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**	Evolving Authentication Design Consideration and Cloud application Architecture for Internet of Biometric things
6	**Name of research student**	Mr. Pravin Jangid
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	**: Mr. Pravin Jangid**
Course/Branch	**: Ph. D. Information Technology**
Research Title	**: Evolving Authentication Design Consideration and Cloud application Architecture for Internet of Biometric things**
Name of the Research Guide	**: Dr. Vinayak Ashok Bharadi**
Date of Submission	**:**

Mr. Pravin Jangid
Research Scholar

Dr. Vinayak Ashok Bharadi
Head of Research Center

Dr. Vinayak Ashok Bharadi
Guide

Dr. Kaushal Prasad
Principal

Table of Contents

List of Figures

List of Tables

Abbreviations and Symbols

GPU	Graphics Processing Unit
IDM	Identity management
BaaS	Biometric authentication as a Service
IaaS	Infrastructure as a service
PaaS	Platform as as a service
SaaS	Software as a service
IoT	Internet of Things
IoBT	Internet of Biometric Things
RFID	Radio-frequency identification
AWS	Amazon Web Service

ABSTRACT

Cloud computing has opened many possibilities for the design and implementing various models of software for addressing variety of problems. Biometric authentication is an important aspect of security and need for the same is increasing day by day. This has resulted in adaptation of biometric security based systems by masses. Further, with the portable sensors and computing devices the biometric authentication will become an integral part of Internet of Things. To handle such a large scale of authentication cloud based implementation is a viable option. In the proposed methodology a cloud based architecture possibilities will be explored for Internet of Biometric Things (IoBT). Further ontology study of the IOBT Architecture will be done. The deployment of Biometric authentication system on the cloud in the form of BAAS will enable enterprise application to integrate Biometric authentication and authorization capability for wide range of application such as banking ,trading, finance and smart cities. Security is one of the prime concerns in the Internet of everything. IOBT is the subpart of this Internet of everything implementation and the other aspect of the study is to provide end to end security mechanism which will be lightweight cryptography suitable for IOBT devices.

1. Introduction

The term "biometric" is taken from the Greek words bio (which means story of a person's life) and metric (to measure). Biometric means identifying automatically body-structure-related to a person or behavioral features. Biometric method is given preference for verification over traditional methods like PIN numbers and passwords because of its case sensitiveness and high accuracy. A Biometric technique is basically a system which recognizes the pattern which identifies the personal things by figuring out the realness of specific body-structure-related or behavioral features which user possessed. These features are measurable and very unique. [1], [2], [3].

A number of biometric attributes have been recognized and are utilized to validate the individual's personality. The thought is to utilize the extraordinary attributes of an individual to distinguish him. By utilizing exceptional qualities we mean utilizing the traits like iris, face, unique mark, and signature and so on. The biometrics qualities are arranged in dual class specifically physiological and behavioral biometric characteristics [3]. Physiological biometrics qualities depend on outer attributes of human physique, similar to face, fingerprint, iris, palm print and so forth. Behavioral biometric characteristics depend on the way human play out a specific activity, Additional, a biometric framework can be also a 'identification' framework for 1:N matching or a 'verification' framework for 1:1 matching [4].

Biometric frameworks have gone distant past local verification. The later advances appear that the utilization of biometrics in dispersed systems with the compelling utilization of multimodal characteristics and portable gadgets has opened a modern door for biometric applications. Biometrics have gotten to be spearheading components of portable administrations over cloud situations as there's a really developing utilization of portable gadgets like smart watches smart phones, and tablets [4].

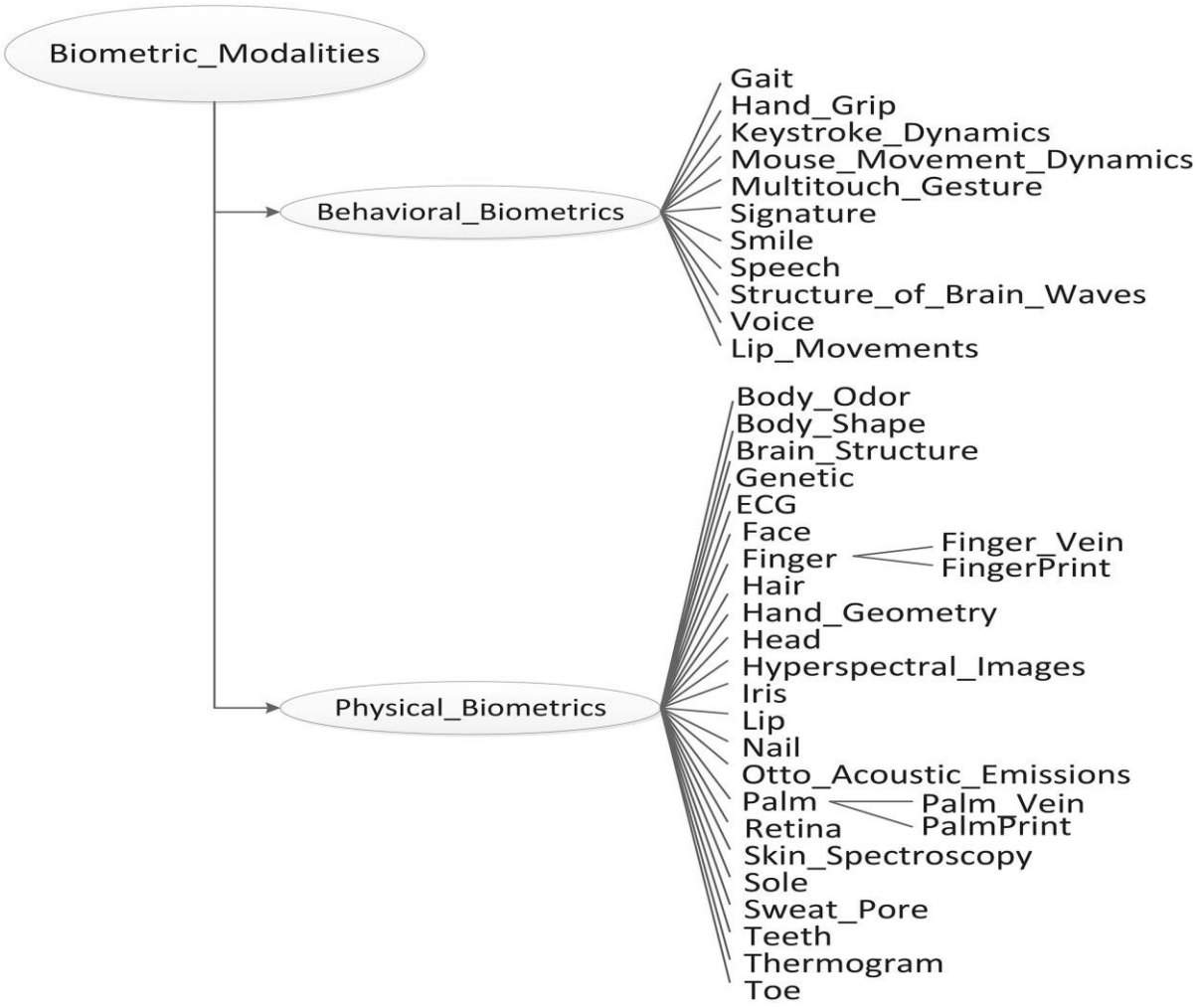


Figure 1 Underlying classes of 'Biometric_Modality' concept [3]

.

1.2 Cloud Computing

Cloud Computing is the use of hardware and software to deliver a service over a network (typically the Internet). With **cloud computing**, users can access files and use applications from any device that can access the Internet. An **example** of a **Cloud Computing** provider is Google's Gmail.

Cloud computing types are service deployment models that let you choose the level of control over your information and types of services you need to provide. There are three main types of cloud computing services, sometimes called the cloud computing stack because they build on top of one another.

The first cloud computing type is **infrastructure-as-a-service (IaaS)**, which is used for Internet-based access to storage and computing power. The most basic category of cloud computing types, IaaS lets you rent IT infrastructure - servers and virtual machines, storage, networks, and operating systems - from a cloud provider on a pay-as-you-go basis.

The second cloud computing type is **platform-as-a-service (PaaS)** that gives developers the tools to build and host web applications. PaaS is designed to give users access to the components they require to quickly develop and operate web or mobile applications over the Internet, without worrying about setting up or managing the underlying infrastructure of servers, storage, networks, and databases.

The third cloud computing type is **software-as-a-service (SaaS)** which is used for web-based applications. SaaS is a method for delivering software applications over the Internet where cloud providers host and manage the software applications making it easier to have the same application on all of your devices at once by accessing it in the cloud [5].

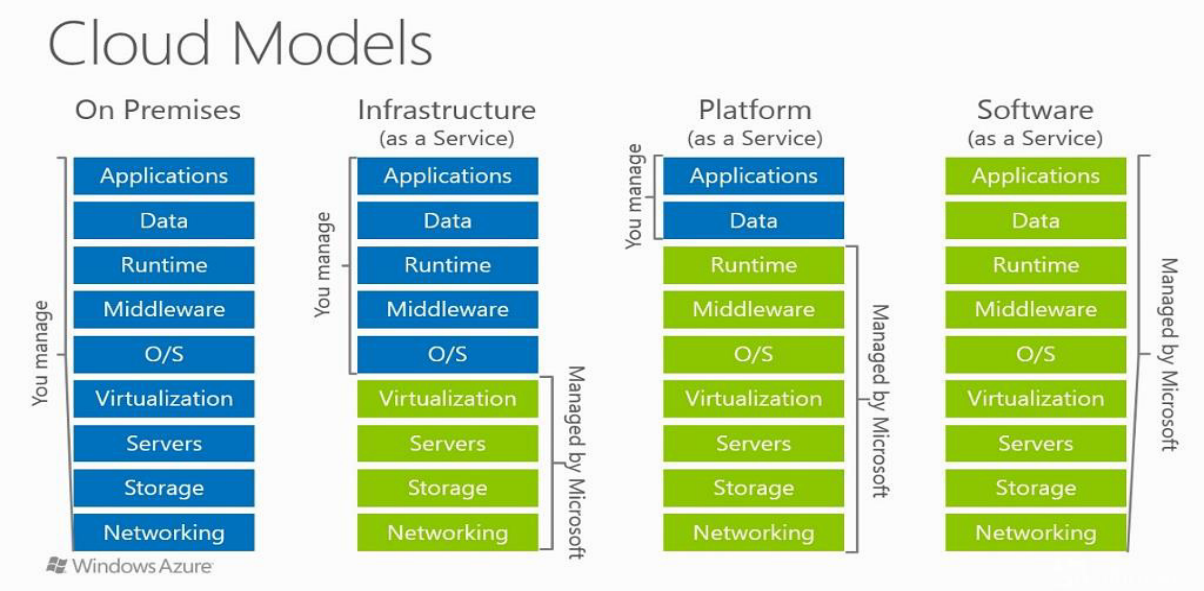


Figure 2. Cloud Models

1.2.1 BIOMETRIC SOFTWARE AS A SERVICE (BaaS)

With the fast adoption of cloud computing, the use of biometric technologies has evolved to a different way of providing security, preserving privacy, and analysing personal traits for various purposes. The main components of any biometric system, such as biometric sensing, data gathering, feature extraction, identification, verification, recognition, and analytics, are now handled over distributed networks.

Many of the biometric system services are presented over such networks which are followed by the creation of a new concept `biometric-as-a-service (BaaS)'. Recent BaaS approaches usually focus on identifying the effective distributed architectures, policies, and use case recommendations. However, there is a strong need to focus on developing a semantic framework which should rely on a biometric ontology.

In the modern applications need to cater for the following aspects

1. Consistent Communication Management

2. Complete Visibility

3. Failure Isolation and Protection

4. Fine Grained Deployment Control

The Cloud based BaaS Deployments are the answer for the above requirements beyond that we propose to increase the speed and security through the use of Deep Learning based classification on cloud based GPU and secure transaction on BlockchainDB. Further, the emergence of Internet of things is also having impact on the way people are being authenticated. As these IoT nodes are becoming more an more powerful, they will have the capacity to capture the biometric traits and this will need changes in existing architectures to provide the BaaS to such devices, besides there is a need of lightweight feature vector extraction for such devices [6].

1.3 BLOCKCHAIN AND BLOCKCHAINDB

Blockchain is a distributed ledger technology where each block carries a list of transactions and a hash key to the previous block. It is a linked list concept which is continuously updated, replicated and imparted to all the nodes in the network. The hash key is used to created interlinking between the blocks, thus creating a chain of blocks or blockchain [5]. The hash of the block gets changed the moment you make any changes in the data contained inside the block. To detect any modifications in the block, hashes play a vital role. Genesis Block is the first block in the blockchain.

The blockchain cloud is a thin cloud in comparison to traditional cloud computing infrastructure. Blockchain was conceptualized in 2008; it was implemented to enable a payment system for the Bitcoin cryptocurrency. Blockchain permits untrusting parties to co-create a permanent, unchangeable and transparent record of exchange and processing without relying on a central authority.Hash function is not enough to prevent tampering. Computing hundreds of thousands of hashes takes only a few seconds, the block can be effectively swindled, and all the hashes of the block can be recalculated. So, to brand blockchain safer, we use proof of work (PoW). PoW is the mechanism that reduces the formation of new blocks.

This mechanism makes the operation of blocks very difficult, because if you modify a block, you need to recompute PoW for all the following blocks.

The efficient use of hashing and proof of work makes the Blockchain more secure. Another important security measure is that Blockchain is P2P in nature and takes consensus from more than 50% of the peers to accept any change. The continuously evolving Blockchain along with the concept of smart contracts is the most recent development.

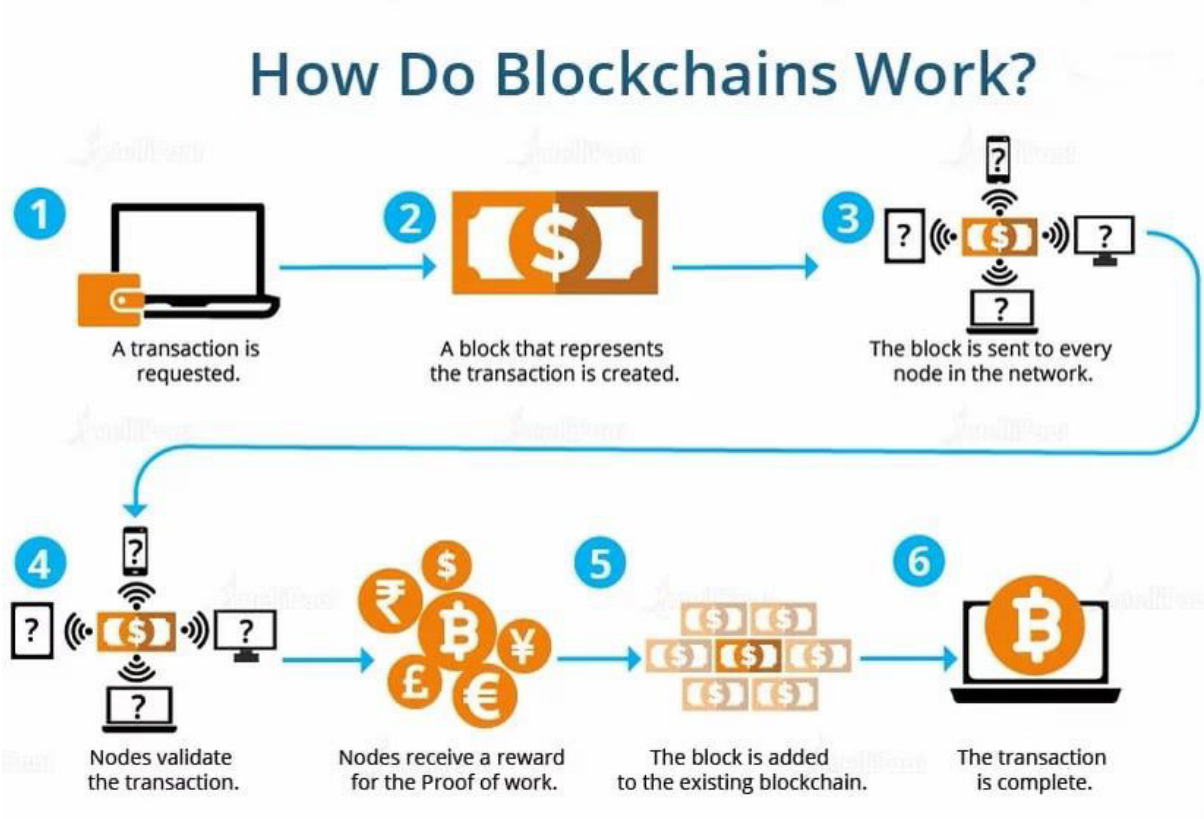


Figure 3. Blockchain[37]

1.3.1 TYPES OF BLOCKCHAIN

In this section we will briefly describe the types of Blockchain.[4] There are two types of ledger for Blockchain: (1) Public or Decentralized ledger, (2) Private or Centralized ledger.[2] Based on permission, blockchain is of two types: Permissioned and Permissionless.

A. Public or Decentralized

In public or decentralized ledger are based on Proof of Work consensus algorithms are upon sourced and not permissioned (pp). Anyone can read, write and send transactions. The buyer creates the transaction or a block, then the transaction is distributed or validated via cryptographic hashing. In distributed databases, the transaction is committed to blockchain and miners are rewarded. Further via trustless peering the seller receives the transaction. These ledgers use Proof of Work, Proof of stake and other consensus mechanisms to secure these ledgers. Examples: Bitcoin, Ethereum, Monero, Dash, Litecoin, Dodgecoin, etc.

B. Private or Centralized

In Private ledger write permissions are centralized to one organization whereas read permissions can be public or restricted. They take the advantage of blockchain technology where end users can verify the transactions internally. It reduces redundancy leading to low cost of transactions. The participants in such a system are preapproved and have known identities. These types of ledgers are more or less obsolete in the current scenario.

C. Permissioned

Bitcoin is the best example of permissioned public blockchain.Each node in the network contributes in consensus method.The permissioned blockchain maybe public-permissioned or private-permissioned. Permissioned public works on Proof of Work protocol where anyone who meets certain predefined criteria can download the protocol and validate transactions whereas in permissioned private only member of consortium can validate transactions using PBFT or multi-signature.

D. Permissionless

Permissionless blockchain have public ownership, open & transparent. In permission less public works on proof of work, anyone can download the protocol and validate transactions.

1.3.2 APPLICATIONS OF BLOCKCHAIN

A. Smart Contracts

In the decentralized cryptographic era, mutually distrustful groups announce to work safely on behalf of third parties, smart contracts are emerging as a solution.[6] They ensure that the parties pay a fair compensation.

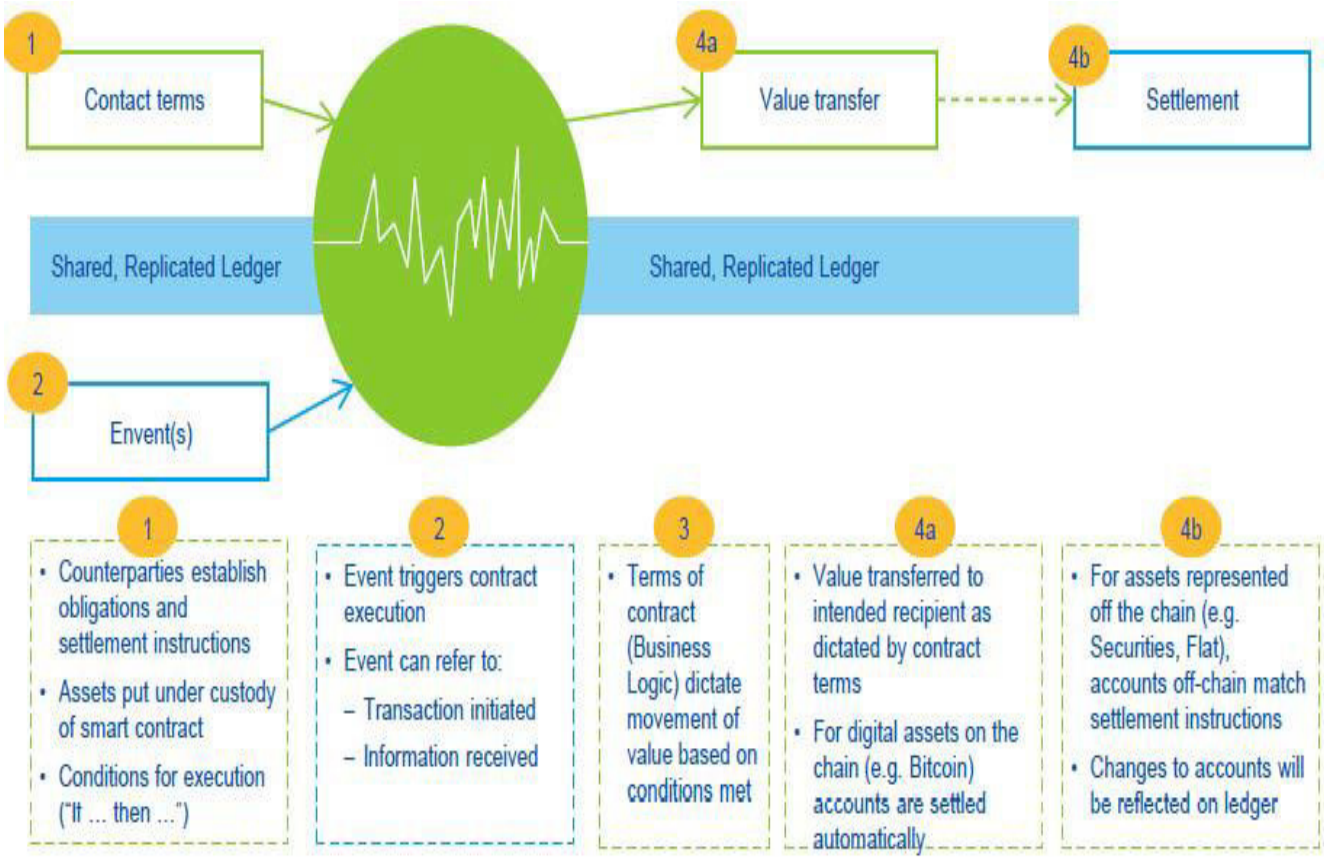


Figure 4: Working of Smart Contracts[34]

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[18].

1.3.2.1 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[19].

B. IoT

Using blockchain technology for your IoT data offers new ways to automate business processes between your partners without creating a complex and costly centralized IT infrastructure. This allows IOTs to participate in a blocking transaction.[10] Imagine again the most important business relationships in the world; Open the door and discover new styles of digital interactions; reduce costs and complexity in implementation.[11]

Biometrics in IoT Applications:

- Smart home
- Smart office
- Intelligent building system
- Healthcare & Hospitals.
- Financial services.
- Automotive Manufacturing.
- Infinite applications wherever Identification and confirmation is required.

1.4 INTERNET OF BIOMETRIC THINGS (IoBT)

The human-to-machine and human-to-human communications are transforming to machine-to-machine communications by which several decision-making systems can be built. When different Internet-enabled smart devices interact with each other to achieve a goal (application depended), then a network is formed in which different sophisticated technologies will integrate to each other to form Internet of Things (IoT). It encompasses the vast amount of diverse smart devices, which collaborate with each other to achieve different smart applications like smart cities, connected cars, automated agriculture, and so on. Through radio-frequency identification (RFID), wireless, mobile, and sensor technologies make IoT feasible, but it suffers from many challenges like scalability, security, and heterogeneity problems. Out of

many challenges, security is one of the primary concerns in IoT. Without proper security and privacy, the business model of IoT will not succeed. Here we discuss the secure solutions for IoT using biometric features of users as well as end users. It demonstrates that biometric security is most feasible, reliable, and efficient with respect to other existing security arrangements.

The Internet of Things (IoT) concept enables connectivity of billions of devices that have computing, communication and sensing capabilities. For the sake of scalability and cost-efficient service provisioning, integration of cloud-computing into the IoT architecture is inevitable while provisioning IoT services. In the literature, this architecture is referred as cloud-centric IoT [14], [15].

Security is reported as a grand challenge in IoT where the objects are seamlessly connected, as well as in cloud systems where resources are virtualized. Identification and authentication of users appear to be among the most crucial security issues against spoofing attacks [16]. As a robust solution, use of biometric identity for access control in cloud computing has been proposed by several researchers [17], [18]. However, biometric authentication has not been considered for IoT applications. The reason behind this is two-fold: 1) IoT architectures aim at automated service and resource discovery with no human intervention [19] whereas biometric identification may require direct biometric inputs from the user, 2) Both hard and soft biometric identification schemes require decision making systems that include identity prediction classifiers and meta-biometric prediction classifiers [20], and the tiny IoT objects such as wearable sensors and other personalized IoT devices may have limited computing capability.

Given that the cloud-centric IoT architecture is inevitable, it is viable to manage access control to the IoT objects via biometrics on a cloud-centric IoT architecture. We introduce the Internet of Biometric Things (IoBT) concept as illustrated in Fig. 2 minimally. As seen in the figure, biometric data is collected through IoT devices and transmitted to the cloud where liveness detection and anti-spoofing procedures [21] run for identification and authentication purposes. It is worthwhile noting that the IoBT architecture should allow multi-modal biometric identification to improve robustness against spoofing attacks [22]. The contribution of this paper is not limited to the IoBT concept but it also introduces the combination of behavior metrics and biometrics within the IoBT architecture for the first time. Identification and quantification of unique behavioral patterns of human beings is named as behaviometrics [23]. Thus, our framework couples biometric and context-aware authentication techniques to protect mobile applications from unauthorized access by malicious users. Despite mobile platforms have recently been integrated with biometric identification methods such as fingerprint recognition, rich contextual information carried on these platforms have not been a part of identification. Therefore, we propose computational offloading of mobile devices and cloud-based context analysis to continuously authenticate an IoT device.

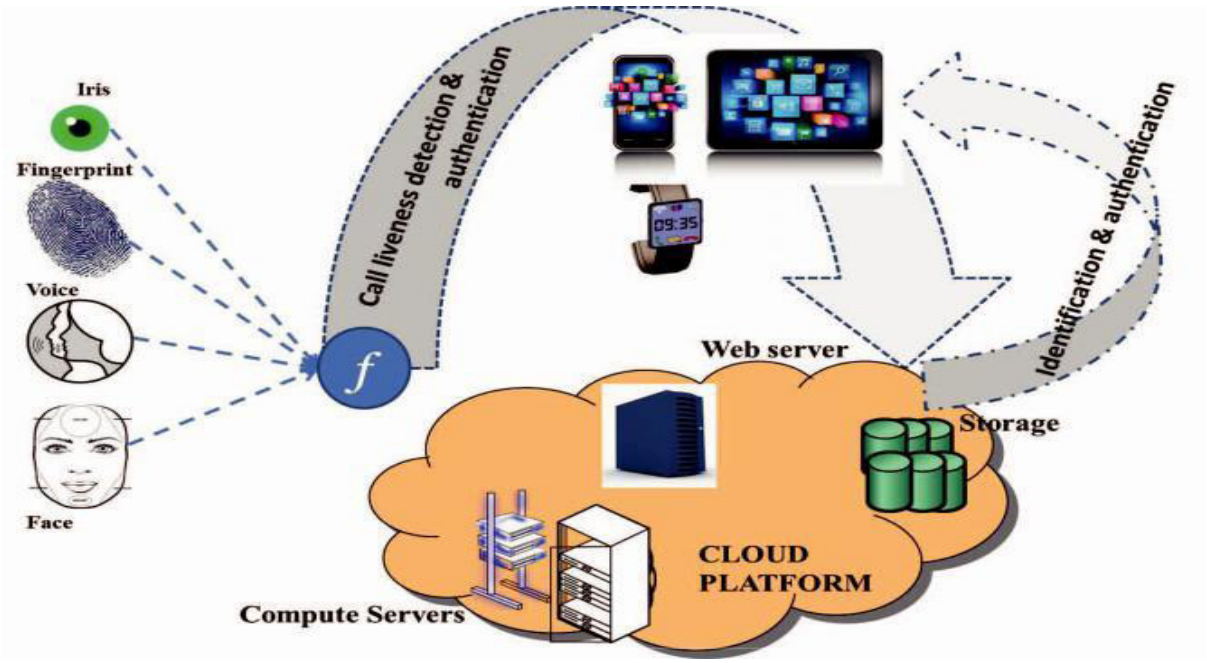


Figure 5.The Internet of Biometric Things (IoBT) concept [31]

1.5 Authentication Consideration for Internet of Everyday thing

1.5.1 IoT Adoption and Expansion

The 'Internet of Things' and IoT devices have been on the rise as of late due to a shift towards more 'cloud-centric' models of interconnected devices performing actions or integrating with the everyday life of users. Over time the hype and expectations of IoT technology have changed, but the overall desire to have a more vibrant and interconnected 'smart' Internet still runs deep in the human consciousness [20]. As one can see in the Figure 2, the Internet of Things will continue to grow and develop, all while influencing its domain by providing new evolving data and the required computational resources for allowing users and developers to create revolutionary applications [20]. With this expansion of use cases and implementations comes a requirement to examine the security needs and specifications that can secure the new flux of information and data from prying eyes or malicious action.

1.5.2 IoT Design & Security Considerations

IoT is generally a large number of wireless devices that form a network. The resulting 'Internet of Things' is as powerful as it is susceptible to the same vulnerabilities and security flaws as any computer system or distributed system of computers. Securing any stored data, ensuring access control to sensitive or critical areas of function, encrypting communications channels and authenticating new/connected devices are all aspects of IoT security that must be taken into consideration when designing everything from a single IoT device to a distributed network of IoT devices. Security considerations for IoT devices are the same as those required for distributed systems or embedded devices. One must secure not only the information being interacted with on an internal level, but also ensure that any data/information exported by the device must maintain a level of security assurance desired by the developer and user. Work byWest et. al. [40] has taken an in-depth analysis of the complications and errors that occur when security is implemented in fitness tracking IoT devices, along with a detailed postulation on how to suitably implement security policies and principles in an all-encompassing method. Common erroneous implementations of security lead to issues ranging from denial of service vulnerabilities, falsification of data (both local and remote users), stealing or abuse of sensitive information, compromise of device integrity, or as simple as incorrect handling of shared data leading to sensitive information being leaked. A developer's focus can be placed at a variety of abstractions, all with the intention of making a device, or larger system more secure and trustworthy. Beyond the security concerns, embedded systems have greater constraints in system design then other computer systems. Being an embedded system, the nonsecurity considerations boil down to power consumption, total PCB space, heat distribution, production costs, and component operation conditions. All of these different aspects play into the constraints and optimization of designing any secure embedded/IoT device.

1.5.3 INTERNET OF BIOMETRIC THINGS AUTHENTICATION

1.5.3.1 Biometrics in IoT

Biometric authentication, identification and key generation systems have assumed increasing importance in recent years. There are two types of biometric methods that can be categorized into internal and external physiological traits of humans. Each of the biometric modalities, including fingerprint based and iris based approaches, exhibits particular strengths and weaknesses. Fingerprints are very popular due to their low-cost implementation and well-

developed feature extraction approaches. Iris identification is acclaimed for its high-level security, providing unique features even for identical twins. Even though these kind of biometrics are common, they are easy for attackers to access and are not robust against cloning. For instance, our fingers are involved in many daily tasks such as touching keyboards and doorknobs and can be easily replicated to bypass biometric systems. Iris systems are susceptible to being spoofed by printed photos. They are also expensive

to implement. Electrocardiogram (ECG), Phonocardiogram (PCG), and Photoplethysmogram (PPG) are cardiovascular biometrics that are emerging as interesting choices for biometric systems that are internal physiological signals. Based on [31], bioelectrical signals recorded from the heart (electrocardiography, ECG) are distinctive enough for each individual person to be used for biometric applications, with the additional bonus of being inherently difficult, though not impossible, to forge. Also, they can be measured using low cost devices. Unlike other biometric systems, ECG signals can be monitored for prolonged periods of time: for example to continuously authenticate the user of a protected device after initial authentication. The Apple Watch applies the same principle of continuous monitoring, requiring the user to authenticate their identity with a password when the watch is strapped to their wrist, but then monitoring for constant heartbeat to avoid the need for further authentication. As additional security, once there is an interruption in the hearbeat detected by the watch, the watch locks itself down.

For the proposed key generation and authentication methodology there should be a requirement of two phases for implemented use: an enrollment phase where a user registers their ECG signal to generate keys, and an authentication phase where user provided data generates a new key that is compared to previous stored keys.Section 5 shows implementation of these phases for a postulated IoT device.

1.6 Ontology

In the last decade we faced a great number of publications in the field of biometrics and a lot of new biometric methods, techniques, models, metrics and characteristics were proposed. Due to this explosion of research, scientific and professional papers certain inconsistencies in terminology emerged. What some authors call a biometric method, others call model, system or even characteristic. There wasn't enough effort in creating a unique systematization and categorization which would approach the stated issues and open new areas of research. We argue that it is possible to approach biometrics in a narrower and in a broader perspective. We observed biometrics in the narrower one and created a unique framework for the systematization and categorization of biometric methods, models, characteristics and patterns

based on a general biometric system. This systematization is a fundamental step forward towards the creation of an open biometrics ontology.

With the fast adoption of cloud computing, the use of biometric technologies has evolved to a different way of providing security, preserving privacy, and analysing personal traits for various purposes. The main components of any biometric system, such as biometric sensing, data gathering, feature extraction, identification, verification, recognition, and analytics, are now handled over distributed networks. Many of the biometric system services are presented over such networks which are followed by the creation of a new concept 'biometric-as-a-service (BaaS)'. Recent BaaS approaches usually focus on identifying the effective distributed architectures, policies, and use case recommendations. However, there is a strong need to focus on developing a semantic framework which should rely on a biometric ontology. This research presents such an ontology covering the uses of different biometric modalities, evaluation and assessment of biometric systems, modelling biometric processes, and analyses through interlinked relations with biometric stakeholders.

The so-called diversified usage of biometrics has brought the distributed use of biometric services which significantly boosts the need on biometric-as-a-service (BaaS). Whatever the field of application considered, the biometric systems rely on distributed networks where remote authentication, remote analysis, or tracking are conducted. Within these distributed networks, secure transaction of too much data has become an issue where biometric services contribute to the creation of big data over networks [8]. The use of BaaS in coordination with other layers of cloud environments, such as infrastructure-as-a-service (IaaS), platformas-

a-service (PaaS), and software-as-a-service (SaaS), has become forward to provide effective and parallel use of biometric services at different locations and times. Here, there is a strong need to cover such a highly diversified use of biometric services by considering all stakeholders and different application areas. Hence, any intelligent approach incorporating the diversified use cases and linking them with main biometric concepts like modalities, evaluation factors and metrics, biometric processes, and biometric analyses is now an emerging need.

2. Motivation

Main motivation is to implement the traditional Biometrics for Internet of Biometric things. Establishing, Evolving Authentication Consideration Architectures with the help of Cryptographic mechanisms or lightweight cryptographic algorithm for the process. To make the system scalable in which thousands of clients can connect simultaneously and to get wide appreciation, it needs to be deployed on cloud infrastructure in form of Biometric authentication as a Service i.e. BaaS.

Further a biometric ontology that can be centered in cloud-based biometric service platforms relying on BAAS concept will be developed for every deployment Blockchain Technology adds the immutable aspect to the system. So addition or the possibilities in the cloud based architectures using BlockchaindB to store biometric traits or transaction logs will be explored to add further the notion of the immutability to the proposed architecture. There end to end secure IoBT deployment will be further integrated with smart contact to make ready for enterprise application such as trade and finance.

3. Literature Review

The literature survey is carried out by referring papers from reputed journal like IEEE Transaction, Springer, and Elsevier. The literature survey is summarized in table 1 as shown below.

Table 2: literature Survey

Sr. No.	Title of the paper	Publication	Authors	Key Finding	Gap Identified
1	Biometric ontology for semantic biometric-asa-service (BaaS) applications: a border security use case	IET, 2018	Alper Kanak	Reviewed recent advances in biometric authentication and pointed out potential risks and proposed evaluation criteria for measuring performance of classifiers.	Verification of the ontology in a realistic case is another study left for further attempts. Additionally, new biometric modalities, performance criteria, or analysis methods can be defined to get a more improved version of the biometric ontology.
2	Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments	IEEE, 2017	Afan Ali, Fan Yangyu	Design of an effective blockchain-based database for cloud computing environments.	Researching on the feasibility of emodeled more stable blockchains is fundamental to enable their wide adoption as reliable storage infrastructures, e.g.in the context of cloud computing environments
3	Building Secure Infrastructure for Cloud Computing using Blockchain	IEEE, 2018	Shweta Gaur Sharma, Dr.	Compare the various platforms on which blockchain can be implemented. The paper illustrates the	Different platforms are not yet exposed to the radical cloud conditions in terms of data integrity.

			Laxmi Ahuja	use of Blockchain applications for building secure infrastructure of cloud computing.	
4	Dynamic Deployment and Auto-scaling Enterprise Applications on the Heterogeneous Cloud	IEEE, 2016	Satish Narayana Srirama, Tverezovskyi Iurii, Jaagup Viil	This paper joined the approaches of multi-cloud deployment using CloudML and identifying the ideal resource provisioning and deployment configuration using an optimization model, in order to dynamically scale an enterprise application across multiple clouds, without any user intervention.	Following the approach and joining the CloudML and optimal resource provisioning policy, we would like to achieve a framework to which any enterprise application can be provided, which would be studied, modeled, migrated to, performance monitored and auto-scaled on the cloud, seamlessly.
5	ProvChain: A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability	IEEE, 2017	Xueping Liang, Sachin Shetty, Deepak Tosh, Charles Kamhoua, Kevin Kwiat, and	Proposed a decentralized and trusted cloud data provenance architecture using blockchain technology.	Provchain was not develop for federated cloud provider. Validation is not done on top of an open source architecture which impact overall performance, security and flexibility.

			Laurent Njilla4		
6	Biometric Authentication using Software as a Service (SaaS) Architecture with real-time insights	IEEE, 2016	Mr. Godson Michael D'silva,Dr. Vinayak Ashok Bharadi	Proposed a highly secure, scalable, pluggable and faster biometric system architecture, that can handle a billion of biometric events per second that are going to come from the devices, guaranteed delivery and processing of the biometric events, faster enrollment and verification process, fault tolerant & infinitely scalable database	No Internet of Biometric Things implemented. Authors has not proposed security mechanism. Scalable architecture with latest cloud tools needs to explored.
7	Biometrics-as-a-Service: A Framework to Promote Innovative Biometric Recognition in the Cloud	IEEE, 2018	Veeru Talreja, Terry Ferrett,Matthew C. Valenti, Arun	Put forth a framework to deploy Biometric Recognition as a Service(BaaS)	Optimal matching algorithm selection and using concepts from game theory to determine optimal pricing points has not been implemented.
9	Biometric Authentication as a Service (BaaS): a NOSQL Database and CUDA based Implementation		Vinayak Ashok Bharadi, Harshad A.	Paper discussed biometric authentication system architectures that will enable	No SQL database is used Instead of Blockchaindb Which provides more

			Mestry, Abhinav Watve	massive scalability and speed for the BaaS. In the first part the work a scalable biometric system is proposed with a Column Family Database, this will enable massive scaling capacity and other implementation is done with NVIDIA CUDA based architecture for faster feature vector extraction, both the implementations will serve as building blocks for faster and scalable Biometric Authentication as a Service.	Security.
10	An Overview of Smart Contract: Architecture, Applications, and Future Trends	IEEE, 2018	Shuai Wang, Yong Yuan, Xiao Wang, Juanjuan Li, Rui	Discussed the immutable and irreversible characteristics of smart contract	Integration of SaaS with permissioned blockchain to automate execution of smart contract is an untouched issue.

			Qin, Fei-Yue Wang		
11	On the Road to the Internet of Biometric Things: A Survey of Fingerprint Acquisition Technologies and Fingerprint Databases	IEEE, 2016	Fatimah Al-alem, Mohammad A. Alsmirat and Mahmoud Al-Ayyoub	Internet of Biometric Things (IoBT) mixes traditional biometric technologies with context-aware authentication techniques	No Blockchain databaseused.
12	Towards secure cloud-centric Internet of Biometric Things	IEEE, 2015	Burak Kantarci, Melike Erol-Kantarci, Stephanie Schuckers	The cloud-centric authentication in IoBT couples biometric and context-aware authentication techniques to protect mobile applications from unauthorized access by malicious users.	No end to end lightweight cryptography implemented.

4. Research Problem

The purpose of research is to implement Authentication consideration architecture, implement cryptography or key generation or secure communication in IoBT(Internet of Biometric Things), developing architecture which is automatically scalable and exposing this system as BaaS. Further augment the architecture by exploring services provided by various cloud service providers.To make transaction secure and accountable by using BlockchainDB by storing authentication transaction in it, adding provenance of transaction and immutability. To develop a biometric ontology for the overall architecture that can be center in cloud-based biometric service platforms relying on BaaS concept. Deploy unimodal and multimodal Biometric Authentication on cloud which will integrate smart contract for automation.

5. Research Objectives

The aim of this research is:

Our Proposed system as shown in the figure 4 is deployed on cloud along with GPU.It is scalable .Its security an aunthencity can be increase by using blockchaindb .Record or authentication request cannot be altered thus making it immutable. Scope of Research for the purposed system will be

1. Deploying Unimodal and Multimodal Biometric Authentication Systems on Cloud in SaaS type of Cloud Deployment model to provide Biometic Authentication as a Service (BaaS) [24],[25],[26].

2. Design Cloud application architectures for the low latency service needs by the use of GPU, Hybrid clouds [25].

3. To recognize the perfect asset provisioning and arrangement design utilizing an advancement model, to progressively scale a venture level application over various clouds, with no client mediation [26-28].

5. Evolving Authentication Design Considerations and cloud application architecture for the Internet of Biometric Things (IoBT) which will be secure and privacy-preserving solutions guaranteeing privacy properties such as anonymity, unlinkability, minimal disclosure of personally identifiable information, as well as assuring security properties, such as content integrity and authenticity. [29-31].

6. Integrating Blockchain Database with the proposed systems for better Provenance support for the Biometric traits enrollment, update and matching [12],[13], [14].

6. Research Design

In the proposed architecture ensemble or composite classifier with favorable accuracy and computational cost will be deployed on cloud to avail it in form of Biometric Authentication as a Service (BaaS). 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 authentication biometric recognition.Develop ontology model for the purposed system

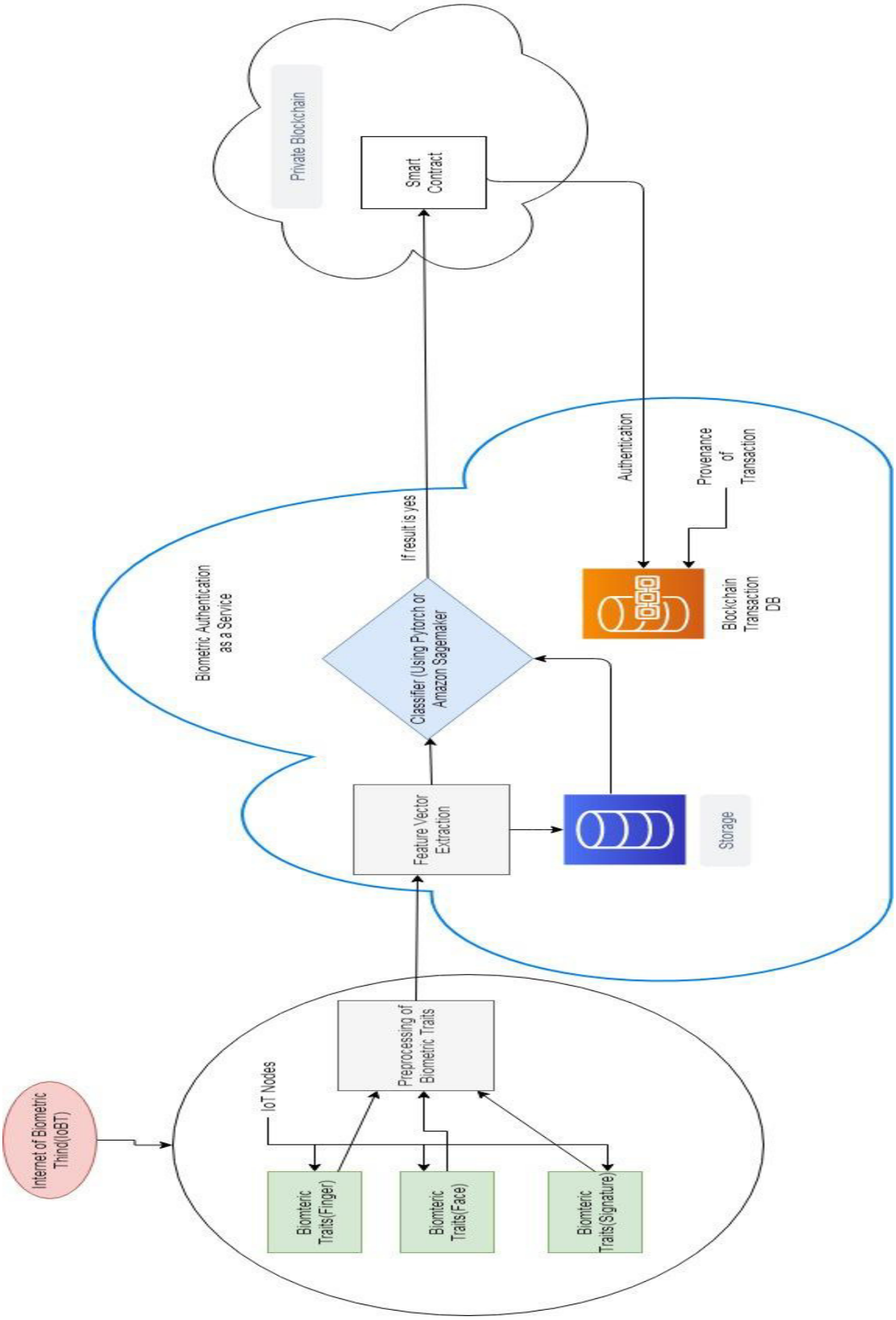
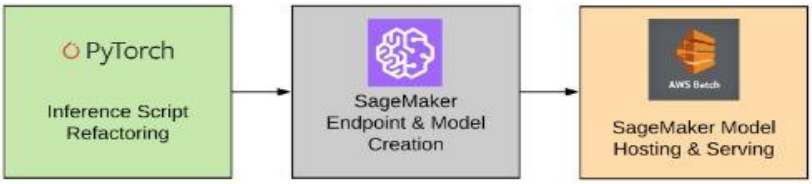


Figure 6 Proposed Architecture of a Biometric Authentication as service (Baas) running on AWS and Blockchain Database

6.1 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 authetication 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]



ii. **Permissioned blockchain:** Hyperledger Fabric (HLF) is an open-source implementation of a distributed ledger platform for running smart contracts in a modular architecture. The execute-order-validate blockchain architecture introduced by fabric could be employed for permissioned blockchain.

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].

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	**Cloud Computing [19]**		
	i	**Service capability**	Service capability is the degree of capability in a service system to provide services and is commonly defined as the maximum output rate of the system.
	ii	**Security**	Cloud solution adhere to industry standard policies like SSAE16 and PCI DSS.
	iii	**Accuracy**	The capability of correctly classifying an individual as an imposter or a legitimate user.
	iv	**Disaster recovery**	It involves a set of policies, tools and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.
	v	**Cloud service scalability**	System ability to sustain increasing workloads by making use of additional resources.
	vi	**Cloud service elasticity**	It is an ability of a system to adapt to change in workloads and resource demands.
2.	**Biometric Recognition System Software as a Service** [20]		
	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.

<table>
<tr><td>3.</td><td colspan="3">Blockchain based Smart Contract</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 rowspan="7"></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>Broadcast latency</td><td>The time delay between client submitting to orderer and orderer acknowledges the client.</td></tr>
<tr><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>Ordering latency</td><td>The time transaction spent on the ordering service.</td></tr>
<tr><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>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>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 architecture for Internet of Biometric thing (IoBT) i.e. biometric authentication as a service (BaaS).
- **ii.** Integrated smart contract based enterprise application which need user authentication to perform transaction such as trade execution, etc.

9. Conclusion

In this we have a proposed an Architecture of a Biometric Authentication as service (Baas) which runs on cloud platform like AWS, Microsoft Azure and Google cloud. Internet of Biometric things (IoBT) will be used to capture biometric data. Biometric ontology that can be centered in cloud-based biometric service platforms relying on BAAS concept will be developed. For security end to end lightweight cryptography will be implemented. Also there will be integration of smart contract based enterprise application which need user authentication to perform transaction.

Presented paper: **Mr. Pravin Jangid, Dr. Vinayak Bharadi**, presented paper on "**Evolving Authentication Design Consideration and BAAS Architecture for Internet of Biometric things**", at the **IEEE International Conference** on **Convergence to Digital World (ICCDW)-Quo Vadis** from 19th to 20th **February, 2020.**

References

[1] H B Kekre, V A Bharadi, "Dynamic Signature Pre-Processing By Modified Digital Difference Analyzer Algorithm" , Proceedings ofThinkQuest 2010, Mumbai India

[2] A. K. Jain, P. Flynn, A. A Ross, "Handbook of Biometrics", Springer,USA, ISBN-13: 978-0-387-71040-2, pp.:1-23, 2007.

[3] A. K. Jain, A. Ross, S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, January 2004.

[4] A. Kanak, "Biometric ontology for semantic biometric-as-a-service (BaaS) applications: a border security use case," in IET Biometrics, vol. 7, no. 6, pp. 510-518, 11 2018. doi: 10.1049/iet-bmt.2018.5067

[5] Shweta Gaur Sharma, Dr. Laxmi Ahuja, "Building Secure Infrastructure For Cloud Computing using Blockchain", Proceedings of the Second International Conference on Intelligent Computing and Control Systems(ICICCS 2018)

[6] Edoardo Gaetani, Leonardo Aniello, Roberto Baldoni , Federico Lombardi , Andrea Margheri , Vladimiro Sassone "Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments", In Proceedings of the First Italian Conference on Cybersecurity (ITASEC17), Venice, Italy,2017

[7] Castiglione, A., Choo, K.-K.R., Nappi, M., et al.: 'Biometrics in the cloud: challenges and research opportunities', IEEE Cloud Comput., 2017, 4, pp. 12–17

[8] Talreja, V., Ferrett, T., Valenti, M.C., et al.: 'Biometrics-as-a-service: a framework to promote innovative biometric recognition in the cloud'. arXiv preprint arXiv:1710.09183, 2017

[9] Stojmenovic, M.: 'Mobile cloud computing for biometric applications'. 2012 15th Int. Conf. Network-Based Information Systems (NBiS), 2012, pp. 654–659.

[10] Bommagani, A.S., Valenti, M.C., Ross, A.: 'A framework for secure cloudempowered mobile biometrics'. Military Communications Conf. (MILCOM),2014, 2014, pp. 255–261ystems (NBiS), 2012, pp. 654–659

[11] Ross, A., Jain, A.K.: 'Multimodal biometrics: an overview'. 2004 12th European Signal Processing Conf., 2004, pp. 1221–12249

[12] Anniruddha S. Rumale, Dinesh N. Choudhari, "Cloud Computing: Security Issues and Measures", 2014

[13] Anniruddha S. Rumale, Dinesh N. Choudhari, "Cloud Computing: Software as a Service", 2017 IEEE.

[14] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645 – 1660, 2013.

[15] B. Kantarci and H. T. Mouftah, "Trustworthy sensing for public safety in cloud-centric Internet of Things," IEEE Internet of Things Journal, vol. 1/4, pp. 360–368, Aug 2014.

[16] Honggang Wang, Shaoen Wu, Min Chen, and Wei Wang, "Security protection between users and the mobile media cloud," IEEE Communications Magazine, vol. 52, no. 3, pp. 73–79, March 2014.

[17] K. Huang, J. Shi, M. Xian, and J. Liu, "Achieving robust biometric based access control mechanism for cloud computing," in International Conf. on Information and Network Security (ICINS), Nov 2013, pp. 1–7.

[18] S. Sharma and V. Balasubramanian, "A biometric based authentication and encryption framework for sensor health data in cloud," in International Conf. on Inf. Tech. and Multimedia, Nov 2014, pp. 49–54.

[19] S. Cirani, L. Davoli, G. Ferrari, R. Leone, P. Medagliani, M. Picone,and L. Veltri, "A scalable and self-configuring architecture for service discovery in the internet of things," IEEE Internet of Things Journal,vol. 1, no. 5, pp. 508–521, Oct 2014.

[20] M.C. Da Costa Abreu and Michael Fairhurst, “Enhancing identity prediction using a novel approach to combining hard- and soft-biometric information,” IEEE Trans. on Systems, Man, and Cybernetics, Part C:Applications and Reviews, vol. 41, no. 5, pp. 599–607, Sept 2011.

[21] B. Tan, A. Lewicke, D. Yambay, and S. Schuckers, “The effect of environmental conditions and novel spoofing methods on fingerprint antispoofing algorithms,” in IEEE International Workshop on Information Forensics and Security (WIFS), Dec 2010, pp. 1–6.

[22] Johnson. P. A., F. Hua, and S. Schuckers, “Comparison of qualitybased fusion of face and iris biometrics,” in International Joint Conf. on Biometrics (IJCB), Oct. 2011, pp. 1–5.

[23] J. Zhu, h. Hu, S. Hu, P. Wu, and J.Y. Zhang, “Mobile behaviometrics: Models and applications,” in IEEE/CIC International Conf. on Communications in China (ICCC), Aug 2013, pp. 117–123.

[24] Bharadi, V.A., D'Silva, G.M.: ‘Online signature recognition using software as a service (saas) model on public cloud’. 2015 Int. Conf. ComputingCommunication Control and Automation (ICCUBEA), 2015, pp. 65–72.

[25] R. Sahl, P. Dupont, C. Messager, M. Honnorat and T. Vu La, "High-Resolution Ocean Winds: Hybrid-Cloud Infrastructure for Satellite Imagery Processing," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2018, pp. 883-886. doi: 10.1109/CLOUD.2018.00127.

[26] Shwe, H. Y., & Chong, P. H. J. (2016). Scalable Distributed Cloud Data Storage Service for Internet of Things. 2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld). doi:10.1109/uic-atc-scalcom-cbdcom-iop-smartworld.2016.0137.

[27] Srirama, S. N., Iurii, T., & Viil, J. (2016). Dynamic Deployment and Auto-scaling Enterprise Applications on the Heterogeneous Cloud. 2016 IEEE 9th International Conference on Cloud Computing (CLOUD). doi:10.1109/cloud.2016.0138

[28] T. Kiss, "Scalable multi-cloud platform to support industry and scientific applications," 2018 41st International Convention on Information and Communication

Technology, Electronics and Microelectronics (MIPRO), Opatija, 2018, pp.0150-0154. doi: 10.23919/MIPRO.2018.8400029.

[29] O. Olazabal et al., "Multimodal Biometrics for Enhanced IoT Security," 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2019, pp. 0886-0893.doi: 10.1109/CCWC.2019.8666599

[30] Roy, S., Chatterjee, S., Das, A. K., Chattopadhyay, S., Kumari, S., & Jo, M. (2018). Chaotic Map-Based Anonymous User Authentication Scheme With User Biometrics and Fuzzy Extractor for Crowdsourcing Internet of Things. IEEE Internet of Things Journal, 5(4), 2884–2895. doi:10.1109/jiot.2017.2714179.

[31] N. Karimian, P. A. Wortman and F. Tehranipoor, "Evolving authentication design considerations for the Internet of biometric things (IoBT)," 2016 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS), Pittsburgh, PA, 2016, pp. 1-10.

[32] J. L. C. Sanchez, J. B. Bernabe and A. F. Skarmeta, "Towards privacy preserving data provenance for the Internet of Things," 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 2018, pp. 41-46. doi: 10.1109/WF-IoT.2018.8355229

[33] Y. Zhu, Z. Zhang, C. Jin, A. Zhou and Y. Yan, "SEBDB: Semantics Empowered BlockChain DataBase," 2019 IEEE 35th International Conference on Data Engineering (ICDE), Macao, Macao, 2019, pp. 1820-1831. doi: 10.1109/ICDE.2019.00198.

[34] 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.

[35] 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

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

[37] Suporn Pongnumkul, Chaiyaphum Siripanpornchana, and Suttipong Thajchayapong, “Performance Analysis of Private Blockchain Platforms in Varying Workloads”, IEEE,2017