Ratnagiri
3	**Department**	Information Technology
4	**Name of Research Guide**	Dr. Vinayak Ashok Bharadi
5	**Research topic**	Permission Blockchain based Smart Contract utilizing Biometric Authentication as a Service
6	**Name of research student**	Mrs. Geetanjali Nilesh Sawant
7	**Signature of Guide with Date**	
8	**Signature of Research Student with date**	
9	**Name & Signature of Research Centre Head with Date**	
10	**Table of content**	1. Introduction 2. Motivation 3. Literature review 4. Research Problem 5. Objectives 6. Methodology 7. Scope of research 8. Expected outcomes 9. Summary References

Name of the student	**: Mrs. Geetanjali Nilesh Sawant**
Course/Branch	**: Ph. D. Information Technology**
Research Title	**: Permission Blockchain based Smart Contract utilizing Biometric Authentication as a Service**
Name of the Research Guide	**: Dr. Vinayak Ashok Bharadi**
Date of Submission	**:**

Mrs. G. N. Sawant
Research Scholar

Dr. V. A. Bharadi
Guide

Head of Research Center

Principal

Table of Contents

List of Figures

List of Tables

Abbreviations and Symbols

BaaS	Biometric authentication as a Service
FNN	Feed Forward Neural Network
RNN	Recurrent Neural Network
RBFNN	Radial Basis Function Neural Network
KSONN	Kohonen Self Organizing Neural Network
MNN	Modular Neural Network
CNN	Convolutional Neural Network
DNN	Deep Neural Network
RBM	Restricted Boltzmann Machine
LSTM	Long Term Short Memory
VGG	Visual Geometry Group
PAYG	Pay As You Go
CSP	Cloud Service Provider
CU	Cloud User
VPN	Virtual Private Network
SLA	Service Level Agreement
SSL	Secure Socket Layer
AWS	Amazon Web Service
KNN	k-Nearest Neighbours
VSCC	Validation System ChainCode
CASIA	Chinese Academy of Sciences
BATH	Dataset created by University of Bath
UPOL	Dataset created at University of Palackého and Olomouc
UBIRIS	Database of Visible Wavelength Iris Images
HKPU	Dataset from Hong Kong Polytechnic University
FERET	Facial recognition technology
LFW	Labeled Faces in the Wild
MOBISIG	Online signature database
TEDLIUM	Automatic Speech Recognition dedicated corpus
GPU	Graphics Processing Unit
HLF	HyperLedger Fabric
FAR	False Acceptance Rate
FRR	False Rejection Rate
ERR	Equal Error Rate
CCR	Correct Classification Ratio
MVCC	Multi Version Concurrency Control

Abstract:

With the rapid development of the internet and mobile devices, authentication systems have been widely used in the internet service access and mobile device access for protecting user devices, contents, and accounts. Biometric recognition is advantageous over the token based authentication, since the focus is on ‘who the person is’ than ‘what person possess’. Research shows that shallow classifiers have been used by many business applications for biometric traits classification, but emerging deep learning has proved its high learning capability and predictability over the shallow classifiers. The proposed system aims to build biometric authentication performing classifier using deep learning techniques. To achieve wide appreciation, application integrity and scalability, biometric authentication system will be deployed on cloud in form of BaaS i.e. Biometric authentication as a Service. The system will be strengthened more by integrating it with permissioned blockchain. A permissioned blockchain network is highly suitable for enterprise applications that require authenticated participants, where each node in a permissioned network can be owned by different organizations and may get into the smart contract by agreeing upon certain rules and regulations which would be triggered when particular condition/s met.

Keywords : Deep learning, BaaS, blockchain, smart contract.

1. Introduction

1.1 Topic area

Biometric recognition has become a hot research area since many ways are introduced to spoof, repudiate or/and to carry out reply attacks on the available or wide spreaded systems used for biometric authentication. Biometric authentication involves physiological or behavioral or both kinds of biometric traits collection. To fulfill the evaluating criteria of authentication such as universality, uniqueness, permanence, acceptability; multimodal biometric system is preferred over unimodal biometric system. Multimodal biometric recognition system uses two or more fused biometric traits to classify a user.

Biometric authentication involves following steps:

i. Biometric traits collection: Physiological or behavioral or both kinds of biometric traits are collected and stored for feature extraction.

ii. Feature extraction: The person's uniqueness revealing features are extracted and stored for processing.

iii. Matching: The stored features are compared against the extracted features of newly sampled trait/s to obtain matching score.

iv. Classification: Based on obtained matching score, the input get classified as authenticated or not authenticated.

To perform classification, various supervised learning mechanisms are available such as K-Nearest Neighbor, Decision Tree, Bayes classification, Support Vector Machine, K-Means, Euclidean distance, etc. Since, deep learning has strong learning ability and can make better use of dataset for feature extraction, it has become one of the promising area to perform classification on supervised dataset. Neural network based deep learning technique or shallow classifier as a standalone technique or combination of both can be used to carry out classification.

The ensemble or composite classifier with reasonable accuracy and computational cost will be deployed on cloud to avail it in form of Biometric authentication as a Service (BaaS). Its not enough to have biometric authentication system be only precise and useful. The system will be strengthened more by integrating it with permissioned blockchain. Successful authentication should lead to trigger smart contract dealing with applications requiring end to end biometric recognition.

1.2 Biometric Authentication

Biometric recognition or, simply, biometrics refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics. By using biometric trait, it is possible to confirm or establish an individual's identity based on "who she is," rather than by "what she possesses" (e.g., an ID card) or "what she remembers" (e.g., a password). Biometric trait refers to the physiological or behavioral trait of a user that can identify user for a session[1]. Figure 1 represents a general architecture of biometric authentication system:

1.2.1 General architecture of biometric authentication system

General architecture of biometric authentication system is consisting of following main modules[2]:

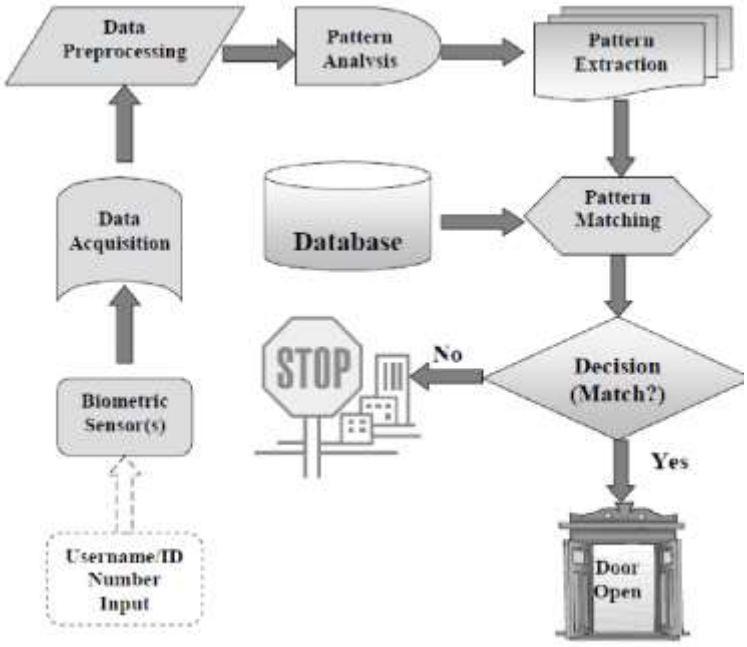

Figure1: General architecture of Biometric Authentication System

i. **Sensor module,** which captures the biometric data of an individual. An example is a fingerprint sensor that images the ridge and valley structure of a user's finger.

ii. **Feature extraction module,** in which the acquired biometric data is processed to extract a set of salient or discriminatory features. For example, the position and orientation of minutiae points (local ridge and valley singularities) in a fingerprint image are extracted in the feature extraction module of a fingerprint-based biometric system.

iii. **Matcher and Classification module** , in which the features extracted during recognition are compared against the stored templates to generate matching scores. For example, in the matching module of a fingerprint-based biometric system, the number of matching minutiae between the input and the template

fingerprint images is determined and a matching score is reported. The matcher module also encapsulates a decision making module, in which a user's claimed identity is confirmed (verification) or a user's identity is established (identification) based on the matching score.

iv. **System database module**, which is used by the biometric system to store the biometric templates of the enrolled users. The enrollment module is responsible for enrolling individuals into the biometric system database. During the enrollment phase, the biometric characteristic of an individual is first scanned by a biometric reader to produce a digital representation of the characteristic. In order to facilitate matching, the input digital representation is further processed by a feature extractor to generate a compact but expressive representation, called a template. Depending on the application, the template may be stored in the central database of the biometric system or be recorded on a smart card issued to the individual. Usually, multiple templates of an individual are stored to account for variations observed in the biometric trait and the templates in the database may be updated over time[3].

1.2.2 Biometric traits requirements

Any human physiological and/or behavioral characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

i. Universality: Each person should have the characteristic.

ii. Distinctiveness: Any two persons should be sufficiently different in terms of the characteristic.

iii. Permanence: The characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time.

iv. Collectability: The characteristic can be measured quantitatively[3].

1.2.3 Types of biometric authentication systems

Primarily, there are two types of biometric recognition system based on the number of traits used by classifier[4][5]:

i. **Unimodal biometric recognition system:** It performs authentication using the features of single biometric trait and suffers from the limitations such as universality, uniqueness, permanence, intraclass variation and inter class similarity.

ii. **Multimodal biometric recognition system:** In multimodal biometric system, more than one biometric traits are used for identity verification. It is nowadays a promising research area, that has generated expectations as an alternative in solving, among other problems, performance requirements in real applications. Multimodal biometrics fusion techniques have attracted much attention as the

supplementary information between different modalities could improve the recognition performance. Multibiometrics are fused at different levels of authentication system and these levels of fusion appear at the sensor level, at the feature level, at the match level and at the decision level [6]as shown in figure 2[7]. However it has been observed that, a biometric system that integrates information at an earlier stage of processing provides more accurate results than the systems that integrate information at a later stage, because of the availability of more richer information. Since the feature set obtained from dataset[8][9][10][11][12] contains much richer information on the source data than the matching score or the output decision of a matcher, fusion at the feature level is expected to provide better recognition performances. But, it complicates the system.

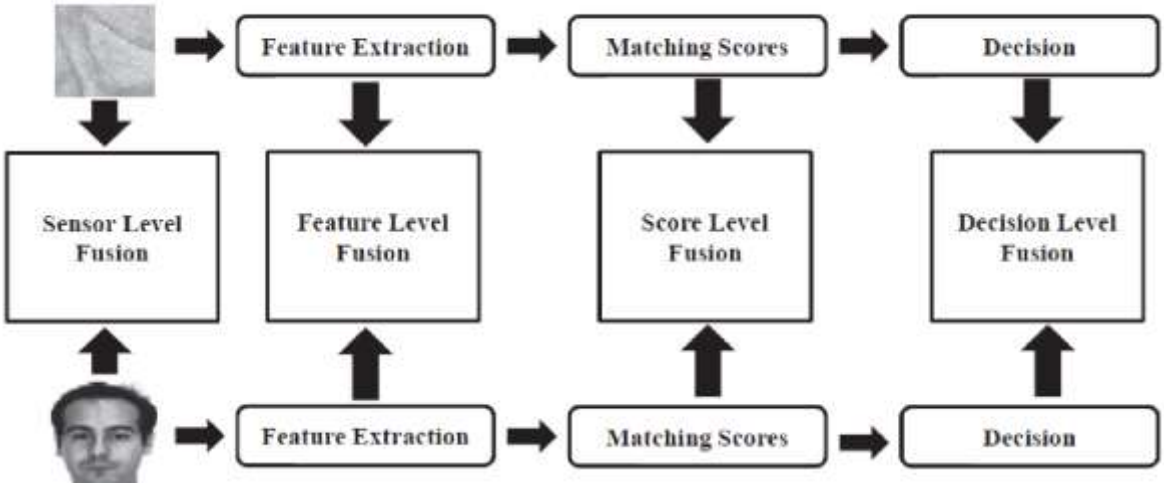

Figure 2: Fusion of biometric traits at different levels of biometric authentication system

1.3 Deep Learning

Many classification mechanism are available such as K-Nearest Neighbor, Bayes Classification, Decision tree based classification, Support Vector Machine, etc. which are termed as shallow classifiers. Since, deep learning has strong learning ability and can make better use of dataset for feature extraction, it has become one of the promising area to perform classification on supervised as well as unsupervised dataset[13]. Neural network based deep learning technique or shallow classifier as a standalone technique or combination of both are used to carry out classification[14][15].

1.3.1 Implementation of deep learning

The implementation of neural networks consists of the following steps:

i. **Acquire training and testing data set**: Bootstrap method is applied for sampling the data. Data get sampled and bifurcated into training and testing data sets. With

biometric implementation, extracted feature vector get fed as training data set and classifier get evaluated against testing data set[16].

ii. **Train the network**: Network learns and trains over the training data set and training algorithm on convergence outputs the finalized weights and bias.

iii. **Make prediction with test data**: Data from testing data set get fed to the network for classification and classified label get tested against actual class label with the application of weight and bias obtained in earlier step. With our biometric authentication system, feature vector of both i.e. the one which is already stored and another which is unknown are provided as input to the system to get result as "authenticated" or "unauthenticated".

1.3.2 Classification of Neutral Network

Neural networks are classified as[17]:

i. **Feedforward Neural Network (FNN)**: In feed forward neural network, information flows in just one direction from input to output layer (via hidden nodes if any).

ii. **Recurrent Neural Network (RNN)** : RNN can take a sequence of inputs and generate a sequence of output values as well, rendering it very useful for applications that require processing sequence of time phased input data like speech recognition, frame-by-frame video classification, etc.

iii. **Radial Basis Function Neural Network(RBFNN):** It consists of input, hidden and output layers. The hidden layer includes a radial basis function (implemented as Gaussian function) and each node represents a cluster center. The network learns to designate the input to a center and the output layer combines the outputs of the radial basis function and weight parameters to perform classification or inference.

iv. **Kohonen Self Organizing Neural Network (KSONN):**It self organizes the network model into the input data using unsupervised learning. It consists of two fully connected layers, i.e., input layer and output layer. The output layer is organized as a two dimensional grid. There is no activation function and the weights represent the attributes (position) of the output layer node.

v. **Modular Neural Network(MNN)**: Modular neural network breaks down large network into smaller independent neural network modules. The smaller networks perform specific task which are later combined as part of a single output of the entire network.

1.3.3 Architectures of deep neural networks

Below are three of the most common architectures of deep neural networks[17]:

i. **Convolution Neural Network(CNN)**:CNN is based on the human visual cortex and is the neural network of choice for image and video recognition. A CNN consists of a series of convolution and sub-sampling layers followed by a fully connected layer and a normalizing (e.g., softmax function) layer as shown in figure 3. The series of multiple convolution layers perform progressively more refined feature extraction at every layer moving from input to output layers.

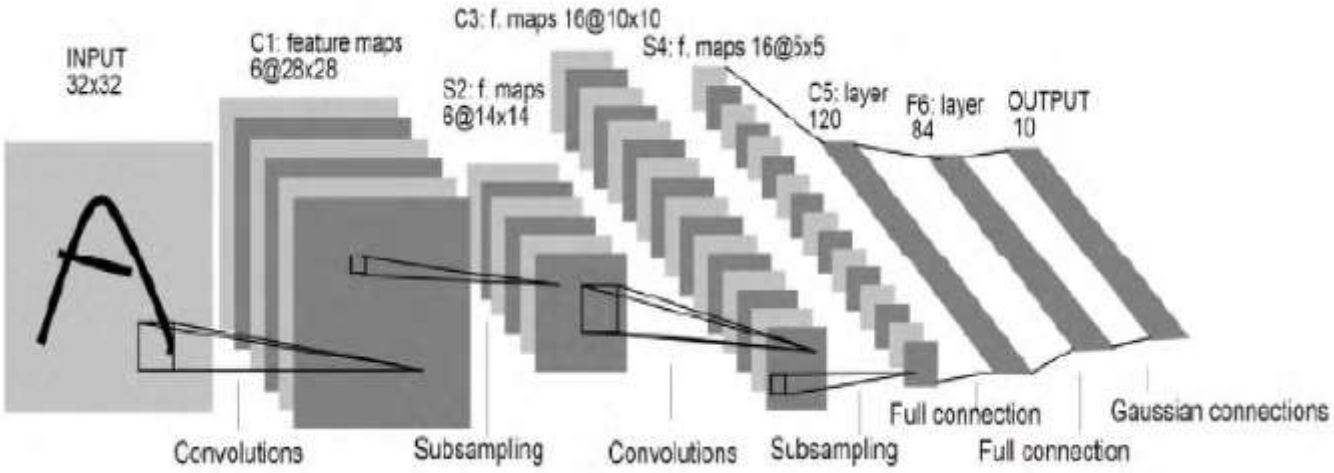

Figure 3: 7-Layer CNN architecture for character recognition

Fully connected layers that perform classification follow the convolution layers. Sub-sampling or pooling layers are often inserted between each convolution layers. Max/mean pooling or local averaging filters are used often to achieve sub-sampling. The final layers of CNN are responsible for the actual classifications, where neurons between the layers are fully connected.

Here are the well-known variation and implementation of the CNN architecture.

- AlexNet: A CNN developed to run on Nvidia parallel computing platform to support GPUs.
- Inception: A Deep CNN developed by Google.
- ResNet: A Very deep Residual network developed by Microsoft. It won 1st place in the ILSVRC 2015 competition on ImageNet dataset.
- VGG: A Very deep CNN developed for large scale image recognition.

ii. **Autoencoder:**Autoencoder is an neural network that uses unsupervised algorithm and learns the representation in the input data set for dimensionality reduction and to recreate the original dataset. The learning algorithm is based on the implementation of the backpropagation.

iii. **Restricted Boltzmann Machine (RBM):** Restricted Boltzmann Machine is an artificial neural network where we can apply unsupervised learning algorithm to build non-linear generative models from unlabeled data. The goal is to train the network to increase a function (e.g., product or log) of the probability of vector in the visible units so it can probabilistically reconstruct the input. It learns the probability distribution over its inputs. RBM is made of two-layer network called the visible layer and the hidden layer. Each unit in the visible layer is connected to all units in the hidden layer and there are no connections between the units in the same layer.

iv. Long Short-Term Memory (LSTM): LSTM can retain knowledge of earlier states and can be trained for work that requires memory or state awareness. LSTM consists of blocks of memory cell state through which signal flows while being regulated by input, forget and output gates. Single LSTM cell is represented in figure 4[18][19]. These gates control what is stored, read and written on the cell. LSTM is used by Google, Apple and Amazon in their voice recognition platforms. Its applicable for online signature based recognition also[20].

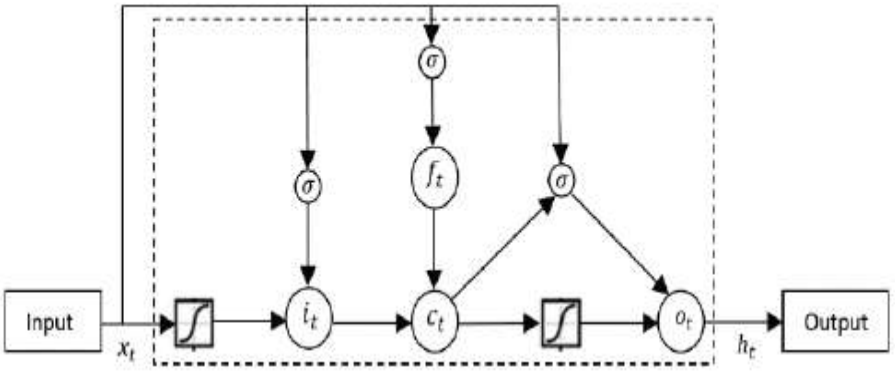

Figure 4 : LSTM single cell representation

where, σ is the logistic sigmoid function, and i, f, o and c are respectively the input gate,forget gate, output gate and cell state. Wci,Wcf and Wco are denoted weight matrices for peep hole connections.

1.4 BaaS- Biometric authentication as a Service

The biometric authentication system with the built in composite classifier can be deployed in form of BaaS i.e. Biometric authentication as a Serive. Software as a Service(SaaS) is a cloud computing's architectural model in which the software itself is offered as a service to end user[21][22][23]. Using a SaaS, an industry or individual can create an archive of their software versions, available to end users for usage, using PAYG. User is provided with remote access to the service. SaaS require a high performance Internet connection to connect our machine(or LAN) to CSP-sever offering SaaS. It addresses issues such as multitenancy, virtualization and security. Multi-tenancy utilizes sharing of single sharable resource among more than one tenant, while each tenant getting the impression that the resource is dedicated only to single user. A CSP uses virtualization to provide the different platforms to the CUs. Buying all the supporting hardware for each and every service isn't a feasible solution, so CSPs generally relay on the Virtual machines. Secure communication channel, secure data transmission, and secure data storage, these are the primary requirements of any SOC. Various measures for providing security, like VPN, SSL, Encryption, etc. can be used. A new paradigm of SLA based security [24] is gaining popularity among the CSPs and CUs.

1.4.1 Advantages of SaaS are[25]:

i. User won't need to make any capital investment in Software and other supporting system.
ii. For CU software maintenance cost reduces to zero, as software is actually maintained by SaaS provider.
iii. Reduces software piracy and dangers of it to a substantial amount due to flexible PAYG model.
iv. SaaS support flexible and effective collaborative development.
v. SaaS makes it possible to work from anywhere and whenever, for the user, subject to Internet connectivity with CSP.

1.4.2 Limitations of SaaS are[25]:

i. SaaS users have no control over the usage of versions of software offered as a service.
ii. Denial of Service attack, data theft by sniffers or hackers, inconsistency in data processing due to poor Internet connectivity are the few major threats to SaaS.

1.5 Blockchain

To achieve more security, BaaS can be integrated with blockchain to trigger the smart contract. A blockchain is a shared, distributed ledger that records transactions and is maintained by multiple nodes in the network where nodes do not trust each other. Each node holds the identical copy of the ledger which is usually represented as a chain of blocks, with each block being a logical sequence of transactions. Blockchain provides serializability, immutability and cryptographic verifiability without a single point of trust[26].

1.5.1 Types of blockchain

Blockchain is of two types:

i. **Permissionless Blockchain**: This is the public network where anyone can join the network to perform transactions. e.g. Ethereum. Due to a large number of nodes in a public network, a proof-of-work consensus approach is used to order transactions and create a block.

ii. **Permissioned Blockchain**: The identity of each participant is known and authenticated cryptographically such that blockchain can store who performed which transactions.

The integration of BaaS with blockchain will enable execution of smart contract. Smart contracts are defined as the computer protocols that digitally facilitate, verify, and enforce the contracts made between two or more parties on blockchain [27].

1.5.2 Operating mechanism of Smart Contract

Smart contracts are a set of Scenario-Response procedural rules and logic. The parties signing a contract should agree on contractual details, conditions of breach of contract, liability for breach of contract and the external verification data sources (oracles), then deploy it on the blockchain in the form of smart contract thus to automate the execution of contract on behalf of the signatories. The whole process is independent of any central agencies.

The operating mechanism of smart contracts is shown in figure 2. Normally, after the smart contracts are signed by all parties, they are attached to the blockchain in the form of program codes and are recorded in the blockchain after being propagated by the P2P network and verified by the nodes.

Smart contract encapsulates a number of pre-defined states and transition rules, scenarios that trigger contract execution (such as at a given time or a particular event occurs), responses in a particular scenario, etc. The blockchain monitors the real-time status of smart contracts and executes the contract after certain trigger conditions have been met[28].

1.5.3 Characteristics of Smart Contract

As smart contracts are typically deployed on and secured by blockchain, they have some unique characteristics.

i. The program code of a smart contract will be recorded and verified on blockchain, thus making the contract tamper-resistant.
ii. The execution of a smart contract is enforced among anonymous, trustless individual nodes without centralized control, and coordination of third-party authorities.
iii. A smart contract, like an intelligent agent, might have its own cryptocurrencies or other digital assets, and transfer them when predefined conditions are triggered[29].

2. Motivation

Biometric authentication system's success is relying on how well the classifier classifies the user as registered user or an imposter. Ongoing research on deep learning proves that deep learning techniques have strong learning ability and high predictability over shallow classifiers, but in compromise of high computational cost.[14][15][16]. To have optimal balance of getting high accuracy with reasonable computations, shallow classifiers are combined with deep learning techniques[17].

To make the system scalable and to get wide appreciation, it needs to be deployed on cloud such as Amazon Web Service (AWS) in form of Biometric authentication as a Service i.e. BaaS. Amazon SageMaker makes it easy to deploy in production to start running generating predictions on new data[23][24]. Security can be offered to BaaS by integrating it with permissioned blockchain, since serializability, immutability, and cryptographic verifiability without a single point of trust[26]. Hyperledger fabric based blockchain enables automatic execution of smart contract. Due to the characteristics such as immutablity and irreversibility gained from permissioned blockchain, smart contracts can help people exchange money, shares, intellectual property, etc. in a transparent, conflict-free way while avoiding the interference of third-party[28].

3. Literature review

Sr No	Title of the paper	Publication	Authors	Key Finding	Gap Finding
1	A Survey on Biometric Authentication : Towards Secure and Privacy-Preserving Identification	IEEE, 2018	Zhang Rui , Zheng Yan	Reviewed recent advances in biometric authentication and pointed out potential risks and proposed evaluation criteria for measuring performance of classifiers.	Classification is performed by using shallow classifiers.
2	Unsupervised feature learning and automatic modulation classification using deep learning model	IEEE, 2017	Afan Ali, Fan Yangyu	Proposed network with 2autoencoders extract two features separately and then stacks to final DNN followed by softmax classification layer to get high accuracy	Minimum to maximum number of hidden layers are not specified.
3	DeepMalNet: Evaluating shallow and deep networks for static PE malware detection	Sci. Direct	Vinayakumar R., Soman K.P.	DNN is proved to be better than shallow classifiers on EMBER dataset. ReLU activation function is proved to be good over sigmoid, tanH, SeLu.	Deep learning through classification involves huge number of computations.
4	KNN-based Ensemble of Classifiers	ICCSCI, 2016	YehyaAbouelnaga, Ola S. Ali, Hager Rady, and Mohamed Moustafa	Combined KNN with CNN and obtained improved accuracy.	As dataset increases, KNN comparisons get increased and affects time and space complexity.

Sr No	Title of the paper	Publication	Authors	Key Finding	Gap Finding
5	Data augmentation for improving deep learning in image classification problem	IEEE 2018	Agnieszka Mikołajczyk, Michał Grochowski	Introduced an error mechanism to make classifier more robust to improve classifier's accuracy over test data set	It overheads the performance of system due to additional data.
6	Biometrics-as-a-Service: A Framework to Promote Innovative Biometric Recognition in the Cloud	IEEE 2017	VeeruTalreja, Terry Ferrett, Matthew C. Valenti, Arun	Put forth a framework to deploy Biometric Recognition as a Service(BaaS)	File system performance may be improved by using database techniques to handle many small files. A low ratio of free space to average object size leads to fragmentation and performance degradation.
7	Biometric Authentication using Software as a Service (SaaS) Architecture with Real-time Insights	IEEE 2016	Godson Michael D'silva, Vinayak Ashok Bharadi, Shridhar Kamble	Proposed a highly secure, scalable, pluggable and faster biometric system architecture, that can handle a billion of biometric events per second.	
8	Performance benchmarking and optimizing Hyperledger fabric blockchain platform	IEEE 2018	ParthThakkar, Senthil Nanthan N, Balaji Vishwnathan	Performed three kinds of optimizations such as MSP cache,parallel VSCC validation, commit phase to improvesingle channel performance from 16 to 2250tps.	Integration of SaaS with permissioned blockchain to automate execution of smart contract is an untouched issue.
9	An Overview of Smart Contract: Architecture, Applications, and Future Trends	IEEE 2018	Shuai Wang, Yong Yuan, Xiao Wang, Juanjuan Li, Rui Qin, Fei-Yue Wang	Discussed the immutable and irreversible characteristics of smart contract	

4. Research Problem

The purpose of research is to evaluate and enhance the supervised deep learning techniques to classify the combined feature vector of the physiological and behavioral traits collected from the person and deploy it as a SaaS on cloud to build smart contract among authenticated parties.

5. Research Objectives

This research aims to build service model which will authenticate the users by their biometric traits using composite classifiers and implement the business logic in the form of smart contract.

i. Select and perform fusion of features of physiological biometric traits such as fingerprint, face,iris, palmprint, etc. and behavioral biometric traits such as signature, voice,etc. at feature extraction level and successive levels.
ii. Apply deep learning technique as standalone technique as well as with shallow classifiers in combined way on the fused dataset in Python and evaluate classifier's performance.
iii. Deploy the system in form of BaaS i.e. Biometric authentication as a Service on Amazon Web Service(AWS).
iv. Integrate BaaS with permissioned blockchain by using Pytorch deep learning framework in order to trigger smart contract and evaluate the performance of the system.
v. To write smart contract for enterprise applications such as IoT or Trade Finance, etc.

6. Research Design

The proposed architecture basically consists of three phases as shown in figure 5.

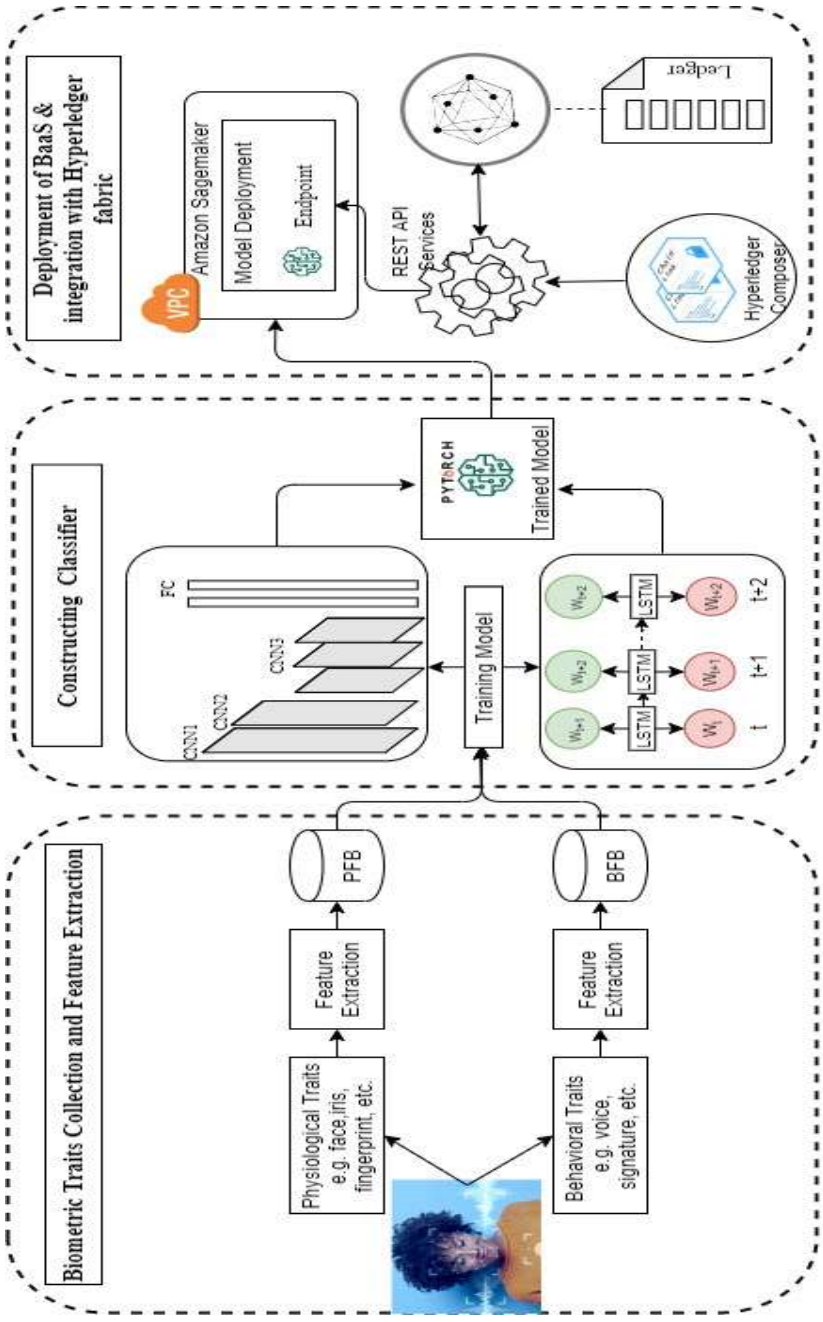

Figure 5.Proposed architecture of Permissioned Blockchain based Smart Contract utilizing Biometric Authentication as a Service

i. Biometric traits acquisition and features extraction.
ii. Building Biometric authentication performing classifier using deep learning techniques.
iii. Biometric authentication performing classifier's deployment on AWS cloud and integration of BaaS with amazon managed blockchain.
iv. Implementation of any use case such as trading and asset transfer or retail, etc., to evaluate the performance of overall system.

6.1 Biometric traits acquisition and feature extraction

i. **Biometric Traits Collection module**: The proposed system is based on recognition from combination of physiological and behavioral traits. Since, only physiological trait could be easily duplicated and reliance on only behavioral trait may result in intra class differentiability if there is even slight difference in the behavior of person.

Table 2: Biometric trait, their features and techniques used to extract features

Biometric trait	**Datasets**	**Features extracted for matching**	**Techniques used to extract features**
Iris Datasets	CASIA, MMU, BATH, UPOL, UBIRIS	Contraction furrows, striations, pits, collagenous fibers, filaments, crypts (darkened areas on the iris), serpentine vasculature, rings	Hough tranform to identify pupil boundaries
			Wavelet transform
			Gabor filter is used for eyelid detection, noise removal
			Circular Hough transform can be employed to deduce the radius and centre coordinates of the pupil and iris regions.
Finger	SDUMLA, FVRC, HKPU	Papillary pattern (Arches, loops and a whorls), hills and valleys, centration	Discrete Wavelet transform ia apllied on decomposed image to collect the mentioned features.

Biometric trait	Datasets	Features extracted for matching	Techniques used to extract features
Face	FERET, LFW, FERET, CSU, Yale	Feature based method is used to extract structural features of face. With knowledge based method geometry of face get extracted. Appearance based method face patterns are compared, whereas template matching method uses pre-defined or parameterised face templates to locate or detect the faces by the correlation between the templates and input images.	Gabor wavelets are widely used in image processing field in that they capture local structure corresponding to spatial frequency, spatial localization (face geometry)
			The face area is first divided into small regions from which Local Binary Patterns (LBP), histograms are extracted and concatenated into a single feature vector. This feature vector forms an efficient representation of the face and is used to measure similarities between images
			Scale-invariant feature transform (SIFT)[63] has the merit of invariance to translations, rotations and scaling transformations in the image domain and robustness to moderate perspective transformations and illumination variations
			Corelation between pixels is determined by PCA, DCT, Wavelet Hadamard Transform
Signature	MOBISIG , UTSig	Static features of a signature (e.g., shape, slant, size), and its dynamic features (e.g., velocity, pen-tip pressure, timing)	Hough transform to detect stroke lines from signature image.
Keystroke dynamics	CMU keystroke dynamics, BeiHang Keystroke dynamics	Hold time or dwell time of individual keys, and the latency between two keys, i.e., the time interval between the release of a key and the pressing of the next key.	Digraph, Trigraph to record latencies occurred in pressing keys.Pressure sensors are used to record pressure.
Voice	TED-LIUM Corpus, Google AudioSet, common voice	Pitch,accent	Mel Frequency Cepstral Coefficients (MFCC), Linear Prediction Coefficients (LPC), Linear Prediction Cepstral Coefficients (LPCC), Line Spectral Frequencies (LSF), Discrete Wavelet Transform (DWT) and Perceptual Linear Prediction (PLP)

ii. **Feature processing module**: The combination of physiological and behavioral traits such as ECG and fingerprint or voice and face biometric traits are necessary to get the liveliness assurance of the user. These extracted features are fused at different levels of recognition system. Past research work says the fusion at earliest stage of system is more complex but produces result with high accuracy. The fig.1a) architecture is drawn with the assumption that fusion is performed manually at feature extraction level, where the convolution matrices are user defined and are feature-of- interest specific. Convolutional neural network using VGG net architecture get applied on fused dataset to classify the traits[6]. Alternative way is to use a fully connected layer following the convolutional neural network to fuse the extracted eminent features from the traits[7].

6.2 Building Biometric authentication performing classifier using deep learning techniques

i. **Learning Module**: Feed the fused dataset from earlier stage to deep learning framework for getting it classified. Convolutional neural networks are going to be used to classify users based on the unimodal physiological biometric trait images, whereas Long short term memory architecture is preferred for classifying user based on unimodal behavioral biometric traits as well as multimodal biometric traits.

PyTorch deep learning framework enables building of neural network such as CNN, LSTM etc., by providing an array-based programming model accelerated by GPUs and differentiable via automatic differentiation integrated in the Python ecosystem[18][19].

ii. **Testing module**: With testing module, registered as well as unregistered user's traits are classified to measure the prediction capability of classifier. Research informs that deep convolutional neural networks can be easily fooled into misclassification of images just by partial rotations and image translation, adding the noise to images and even changing one, skillfully selected pixel in the image. Regularization helps in this matter of avoiding overfitting. Increasing the dataset size via data augmentation (which is a method of regularization) and image synthesis make it generally more robust and less vulnerable for the adversarial attacks[20]. Deep Dream, Deep Art are few of the data augmentation techniques. Regularization prevents the error between the original and predicted value for getting reduced to zero when training data set is learnt by classifier, ultimately reducing the error rate when it comes to the test dataset.

6.3 Classifier's deployment in form of BaaS on AWS Cloud and integration of BaaS with permissioned blockchain to trigger smart contract

i. **Implementation of BaaS:** Biometric authentication system with deep neural network based classifier will be deployed on Amazon Web Service (AWS) cloud in form of BaaS i.e. Biometric authentication As A Service. Once classifier is built, trained and tuned, Amazon SageMaker makes it easy to deploy in production to start running generating predictions on new data (a process called inference). Amazon SageMaker deploys classifier on an auto-scaling cluster of Amazon EC2 instances that are spread across multiple availability zones to deliver both high performance and high availability. Amazon SageMaker also includes built-in A/B testing capabilities to help to test model and experiment with different versions to achieve the best results.[aws.amazon.com]

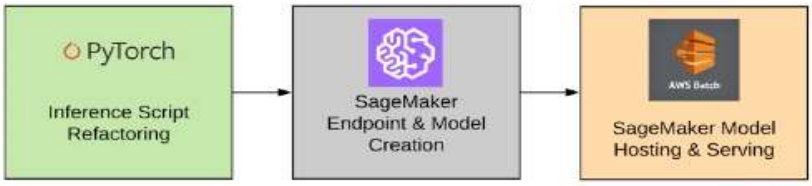

Figure 6.Blockdiagram of blockchain managed by AWS

ii. **Permissioned blockchain:**Hyperledger Fabric (HLF) is an open-source implementation of a distributed ledger platform for running smart contracts in a modular architecture.

It is a platform for distributed ledger solutions, underpinned by a modular architecture delivering high degrees of confidentiality, resiliency, flexibility and scalability. It is designed to support pluggable implementations of different components, and accommodate the complexity and intricacies that exist across the economic ecosystem. Hyperledger Fabric leverages container technology to host smart contracts called "chaincode" which comprise the application logic of the system. Besides that, "chaincode" is the only channel that interacts with the blockchain and the only source that generates the transactions [15].

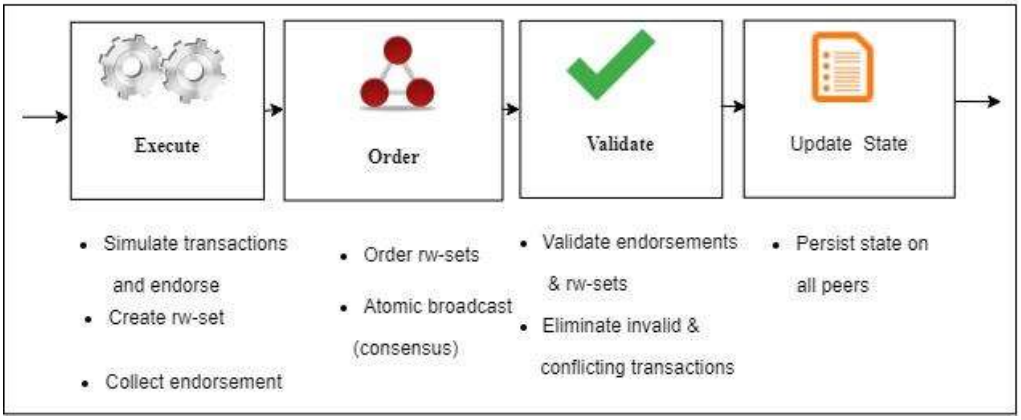

Figure 7: Execute-Order-Validate Blockchain Architecture

Prior permissioned blockchain suffer from many limitations such as fixed trust model, hard-coded consensus, smart contracts are supposed to be written in fixed format which often stem from their permissionless relatives or from using the order-execute architecture.

iii. **Smart Contract:** Elimination of third party leads to the reliance of smart contract on blockchain to infer the security from its working mechanism.Smart contracts are computer protocols intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts have broad range of applications, such as financial services, prediction markets and Internet of Things (IoT), etc.[18].

7. Evaluation of System

1	**Biometric authentication system** [5]		
	i	**False Acceptance Rate (FAR)**	The possibility of identifying an imposter as a legitimate user.
	ii	**False Rejection Rate (FRR)**	The possibility of identifying a legitimate user as an imposter.
	iii	**Equal Error Rate (EER)**	It is the rate when the proportion of false acceptance is equal to the proportion of false rejection.
	iv	**Accuracy**	The capability of correctly classifying an individual as an imposter or a legitimate user.
	v	**Precision**	This gives exactness, how many correctly classified as legitimate user out of total registered legitimate users.
	vi	**Recall**	This gives completeness how many are authenticated correctly out of total legitimate users.
2.	**Biometric Recognition System Software as a Service** [23]		
	i	**CPU utilization**	The utilization of CPU to offer the service at the customer and service provider ends.
	ii	**Availability**	The time for which system is functioning properly without any failure.
	iii	**Reliability**	The system's capability to function under given environmental conditions, for a particular amount of time.
	iv	**Response Time**	The time system takes to classify the input.
	v	**Latency**	The time system takes from submission of input to produce the classified output.
	vi	**Throughput**	Number of requests handled per second.

<table>
<tr><td>3.</td><td colspan="3">Blockchain based Smart Contract [31]</td></tr>
<tr><td></td><td>i</td><td colspan="2">Queue length: Queue length of a node is the number of jobs waiting for service or in service at that node.</td></tr>
<tr><td></td><td>ii</td><td colspan="2">Latency: It is the time taken between when the transaction is submitted and when the transaction is confirmed committed across the network. For a set of transactions, the average latency is the average of latency of all transactions in the data set.</td></tr>
<tr><td></td><td></td><td>Endorsement latency</td><td>The time taken for the client to collect all proposal responses along with the endorsements.</td></tr>
<tr><td></td><td></td><td>Broadcast latency</td><td>The time delay between client submitting to orderer and orderer acknowledges the client.</td></tr>
<tr><td></td><td></td><td>Commit latency</td><td>The time taken for the peer to validate and commit the transaction.</td></tr>
<tr><td></td><td></td><td>Ordering latency</td><td>The time transaction spent on the ordering service.</td></tr>
<tr><td></td><td></td><td>VSCC validation latency</td><td>The time taken to validate all transactions' endorsement signature set (in a block) against the endorsement policy.</td></tr>
<tr><td></td><td></td><td>MVCC validation latency</td><td>The time taken to validate all transactions in a block by employing multi-version concurrency control</td></tr>
<tr><td></td><td></td><td>Ledger update latency</td><td>The time taken to update the state database with write-set of all valid transactions in a block</td></tr>
<tr><td></td><td>iii</td><td colspan="2">Transaction Throughput: It is the rate at which the blockchain network commits valid transactions in the defined period of time i.e. tps -number of transactions per second.</td></tr>
<tr><td></td><td>iv</td><td colspan="2">Utilization: Utilization of a node is a percentage of time the node is busy.</td></tr>
</table>

8. Expected Outcomes

Research is aimed to produce the following results:

i. Cloud based system i.e. biometric authentication as a service (BaaS).
ii. Designing a classifier for such a system performing classification with higher accuracy compared to existing classifiers.
iii. Integrated smart contract based enterprise application which need user authentication to perform transaction such as trade execution, etc.

9. Conclusion

The rapid development of the internet and mobile devices, underlines the necessity of authentication system since it has been widely used in the internet service access and mobile device access for protecting user devices, contents, and accounts. In many business applications for image, chart classification, the deep learning techniques are preferred over shallow classifiers but still certain problems need to be addressed such as longer training time, huge number of computations and related space complexity, etc. Biometric trait based specific architecture involving deep learning standalone technique or deep learning technique combined with shallow classifier need to be devised to achieve accuracy with reasonable computations and time complexity.

The implementation of biometric system through Amazon Web Service will enable scalability, application integrity and wide appreciation among authentication demanding end to end services. A permissioned blockchain network is highly suitable for such services, where each node in a permissioned network can be owned by different organizations and may get into the smart contract by agreeing upon certain rules and regulations which would be triggered when particular condition/s met.

Presented paper: **Mrs. G.N. Sawant, Dr. Vinayak Bharadi**, presented paper on "**Permission Blockchain based Smart Contract utilizing Biometric Authentication as a Service: A Future Trend**", at the **IEEE International Conference** on **Convergence to Digital World (ICCDW)-Quo Vadis** from 19th to 20th **February, 2020.**

References

[1] Krishna Dharavath, F. A. Talukdar, R. H. Laskar, "Study on Biometric Authentication Systems, Challenges and Future Trends: A Review" IEEE 2013

[2] Multimodal biometric system with low cost sensors.pdf

[3] Anil K. Jain, Arun Ross, Salil Prabhakar, "An Introduction to Biometric Recognition", 2004 January.

[4] AnterAbozaid& Ayman Haggag& Hany Kasban& Mostafa Eltokhy, "Multimodal biometric scheme for human authentication technique based on voice and face recognition fusion" Springer November 2018

[5] Zhang Rui, Zheng Yan, "A Survey On Biometric Authentication: Towards Secure And Privacy-Preserving Identification" IEEE 2017

[6] S. Prasad, V. Govindan and P. Sathidevi, "Palmprint authentication using fusion of wavelet and contourlet features," Security and Communication Networks, vol. 4, no. 5, pp. 577–590, 2011.

[7] S Noushath, Mohammad Imran, Karan Jetly, Ashok Rao, Hemantha Kumar G, "Multimodal Biometric Fusion of Face and Palmprint at Various Levels" IEEE 2013

[8] Sandeep Patil, Shreya Gudasalamani, Nalini C. Iyer, "A Survey on Iris Recognition System", ICEEOT,2016

[9] Ankit Shrivastava, Devesh Kumar Shrivastava, "Fingerprint Identification Using Feature Extraction", IEEE 2014

[10] Ankit Srivastava, Suraj Mane, Aaditya Shah, Nirmit Shrivastava, Prof. Bhushan Thakare, "A survey of face detection algorithms", ICISC 2017.

[11] Vinayak Bharadi, Bhavesh Pandya, Georgina Cosma,"Multi-modal Biometric Recognition using Human Iris and Dynamic Pressure Variation of Handwritten Signatures", IEEE 2018

[12] Yunbin Deng, "Recent Advances in User Authentication Using Keystroke Dynamics Biometrics", DOI: 10.15579/gcsr.vol2.ch1, GCSR Vol. 2, pp. 1-22, 2015

[13] Xuedan Du, Yinghao Cai, Shuo Wang and Leijie Zhang, "Overview of Deep Learning", IEEE November 2016

[14] Valentin Radu, Catherine Tong, Sourav Bhattacharya, Nicholas D. Lane, Cecilia Mascolo Mahesh K. Marina, Fahim Kawsar, "Multimodal Deep Learning for Activity and Context Recognition" ACM November 2017

[15] YehyaAbouelnaga, Ola S. Ali, Hager Rady, and Mohamed Moustafa, "KNN-based Ensemble of Classifiers", ICCSCI, 2016

[16] Vinaykumar R., Soman K.P., "DeepMalNet: Evaluating shallow and deep networks for static PE malware detection" KICS 2018

[17] Ajay Shrestha, Ausif Mahmood, "Review of Deep Learning Algorithms and Architectures", IEEE April 2019

[18] Adam Paszke, Sam Gross,Fransisco Massa, "PyTorch: An Imperative Style, High-Performance Deep Learning Librar.pdf"

[19] Jihyun Kim, Jaehyun Kim, Huong Le Thi Thu, and Howon Kim, “Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection”, IEEE 2016

[20] Agnieszka Mikołajczyk, MichałGrochowski, “Data augmentation for improving deep learning in image classification problem”, IEEE 2018

[21] Godson Michael D’silva, Vinayak Ashok Bharadi, Shridhar Kamble, “Biometric Authentication using Software as a Service (SaaS) Architecture with Real-time Insights”

[22] Godson Michael D’silva, Vinayak Ashok Bharadi,”Online Signature Recognition using Software as a Service (SaaS) Model on Public Cloud”, IEEE 2015

[23] VeeruTalreja, Terry Ferrett, Matthew C. Valenti, Arun Ross, “Biometrics-as-a-Service: A Framework to Promote Innovative Biometric Recognition in the Cloud”, arXiv:1710.09183v1 [cs.dc] October 2017

[24] Anniruddha S. Rumale, Dinesh N. Choudhari, “Cloud Computing: Security Issues and Measures”, 2014

[25] Anniruddha S. Rumale, Dinesh N. Choudhari, “Cloud Computing: Software as a Service”, IEEE.2017

[26] Parth Thakkar, Senthil Nanthan N., Balaji Vishwanathan, “Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform”, IEEE 2018

[27] Harish Sukhwani, Nan Wang, Kishor S. Trivedi,AndyRindos,”Performance Modeling of Hyperledger Fabric (Permissioned Blockchain Network)”, IEEE 2018

[28] Shuai Wang, Yong Yuan, Xiao Wang,Juanjuan Li, Rui Qin, Fei-Yue Wang, “An Overview of Smart Contract: Architecture, Applications, and Future Trends “, 2018 IEEE Intelligent Vehicles Symposium (IV) .J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[29] Shuai Wang , Liwei Ouyang, Yong Yuan , Xiaochun Ni, Xuan Han, and Fei-Yue Wang ,” Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends”, IEEE 2019

[30] Jerry Gao, PushkalaPattabhiraman, Xiaoying Bai w. T. Tsai, “SaaS Performance and Scalability Evaluation in Clouds”, IEEE 2011

[31] SupornPongnumkul, Chaiyaphum Siripanpornchana, and SuttipongThajchayapong, “Performance Analysis of Private Blockchain Platforms in Varying Workloads”, IEEE,2017