IoT based Smart Band for Biometric Authentication Using Blockchain Technology

S.V. Abishek, G.M. Dhuruva Priyan, Sridatt More, A. Suganthan

Abstract--- Internet of Things has been 'the next big thing' for a while now and it is estimated that the number of connected devices will exceed 50 billion by 2020. This extravagant growth in number of connected devices has alarmed us to shift the approach in designing identity and access management systems. People tend to provide different passwords and identifications for each of the platforms they use. This could be troublesome as they might forget their password and lose their identifications as well. One more problem is that the user doesn't know if he is providing only the necessary information or he is exposing himself to something he is not supposed to. This makes us think about a solution where the user provides minimum amount of his personal information for verification. We propose an IoT based solution using smart band with fingerprint biometric system to achieve the idea of "one touch multiple login" (i.e. single band to authenticate multiple platforms). We have addressed the Self-sovereign identity crisis using blockchain technology and its derived protocols.

Index Terms--- Biometric, Blockchain, Internet of Things(IOT), Self Sovereign Identity, Smart Band.

I. INTRODUCTION

Internet of Things

Internet of Things, also referred to as Internet of Objects, creates opportunities for more direct integration of the physical world into computer-based systems, resulting in efficiency improvements, economic benefits, and reduced human exertions. The Internet of Things (IoT) is a system of interrelated physical devices, vehicles, and other items embedded with electronics, software, sensors, actuators and connectivity which enables transfer of data over a network without requiring any interaction between humans and computers. The user interacts with the system through a user interface and the devices connected to the system listen to the network and act according to the user's inputs.

IoT is one of the most researched topics globally and the concurrent development in Cloud services and their related APIs will proliferate IoT based applications and the marketplaces that offer them. IHS forecasts that the IoT market will grow from an installed base of 15.4 billion devices in 2015 to 30.7 billion devices in 2020 and 75.4 billion in 2025.With the things/people ratio growing at 1.84 (as of 2010 survey conducted by CISCO), time is not far for IoT making a great impact on our lifestyle.

The current trend in Biometrics

Internet of Things is playing an important role in biometric authentication. There are a number of devices sending and receiving information continuously. There is a need to keep this data out of the hands of an unauthorized individual, but passwords are cumbersome and sometimes consumers use the same password for multiple devices. This makes their identity insecure and they are vulnerable to hacking as the probability of human error cannot be ruled out. Relying on passwords for authentication is risky as they can be easily stolen. Therefore, it is clear that a strong and better form of security is required to protect devices and sensitive data. Biometric traits being inherent and unique to each individual is an effective way to prove his identity. It comprises his physical and behavioural characteristics such as fingerprints, face, iris, gait, voice etc. Biometric security systems can verify an individual's identity with great accuracy and reliability since biometric traits are part of the individual. Fingerprint biometrics are becoming the most common identity feature in smartphones. More than 1 billion fingerprint scanner-equipped phones are going to be shipped in 2018.

Biometric security systems

Although biometric security systems can mitigate the problems associated with the use of passwords, tokens and smart cards, these systems themselves are susceptible to spoof and link-ability attacks. Fingerprint recognition devices can easily be fooled by a fake finger created with gelatin and a plastic mold. Linking of users across applications based on their biometric data is referred to as the link-ability attack.

The process of capturing the biometrics and identifying is significant. Inaccurate results after capturing or partial capture of data and binding can lead to failure of the system. One of the major challenges is also to protect the public by preventing the abuse of biometric technology. Policies and standards need to be established that helps the application of biometrics to many emerging technologies such as the Internet of Things, banking, fraud protection and connected cars. A huge tool to fight hacker's attempts would be providing adequate liveness detection in both online and remote authentication scenarios and is important to maintain user's trust and peace of mind when using biometric systems [8].

Revised Version Manuscript Received on 22 February, 2019

S.V. Abishek, Dept of Computer Science and Engineering, Amrita School of Engineering, Coimbatore. Amrita Vishwa Vidyapeetham, India. (e-mail: abisheksv5@gmail.com)

G.M. Dhuruva Priyan, Dept of Computer Science and Engineering, Amrita School of Engineering, Coimbatore. Amrita Vishwa Vidyapeetham, India. (e-mail: gmdhuruva@gmail.com)

Sridatt More, Dept of Computer Science and Engineering, Amrita School of Engineering, Coimbatore. Amrita Vishwa Vidyapeetham, India. (e-mail: moresridatt@gmail.com)

A. Suganthan, Dept of Computer Science and Engineering, Amrita School of Engineering, Coimbatore. Amrita Vishwa Vidyapeetham, India. (e-mail: suganthansharvesh@gmail.com)

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication*

Biometric security is becoming more prevalent and sophisticated with the technological advancements and is a breakthrough in authentication systems. But the incidents like Equifax data breach, OPM theft of 5.1 million fingerprints brings the necessity of a reliable security system [10]. Current biometric security solutions involve merging of biometrics and cryptography to provide security[13] whereas the true security lies in user controlling his identity. A solution would be to combine biometrics with blockchain technology leading to a stronger security system.

II. TECHNOLOGY

Basic Terminologies

IoT Sensors: A) Capacitive Fingerprint Sensor: The Capacitive Fingerprint Reader is a standard fingerprinting module intended for additional improvement, permits quick and stable unique fingerprint check.

Capacitive Sensors: A capacitive sensor is activated by the slight electrical charge running through your skin. We all have a small amount of electrical current running through our bodies, and capacitive technology utilizes that to sense touch. Based on the lightning-speed digital processor STM32F105R8, joined with high-security commercial finger printing algorithm, and state of the art semiconductor sensor technology, the Capacitive Fingerprint Reader turns into a simple but smart integrated module, gives functionalities like fingerprint enrolling, image processing, feature finding, template generating and storing, fingerprint matching and searching, etc.

RFID Overview

Radio Frequency Identification (RFID) is an information gathering innovation like standardized tags, yet as opposed to scanning a barcode it utilizes radio frequency to gather information from RFID labels. It is normally alluded to as programmed recognizable proof or auto-id, since it utilizes radio waves to uniquely distinguish objects, for example, resources, stock, individuals or creatures. An electronic tag (transponder) is installed with an integrated circuit (IC) that can store unique information about the application being labeled. A reader(interrogator) transmits radio waves at a radio frequency to speak with and recover information from labels in its vicinity. The two such RFID readers used in this paper are: NFC RFID (High Frequency) reader Ultra-High Frequency RFID reader

HSM module

An HSM can perform multiple important security-related functions. It provides accelerated cryptographic operations such as encryption, digital signatures, hashing, and Message Authentication Codes. A Message Authentication Code (or MAC) is an algorithm that mathematically combines a key with a hash to provide a "code" that can be appended with a given piece of data to ensure its integrity.

Wi-Fi module

The module must provide a simple, safe and scalable WIFI solution, allowing it to host an application over Wi-Fi networking. Alternatively, serving as a Wi-Fi adapter, wireless internet access should be to any microcontroller-based design with simple connectivity.

Blockchain Technology: Blockchain is a decentralized incorruptible digital ledger that contains information about the transactions that happen in a peer to peer network. The blockchain is a growing list of records, called blocks, that are linked cryptographically. Each block contains a cryptographic hash of the previous block, a timestamp, transaction data and the computed proof-of-work.

The transactions are verified by a group of special nodes in the network called miners, thereby removing the need for a centralized authority. This process is lot more secure than a traditional database because thousands of computers spread throughout the world validate and keep record of the transactions in the network.

Biometric Open Protocol Standards (BOPS)

Biometric authentication demands high assurance levels such as those required by national and international standards [1]. The IEEE 2410 – 2017 Biometric Open Protocol Standards (BOPS) [2] defines the following elements to achieve the required level of assurance. Collection: The biometric templates should be collected via a hardware security module (HSM), using an application programming interface running in a trusted execution environment (TEE) or trusted platform module (TPM). Such facility when possible will ensure inaccessibility and encrypted memory, to prevent exfiltration of biometric data. Storage: BOPS specifies methods for storing biometric templates in which half the share of biometric template is stored in local machine and the second half is sent to a remote platform. Unauthorized access to any one of the shares does not compromise the complement share nor the biometric template. Transmission: BOPS defines a Representative state transfer (REST) protocol in which the biometrics are encrypted using server's public key before getting transmitted over a two-way TLS channel.

Processing: BOPS allows the matching of templates only in volatile memory or using the local HSM, but never allows any other form of non-transient storage such as files, databases, or other long-term storage media.

Self-Sovereign Identity Ecosystem

In the traditional authentication and identity models, users are forced to waive their personal information such as credit histories, credentials such as birth certificates, or biometric data to a third party, with a centralized database. These authentication systems come with security flaws like data breach and identity theft, which creates the necessity of a new identity ecosystem. Self-Sovereign Identity is a new decentralized ecosystem for private and secure identity management where individuals control and manage their identities. This system is persistent, peer-based, privacy protecting and portable. Existing solutions for Self-Sovereign Identity include Sovrin, Ethereum Uport, Veres One. Although each of these supports decentralized, self-sovereign identity, they are different in the way claim is issued. There are various standards being developed for decentralized identifiers and verifiable claims to provide interoperability.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Unlike the current broken online identity system, Self Sovereign Identity systems will reduce transaction costs, protect user's personal information, prevent cybercrime, and solves identity challenges in healthcare, banking, voter fraud. Moreover, self-sovereign identity solutions provide a way in supporting human activities without threatening their privacy. Self-Sovereign Identity is enabled by more than 10 emerging standards but one of them that is central among others is the Decentralized Identifiers (DID) Standard. DIDs are the fundamental building block of the Self-Sovereign Identity system. A DID is a decentralized, cryptographically verifiable identifier that is persistent, and no centralized registration authority is required. There are a certain set of rules being devised that state how to format a DID document and support the universal resolution. These rules are known as DID standards. DIDs are used as they ensure interoperability. Without using a DID, an organization cannot leverage the power of the interoperable standards. Protocols are both freeing and constraining. Newly documented methods can be added with the help of DID Standards. The following are the brief descriptions of DID architecture.

DID: A globally unique identifiers, registered in a distributed ledger or other form of decentralized network. It resolves to a standard resource describing an entity (a DID document)

DID document: The DID Document typically contains cryptographic material that enables authentication of an entity associated with the DID. The information includes mechanisms to authenticate a DID (e.g., biometric templates, biometric templates or even encrypted part of biometric data). Next, a set of authorization information that outlines which entities may modify the DID document. It also contains a set of service endpoints, which may be used to initiate trusted interactions with an entity. Verifiable claim: Any statement that can be made on the qualification, achievement, quality, or piece of information about an entity's background such as a name, government ID, payment provider, home address, or university degree. Such a claim to the entity establishes its own digital and verifiable identity which is used to confirm that its association with the organization. Identity hubs and repositories: Identity hubs (e.g., Dropbox, Google drive, Stroj) are personal data repositories that curate and coordinate the storage of signed/encrypted DID document. Issuer: An entity which provides verifiable claims to a holder. Issuers can be an organization, government, employer, individual. Etc. The Verifiable claim is cryptographically secured using issuer signature.

Inspector/Verifier: The inspector verifies the claim provided via DID and DID document, also checks the validity of the DID in the blockchain. The inspectors include employers, security personnel, service providers. Etc.

Holder: The entity associated with a DID and its corresponding DID document. The holder has full control on how his/her identity is used. The holder can be a student, an employee, a customer. Etc.

III. IMPLEMENTATION

Smartband

Smartband consists of a Wi-Fi module, RFID reader, Capacitive fingerprint sensor and a HSM module. The Wi-fi module in the smartband is used to connect to the verification system through a dedicated Virtual Private Network. A small RFID reader is set up for reading the high/low frequency RFID tags. A capacitive fingerprint sensor is used for verification purposes. A capacitive sensor plate at the back side of the band helps to identify if the user removed the band. All data from the band is encrypted or decrypted through HSM module in the band. RFID reader and Capacitive Fingerprint sensors are internally connected to a microcontroller present in the band.

Enrollment

Enrollment is registering the user in the public blockchain after verifying his/her identity initially. The process of enrollment is given below:

Step 1: The enrollment procedure starts with an application interface prompting the user to provide his/her biometric (fingerprint) and is collected as Initial Biometric Vector (IBV).

Step 2: The application generates a unique public-private key pair.

Step 3: The Initial Biometric Vector is divided into two shares and both the shares are encrypted using the enrollment private key.

Step 4: One half of the encrypted share is secured locally using the HSM module in the smart band.

Step 5: The encrypted second half and the enrollment public key is sent to a BOPS server to generate a DID and its corresponding DID document.

Step 6: The DID along with the enrollment public key is added as a new record into a block in the blockchain.

Step 7: The issuer grants the verifiable claim and signs (encrypts) with the issuer's private key (which forms the issuer's signature).

Step 8: The lock state of the band is encrypted using the Organization's private key.

Step 9: The DID document containing (1) DID, (2) enrollment public key, (3) verifiable claim, (4) issuer's signature, (5) lock state, (6) encrypted second share of the initial biometric vector is created. The DID document is then stored in an Identity Hub.

Step 10: The DID and the public-private key pair is returned to the user and is securely stored using HSM module in the smart band.

Verification

When the band is in the unlocked state.

Step 1: The user is prompted to enter his/her fingerprint as he wishes to wear the smart band. This fingerprint is collected as a Collected Biometric vector (CBV).

Step 2: The connection is established between the band and the verification system using BOPS transmission protocol.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Step 3: The Collected Biometric Vector is encrypted using the private key.

Step 4: The DID, the enrollment public key, Encrypted CBV, the Encrypted Local share is securely sent from the HSM module to verification system using BOPS transmission protocol

Step 5: The credential verification is done in remote BOPS server.

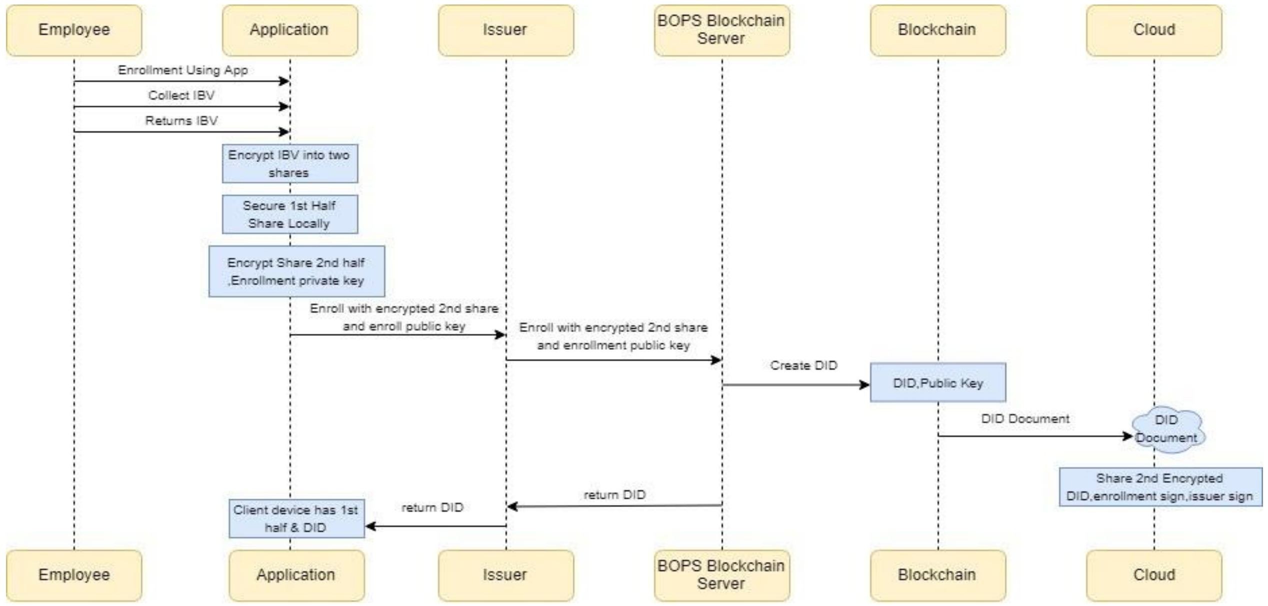

Employee
Application
Issuer
BOPS Blockchain Server
Blockchain
Cloud
Enrollment Using App
Collect IBV
Returns IBV
Encrypt IBV into two shares
Secure 1st Half Share Locally
Encrypt Share 2nd half ,Enrollment private key
Enroll with encrypted 2nd share and enroll public key
Enroll with encrypted 2nd share and enrollment public key
Create DID
DID,Public Key
DID Document
DID Document
Share 2nd Encrypted DID,enrollment sign,issuer sign
return DID
return DID
Client device has 1st half & DID
Employee
Application
Issuer
BOPS Blockchain Server
Blockchain
Cloud

Fig. 1: Enrollment

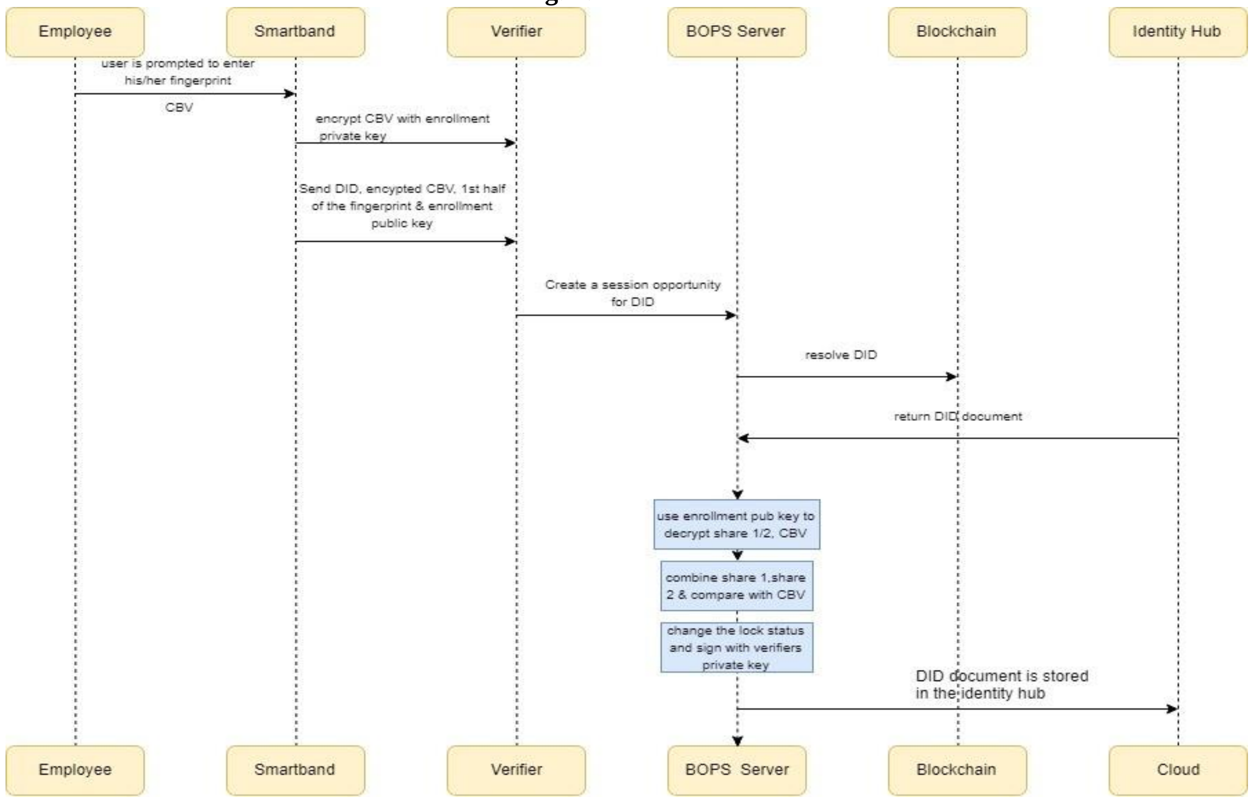

Employee
Smartband
Verifier
BOPS Server
Blockchain
Identity Hub
user is prompted to enter his/her fingerprint
CBV
encrypt CBV with enrollment private key
Send DID, encypted CBV, 1st half of the fingerprint & enrollment public key
Create a session opportunity for DID
resolve DID
return DID document
use enrollment pub key to decrypt share 1/2, CBV
combine share 1,share 2 & compare with CBV
change the lock status and sign with verifiers private key
DID document is stored in the identity hub
Employee
Smartband
Verifier
BOPS Server
Blockchain
Cloud

Fig. 2: Verification

Step 6: The DID and it's corresponding public key is looked up in the blockchain.

Step 7: Once the blockchain validation is completed, the DID document is retrieved from the identity hub. The public key in the DID document is verified.

Step 8: The encrypted half from the DID document and the encrypted half from local share id are decrypted using validated public key and both the decrypted halves are merged. Step 9: The Collected Biometric Vector (CBV) is decrypted using validated public key and it is compared with the mergedIBV.

Step 10: Once biometric validation is successfully completed; the issuer signature is decrypted using the organization's public key and it's checked with the verifiable claim.

Step 11: On successful validation of the verifiable claim, the locked status of the band is changed and is cryptographically secured using the organization's private key.

Now the locked status can be for other authentication services.

Recognition

Every service endpoint consists of an active/passive RFID tag that generates a unique id. The following steps describe how the user unlocks a service endpoint.

Step 1: The RFID reader present in the smart band receives the unique id from the service endpoint.

Step 2: The DID, public key, and a unique id are sent through the HSM module to BOPS server for verification.

Step 3: The DID and the public key are looked up in the public blockchain and the corresponding is retrieved from the identity hub.

Step 4: The locked status is verified from the DID document and the result is sent to the organization.

Step 5: The organization then unlocks the service endpoint. When the capacitive sensor fails to detect human contact, the lock status is changed. If the band gets tampered the emergency protocol is initiated through the HSM module.

System setup

Employee wears a smart band which is assumed to be preconfigured with corresponding employee's ID that he uses to enter the company. The band consists of the following components:

- – *UHF RFID reader NFC RFID reader HSM module
- Capacitive Fingerprint sensor
- Wi-Fi module (or any other means of internet connectivity)

1. The entrance of the company building will be installed with a passive Ultra High-frequency tags (UHF RFID) in the door.
2. RFID tag has an inbuilt memory that is configured with an application ID which is unique to each security endpoint (entrance door in this case).
3. Once activated, they continuously broadcast the application ID over and over again.
4. In case, if the band enters the RFID tag range the application ID is transmitted over Radio Frequency wave to the RFID reader. .
5. This triggers the band and the received application ID is recognized if the band is locked (meaning the employee is verified).
6. Then the organization maps this application ID to the actual physical device (the entry door) the employee is interacting with.

Thus, the permission to enter is granted if all conditions are perfect.

The smart band hence enables the wearer frictionless transit using the concept of self-sovereign identity. Unlike Barcode scanning systems, where the user has to show his barcode in front of the scanner, the UHF RFID gives the necessary range to operate without having the need to come in the line of sight. Such a system can handle several users at once and thus proves to be more efficient and secure than the currently prevailing barcode system.

Here's another instance

Every system in the organization will have a Near-Field Communication (NFC) tag. These tags operate within a very short range (1cm-1m max).

Thus, granting access only to the desired system (pc) with the corresponding employee's login who is nearby. The working is the same as in the previous case.

This, in turn, helps the organization to keep track of the people using the system as well as making the entire process of authentication automated and secured at the same time.

The real strength of this system is that it is impregnable as there is no access point as we use RFID tag. In case if the band is compromised, still the fake user will not be verified so the band will be rendered useless. Also, the de-centralized encrypted architecture provides impenetrable security to the system.

IV. EXPERIMENTAL SETTINGS

Practical Implementation of this paper has been tested and the details of the experiment are discussed below. In this experiment, we have used the SEEED fingerprint sensor and seeduino lotus V1.1.

Equipment

The Fingerprint Sensor is one optical fingerprint sensor which will make adding fingerprint detection and verification simple.

There's a high-powered DSP chip AS601 that does the image rendering, computation, feature-finding and searching.

It also enrolls new fingers directly up to 162 fingerprints can be stored in the onboard FLASH memory.

Seeeduino Lotus is an ATMEGA328 Microcontroller development board. It is a combination of Seeeduino and Base Shield.

It uses an Atmel ATMEGA328P-MU and CH340.

ATMEGA328P-MU is a high performance, low power AVR 8Bit Microcontroller. CH340 is a USB bus converter chip that can realize a USB to serial interface. Seeeduino Lotus has 14 digital input/outputs (6 of which can output PWM) and 7 analogue input/outputs, a micro USB connection, an ICSP header, 12 Grove connections, a reset button.

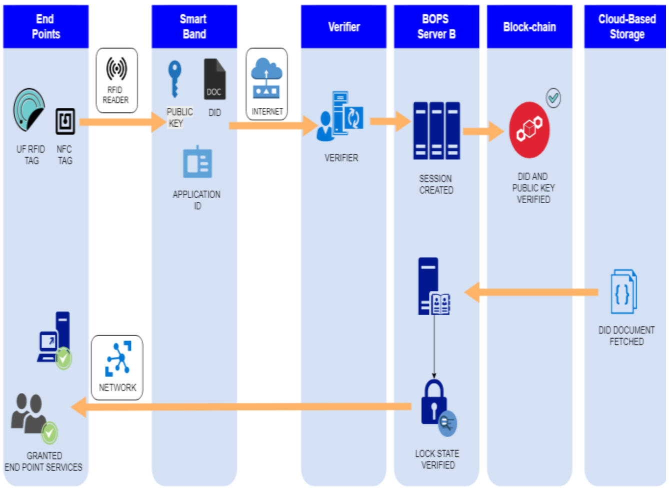


Fig. 3: Recognition

Experimental Setup

The process of enrollment starts with the user being prompted to enter the ID followed by an instruction to place their fingerprint. Multiple fingerprints are sampled to form a super-resolution of the fingerprint. This fingerprint is converted into IBV (Initial Biometric Vector) and then stored.

In the process of recognition, the user is prompted to enter his/her fingerprint. The collected fingerprint is converted into CBV (Collected Biometric Vector). The collected CBV is compared against the previously stored IBV's and the most correlated result is displayed.

The above-mentioned set-up is carried under following assumptions:

The fingerprint procurement was successfully done

The entire set-up is set in an organization environment where the need to verify the identity arises at multiple levels.

The entire facility is sufficiently equipped with proper internet connectivity.

Experimental Results

The analysis of the SEEED fingerprint module is given as such:

From the table 1, we infer that on an average only one out of every thousand entries is a false positive and also only one out of hundred entries are identified as a false negative.

The fingerprint recognition accuracy scores were obtained under different experimental conditions as shown in table 2. (The 'confidence' is a score number (from 0 to 255) that indicates how good of a match the print is, higher is better.)

USE CASES

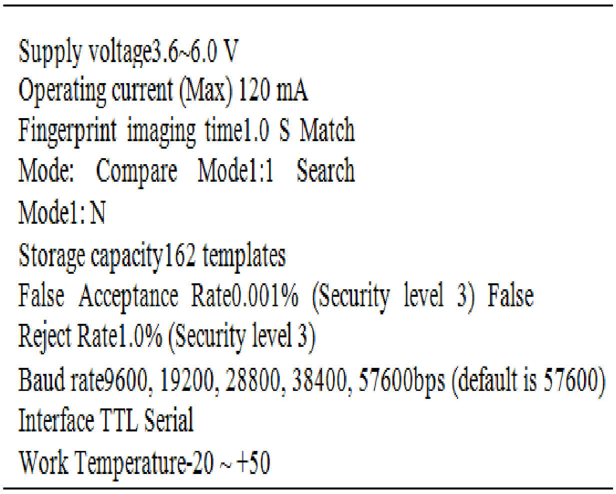
This idea can be extended in multiple cases due to its versatile nature, for example

- The user doesn't have to carry any additional documents to prove his/her identity.
- The patient arriving at the hospital can be identified in seconds without requiring any other sort of identification.
- All the important documents like license, insurance related to the user can be stored away safely and can be recalled as and when the need arises.
- Reduces load of security personnel and officers as they can easily monitor as well as verify any person's identity.
- The user can interact with their surrounding IoT devices in real-time(opening laptop when the user is nearby, have control over all the device that he/she owns cause every user has a unique DID, smart gestures can be used to give customized commands to specific devices).
- Intelligence agencies can have access to the blockchain which in turn helps in efficient tracking down the malicious activities going on (like human trafficking, kidnapping, women safety, border security)by looking up their recent check-in.
- The government can easily carry out the census with even more accurately, efficiently and in a cost-effective way(no-one can fake their identity).
- More flexibility, as well as protection on the personal data of the users which is very difficult to be compromised as explained above there, is no one point of failure.

V. CONCLUSION AND FUTURE WORK

We cannot continue to store credentials in central repositories where they are currently being stolen at an alarming rate.

Table I: Specifications of Speed Fingerprint Module



Supply voltage3.6~6.0 V
Operating current (Max) 120 mA
Fingerprint imaging time1.0 S Match
Mode: Compare Model:1 Search
Model: N
Storage capacity162 templates
False Acceptance Rate0.001% (Security level 3) False
Reject Rate1.0% (Security level 3)
Baud rate9600, 19200, 28800, 38400, 57600bps (default is 57600)
Interface TTL Serial
Work Temperature-20 ~ +50

Table II: Accuracy Scores

Enrollment sample	Recognition sample	Accuracy Score
clean	clean	124,161,249,145,247
dirty	clean	68,67,60,87,67
clean	dirty	127,97,65,90,98
dirty	dirty	45,<40,54,<40,51

The age of the mega breach should be history and only decentralized architecture can make that case.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Our decentralized model secures identity credentials in a trusted environment on a user’s trusted devices to reduce the attack surface and change the whole business models for cybercriminals logically target centralized identity stores. A criminal attack on a decentralized authentication system is neither trivial nor scalable

Today enterprises store many keys in one place and each user is responsible for many keys. Inverting this model will allow enterprises to store many keys in many secure places and for users to own one trusted key to many applications. When the world credentials decentralized in this way authentication becomes so much easier and of course safer.

With the above mentioned functionalities of smartband, it works well in closed environments and with further extension in the capabilities of decentralized identifiers, this idea can be extended to a secured Single Sign On (SSO). Further improvements at the hardware can support multiple logins at same time.

One of the most robust, secure and efficient biometric based recognition compared to other biometric systems is Iris based biometric recognition. Complex features of human iris makes the iris code robust and difficult to break. The iris code is stable, unique, complex and difficult to copy.[14] The future scope of this idea is to implement iris based biometric recognition using blockchain technology.

REFERENCES

1. P. Grassi, M. Garcia, and J. Fenton. SP 800-63-3 Digital Identity Guidelines. Technical report, National Institute of Standards & Technology, Gaithersburg, MD, United States, 2017.
2. 2410-2017 IEEE biometric open protocol standard (BOPS).https://standards.ieee.org/findstds/standard/2410-2017.html.
3. A. Ross and A. Othman. Visual cryptography for biometric privacy. IEEE transactions on information forensics and security, 6(1):70–81,2011.
4. M. Mealling and R. Denenberg. Report from the joint w3c/ietf uri planning interest group: Uniform resource identifiers (uris), urls, and uniform resource names (urns): Clarifications and recommendations. Technical report, 2002.
5. D. Reed and M. Sporny. W3c decentralized identifiers (dids) 1.0. https://w3c-ccg.github.io/did-spec/, 2017.
6. https://en.bitcoin.it/wiki/Proof_of_work
7. https://www.hindawi.com/journals/scn/2018/9675050/
8. https://www.bayometric.com/increasing-importance-ofbiometric-security/
9. https://medium.com/blockchain-education-network/what
10. -is-blockchain-explained-for-beginners-5e747cea271
11. https://www.experian.com/blogs/ask-experian/how-can
12. -biometrics-protect-your-identity/
13. https://www.androidauthority.com/how-fingerprint-scanners-work-670934/
14. www.rfidjournal.com/faq/show?68
15. A. Ashok, Poornachandran, P., and Dr. Krishnashree Achuthan, “Secure authentication in multimodal biometric systems using cryptographic hash functions”, Communications in Computer and Information Science, vol. 335 CCIS, pp. 168177, 2012.
16. N. Lalithamani and R, S., “Countermeasures for indirect attack for iris based biometric authentication”, Indian Journal of Science and Technology, 2016.