Security Issues in Internet Architecture and Protocols Based on Behavioural Biometric Block Chain-Enhanced Authentication Layer

Jhimmy Alberth Quisocala Herrera[1*], Fernando Antonio Flores Limo[2], Abel Alejandro Tasayco-Jala[3], Isabel Menacho Vargas[4], Wilfredo Barrientos Farias[5], Zoila Mercedes Collantes Inga[6] and Eber L. Herrera Palacios[7]

[1*] Professor, Facultad de Ingeniería Mecánica Eléctrica, Electrónica y Sistemas, Universidad Nacional del Altiplano, Puno, Perú. jquisocala@unap.edu.pe, Orcid: https://orcid.org/0000-0001-9586-8491

[2] Professor, Facultad de Educación, Universidad Nacional de Educacion Enrique Guzman y Valle, Lima, Perú. ffloresl@une.edu.pe, Orcid: https://orcid.org/0000-0002-5494-9794

[3] Professor, Facultad de Administración, Universidad Nacional de Cañete, Lima, Perú. atasayco@undc.edu.pe, Orcid: https://orcid.org/0000-0002-3993-1713

[4] Professor, Facultad de Educación, Universidad Nacional Mayor de San Marcos, Lima, Perú. imenachov@unmsm.edu.pe, Orcid: https://orcid.org/0000-0001-6246-4618

[5] Professor, Facultad de Ciencias Sociales, Universidad Nacional de Tumbes, Tumbes, Perú. wilbafarias@gmail.com, Orcid: https://orcid.org/0000-0001-7155-9408

[6] Professor, Facultad de Ingeniería, Universidad César Vallejo, Lima, Perú. zcollantes@ucvvirtual.edu.pe, Orcid: https://orcid.org/0000-0002-8741-9263

[7] Professor, Department of Forestry Engineering and Environmental Management, Universidad Nacional de Tumbes, Tumbes, Perú. eherrerap@untumbes.edu.pe, Orcid: https://orcid.org/0000-0002-7255-9087

Received: June 11, 2023; Accepted: August 19, 2023; Published: August 30, 2023

Abstract

Internet security is of paramount importance due to the pervasive nature of the network in modern society. As the globe grows increasingly interconnected, issues like data breaches, unauthorized access, and service disruptions become more common. Safeguarding private data, ensuring uninterrupted communication, and protecting vital services are all essential to establishing confidence and stability in the online world. Internet security is a complex problem to solve due to the interconnected nature of the Internet's Architecture and Protocols (IAP). Due to the wide variety of devices and platforms that can access the Internet, cybercriminals can breach a complex ecosystem. Constant monitoring and flexibility are required due to the rapid development of new attack methods and vulnerabilities. The difficulty lies in balancing implementing new security measures and minimizing disruptions to the user experience, which calls for adaptive and novel approaches. In this paper, the Behavioural Biometric Block Chain-Enhanced Authentication layer

Journal of Internet Services and Information Security (JISIS), volume: 13, number: 3 (August), pp. 122-142. DOI: *10.58346/JISIS.2023.I3.008*

*Corresponding author: Professor, Facultad de Ingeniería Mecánica Eléctrica, Electrónica y Sistemas, Universidad Nacional del Altiplano, Puno, Perú.

(BBB-EAL) framework recommends a static authentication mechanism for end-users and edge servers. This authentication creates a secure and encrypted link between parties. Access tokens are produced via a smart contract, removing the requirement for a trusted third party. This work emphasizes the importance of architecture design and sequence diagrams in representing participant interactions and information sharing. Additionally, it examines the construction of the Machine Learning (ML) model used to recognize KMT dynamics. Simulations indicate that the recommended design improves user authentication in an IAP-enabled environment. The findings demonstrate the ability to evaluate confidence in real time, achieve minimal authentication time, and utilize resources efficiently.

Keywords: Security, Internet, Protocol, Machine Learning, KMT Dynamics, Behavioural, Biometric, Block Chain, Authentication.

1 Introduction to Behavioural Biometric Block Chain

The first design of the IAP was to provide a shared and decentralized network that facilitated equitable participation. This network operated through peer-to-peer interconnection, eliminating the need for dependence on a singular computer (Yang, W., 2019). A further crucial factor in the initial design of the Internet was the requirement for computers to possess interoperability across diverse systems, enabling a more significant number of devices to be included in the network. Nevertheless, after the first dot-com boom, prominent firms like Google and Amazon came to see that the primary benefit derived from this decentralized network was in aggregating, structuring, and commercializing information via centralized services (Boucher, C., 2022). Consequently, these organizations have established their worth by expanding extensive centralized databases populated with readily accessible private and personal information. Subsequently, this data is utilized on the Internet, resulting in a partial divergence of the Internet's service architecture from its initial intended design.

Currently, the Internet exhibits a physical decentralization. However, it encompasses crucial elements for processing information, social media, marketing, and crowdsourcing, which heavily rely on prominent centralized services. The conventional Internet service comprises three distinct entities: service requesters, large companies (acting as service providers), and a centralized database. Service requesters are responsible for soliciting services from service providers offering Internet-based services. Most service providers possess their own data centers, which serve as repositories for customer data and facilitate the operation of their apps (Luo, H., 2014).

Initially, it is worth noting that conventional Internet service designs exhibit susceptibility to denial of service, resulting in the unavailability of services, as exemplified by the Global Financial Crisis (GFC) (Berentsen, A., 2019). Additionally, many Internet services depend on a centralized database, encountering a single failure point. This vulnerability exposes these services to potential attacks, presenting attackers with a solitary target to exploit. For example, in cases where centralized services such as LinkedIn or Gmail Services experience a failure, all the websites and applications that rely on these services cease to function.

Furthermore, the personal information of users, including their name, email address, and phone number, as well as their job solutions, are stored in a centralized database. This database now raises many concerns regarding data privacy. It is challenging for users to ascertain the activities occurring within the enclosed environments of centralized services. Consequently, individuals need more specific knowledge regarding the extent of data collection by these services and the subsequent utilization of such data. Moreover, when a service requester and supplier disagree, it becomes necessary for them to rely on a reliable network that can provide an impartial adjudication, potentially resulting in a

phenomenon commonly referred to as 'error-reporting.' In summary, it is evident that current IAP implementations effectively provide decentralized information transmission and sharing. However, there has been a lack of thorough examination and proactive measures to ensure transactional confidence and the exchange of wealth or value via the Internet.

Hence, establishing a reliable and credible Internet infrastructure is a crucial and foundational undertaking. Numerous research areas have been explored to address some of the challenges in Internet services. The subjects mostly pertain to identifying and mitigating attacks, the limitations of relying on singular solutions and safeguarding privacy. Various techniques have been suggested in the academic literature to protect personal data privacy, such as data anonymization, differential privacy, and encryption systems (Vasa, J., 2023). Reputation-based security techniques have been developed to assess and forecast the safety of transactions by considering the collective use patterns and reputations of a diverse user community.

The blockchain is a recently emerged platform technology that has gained significant recognition. Its primary development objective was to facilitate the usage of the Bitcoin cryptocurrency (Kassab, M., 2019). Blockchain Technology (BT) is founded upon the principles of decentralized networking, whereby one of its primary attributes lies in its ability to ensure data security and preservation. The system exhibits scalability and robustness since all participating nodes equitably contribute resources, mitigating traffic flow bottlenecks with a many-to-one pattern. This particular approach has been shown to effectively reduce traffic delays and address the potential issues arising from a single point of failure (Mohanta, B.K., 2020).

Biometrics is defined as the process of quantifying human characteristics. Biometric identifiers are identifiable and measurable characteristics used to identify and describe individuals (Alsaadi, I.M., 2021). Prominent instances of biometric verification encompass ocular scans, fingerprint analyses, and DNA investigations. Biometric verification is a technique that involves matching an individual's genetic features or behavioral characteristics with pre-existing data that has been captured, recorded, and arranged in a structured database or stored on a token (Mason, J., 2020). The concept is defined as the process of self-identification through knowledge, possession, or inherent qualities (Sundararajan, A., 2019). In other words, it discerns the intrinsic characteristics.

Biometric characteristics are categorized into two distinct types: physiological biometrics and behavioral biometrics. Physiological features encompass the anatomical and biological traits shown by an individual. The biometric modalities in this category consist of fingerprints, face recognition, iris scan, voice recognition, palm veins, DNA, and other similar methods. The methods are the conventional approaches via which an individual's identification is verified (Tripathi, K.P., 2011). In contrast, behavioral biometrics encompasses gait, GUI interaction, haptics, programming style, database access, system call records, mouse dynamics, and more. Determining an individual's interior characteristics and attributes is contingent upon several factors (Boakes, M., 2021).

Behavioral biometrics (BB) is a nascent area of study that centers on techniques for capturing distinct and quantifiable patterns in human behaviors, specifically in activities such as Keystrokes, Mouse usage, and Touchscreen (KMT) dynamics. In contrast to physiological biometrics, such as fingerprints or iris patterns, which necessitate active user participation with costly sensors or biometric scanning devices, keystroke, and mouse dynamics can be collected passively using readily available hardware, such as a keyboard and mouse.

This research paper explores the integration of behavioral biometrics with BT as a solution to the security difficulties IAP features. This novel methodology acknowledges the dynamic nature of

cybersecurity risks and utilizes distinct behavioral attributes demonstrated by individuals, including KMT dynamics, to augment authentication processes. This study aims to enhance the security framework by integrating behavioral biometric markers into the authentication layer, creating a more robust and user-oriented system. The main contributions of this work are:

- The Behavioural Biometric Block blockchain-enhanced authentication layer (BBB-EAL) is proposed to integrate behavioral biometrics with BT to solve the security difficulties IAP faces.
- The BBB-EAL framework suggests initial static authentication between end-users and edge servers. This authentication process aims to create a safe and encrypted channel between the two parties. This process generates access tokens via a smart contract, eliminating the need for an intermediary or trusted third party.
- This study highlights the significant role played by various architectural components, such as architecture design and sequence diagrams, in depicting the interactions and information exchange among participants. Additionally, it explores the design process of the ML model used to recognize KMT dynamics.
- This study presents a series of experiments showcasing the suggested architecture's effectiveness in providing enhanced user authentication in an IAP-enabled environment. The results exhibit real-time confidence evaluation, minimal authentication time, and low resource usage.

The rest of the paper has been organized as follows: Section 2 describes related research on behavioral biometrics with BT for IAP. Section 3 provides the Behavioural Biometric Block blockchain-enhanced authentication layer (BBB-EAL) that integrates behavioral biometrics with BT as a solution to the security difficulties faced by IAP. Results and discussion have been given in section 4. Finally, the conclusion, limitations, and scope for further research have been shown in section 5.

2 Related Works on Behavioral Biometrics with BT for IAP

BT has gained interest in Bitcoin, financial services, Supply Chain Management (SCM), the IoTs, and Internet services since 2009. Given the prevalence of centralized development in many Internet services, scholars have investigated decentralized frameworks to address the growing security challenges and constraints. Other Internet service areas are being researched in addition to financial applications. These include IoT, public, social, cloud, reputation management, and crowdsourcing services.

Alkhateeb et al. (2022) proposed a systematic literature review to study hybrid BT platforms for the Internet of Things (IoT) (Alkhateeb, A., 2022). Their study shows the widespread use of hybrid systems that combine public and private BT benefits. The findings show hybrid systems can address scaling issues while maintaining security and decentralization. The flexibility of these devices makes them ideal for many IoT applications. However, blockchain technology's interoperability challenges are complex. This study helps scholars and professionals understand the changing landscape of blockchain solutions for the Internet of Things.

Hakiri et al. (2020) presented a BT architecture for IoT networks that prioritizes tamper resistance. This architecture supports SDN. The design uses blockchain technology to increase network security. The findings demonstrate the design's ability to protect IoT networks from unauthorized interference (Jung, S.W., 2022). A comprehensive literature review by Hisseine et al. (2022) examined blockchain technology in social media. This study shows that blockchain improves security and data integrity. However, blockchain have drawbacks, including high computational overhead (Hakiri, A., 2020). Through a thorough review of prior studies, the authors demonstrate how blockchain technology can improve data integrity, user autonomy, and digital identity (Hisseine, M.A., 2022). The findings show

that the technology could solve significant privacy and security issues. This technique has openness benefits, but scalability is limited. This study sheds light on BT's dynamic role in digital transactions and proposes using blockchain for secure and private data exchange.

Sabu et al. (2021) described a blockchain-based system for secure and private E-health and IoT data exchange (Sabu, S., 2021). The suggested method involves developing and implementing a blockchain-based solution to protect healthcare and IoT data. The findings show that a safe sharing architecture can exchange medical data while protecting patient privacy. Petcu et al. (2023) proposed a secure, decentralized authentication method. This mechanism uses Ethereum BT and Web 3.0 (Petcu, A., 2023). The researchers use Web 3.0 to improve authentication and security. The results show that this strategy provides safe, decentralized authentication solutions. The complexity of the underlying technology causes drawbacks, but this technology increases user control and confidentiality.

Hu et al. (2020) proposed continuous authentication using behavioral biometric features to protect blockchain wallet private keys (Hu, T., 2020). The researchers collect and analyze user activity data, such as keystrokes and mouse movements, to create biometric profiles. The findings show that this method provides uninterrupted and unobtrusive authentication. The conclusions emphasize real-time user verification for security. Advanced security measures increase safety and reduce vulnerability to conventional authentication methods. However, false positives and the system's ability to adapt to behavior changes should be considered.

Delgado-Mohatar et al. (2020) examined the pros and cons of blockchain and biometrics (Delgado-Mohatar, O., 2020). The researchers analyzed technology convergence to mitigate security issues. The findings show that diverse applications can improve security and privacy. The implications emphasize the need to address information security and scalability. This method enhances identity verification and data integrity. However, information ownership and compatibility must be addressed to progress. Oak (2018) reviews the literature on behavioral biometric authentication (Oak, R., 2018). To understand behavioral biometric authentication systems, a comprehensive literature study is recommended. The findings cover a wide range of authentication behaviors. Inferences demonstrate their versatility and security potential. The non-intrusiveness of behavioral biometrics is an advantage—however, system reliability and user flexibility present challenges.

Al-Naji and Zagrouba (2022) present the CAB-IoT architecture, which uses blockchain technology for continuous IoT authentication (Al-Naji, F.H., 2022). The researchers use BT and behavioral biometrics for real-time authentication. The findings show that this method can improve IoT security. User-centric and context-aware authentication is a benefit of this approach. However, drawbacks like IoT devices' computational burden must be considered. Zulkifl et al. (2022) introduce FBASHI, a fuzzy logic-BT adaptive security solution for healthcare IoTs (Zulkifl, Z., 2022). The researchers use fuzzy logic and BT to address healthcare IoT ecosystem security issues. The results of this study show that this method provides adaptable and context-sensitive security. This technology protects patient data and adapts to changing conditions. Fuzzy logic's complexity presents a challenge.

Internet service designs typically include basic communication mechanisms between networks, which vary in hardware, software, or technical configuration. A secure and layered service architecture is essential to meet business and user needs. However, a robust and reliable security model must be prioritized to maintain these goals. Most Internet companies or businesses have data centers to store user data and run their proprietary applications (Thooyamani K.P., et.al, 2014). Due to their size and visibility, cybercriminals target these entities to steal confidential information, making strong security measures essential. BT emerged and evolved to address privacy and trust issues in modern Internet

services. Distributed ledgers reduce single points of failure. Blockchain technology uses a decentralized peer-to-peer network to reduce reliance on centralized data storage systems, deviating from client-server architectures. BT could boost competition by eliminating lock-ins and giving consumers complete data control (Pop, C., 2018).

The primary aspect of this proposed solution revolves around utilizing BT, which augments security and transparency. The utilization of BT offers a viable solution for safeguarding critical behavioral biometric data by using its decentralized and tamper-resistant properties. This approach effectively mitigates the risks associated with centralized databases. The amalgamation of behavioral biometrics with BT offers a means to augment the authentication process while concurrently addressing emerging concerns about client privacy, security breaches, and unauthorized transactions.

3 Behavioural Biometric Block Chain-Enhanced Authentication Layer (BBB-EAL) Framework

The BBB-EAL architecture proposes incorporating an initial static authentication procedure between end-users and edge servers. The primary objective of this authentication procedure is to establish a secure and encrypted communication connection between the two entities involved. Access tokens are produced through an intelligent contract, hence obviating the necessity for an intermediary or trustworthy third party. This work emphasizes the crucial significance that different architectural components, such as architecture design and sequence diagrams, play in representing the interactions and flow of information among participants.

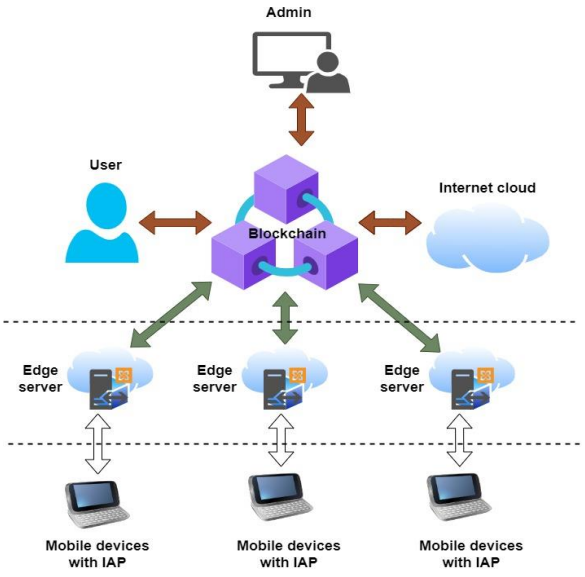

Figure 1: Architecture for the Blockchain-based Enhanced Authentication for Mobile Devices with IAP

Figure 1 shows the architecture for the blockchain-based enhanced authentication for mobile devices with IAP. To enhance authentication in the IAP environment, BBB-EAL recommends the implementation of a distributed architecture that leverages BT. This approach eliminates the requirement for an intermediate or trusted third party, ensuring high trust and availability. The Ethereum Blockchain has been selected due to its ability to allocate a distinct Ethereum address comprising public and private keys to each participating node. This feature enables the creation of access based on bespoke tokens, hence augmenting the security aspect in the context of Identity and Access Management. Ethereum

demonstrates a comparatively swift transaction processing capability, with a block time ranging from 15 seconds to 25 seconds, unlike other BT networks that often need about 15 minutes. Ethereum has a scalability feature through the utilization of block gas restrictions, which determine the cost of each transaction based on factors such as complexity requirements, storage demands, and bandwidth usage. The present study aims to deploy a private Ethereum network utilizing the proof of authority consensus mechanism as an alternative to the commonly employed proof of work consensus mechanism. The utilization of private blockchain has several advantages in comparison to public networks. It enhances security and anonymity while delivering faster computation time, reduced costs, and improved scalability.

The suggested design would facilitate the implementation of an edge server layer. This layer can potentially enhance the limited resources of mobile devices in an IAP environment, namely in terms of storage capacity, computational power, and networking capabilities. Incorporating edge servers into the proposed architecture would contribute to its scalability by facilitating the execution of resource-intensive activities associated with constant authentication and communication with the BT network. The deployment of edge servers near IAP mobile devices, along with the utilization of ML models, enables edge computing to provide real-time learning from IAP device data with more efficacy than cloud computing, which introduces a delay in response time to IAP devices.

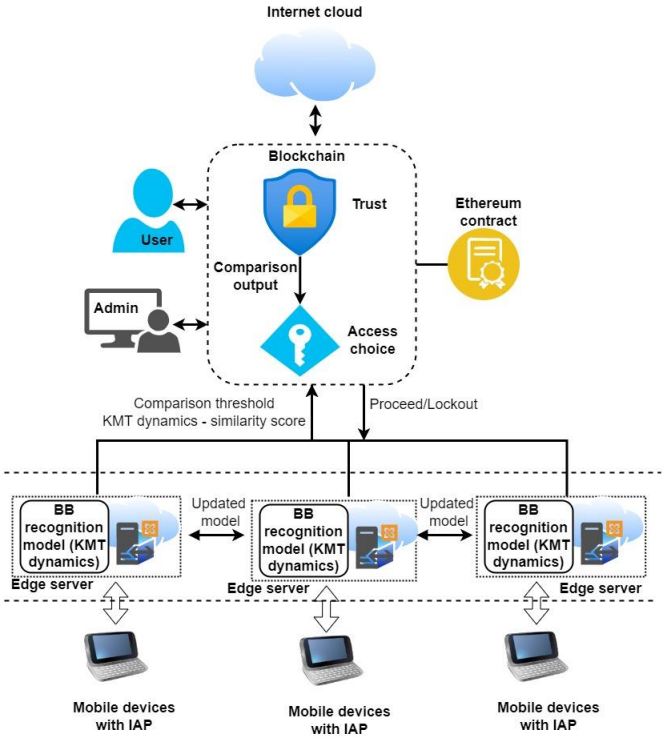

Figure 2: Detailed Architecture of the Proposed BBB-EAL Framework

Figure 2 shows the detailed architecture of the proposed BBB-EAL framework. The architecture elements play a crucial function, as depicted in the following manner:

The internet cloud is utilized for the storage of non-real-time data transactions, which are then analysed for business logic in the context of big data. The suggested system encompasses a real-time enhanced authentication procedure, whereby the edge nodes layer offers localized control response to the IAP mobile devices.

The administrative user is responsible for assigning each IAP device to a certain edge node. Additionally, they grant authorization to end users to access these IAP devices through the utilization of a smart contract. The individual who has the smart contract will bear the responsibility of initiating and deploying it. It is assumed that this individual has the capability to appoint various administrators with management control in accordance with the specific needs of the organization.

End-users are able to submit a formal request for access authorization to a specific IAP device through the utilization of a smart contract. Subsequently, the user will be granted access permissions subsequent to the completion of the authentication procedure at the designated edge node.

In the context of the IAP, it is important to note that each individual device is associated with a specific edge node. Due to the constrained resources of IAP mobile devices, the execution of BT is unfeasible. The edge server layer is activated as a representative of IAP mobile devices.

Edge nodes serve as a direct connection to the Ethereum smart contract, functioning as an intermediary between IAP devices and the BT. Their purpose is to alleviate the burden of ongoing verification for resource-constrained IAP devices. Edge nodes has robust computational capabilities, enabling them to effectively manage numerous concurrent requests associated with the enhanced authentication process. In BBB-EAL, the BB recognition ML model is hosted, and each edge node is responsible for training the model. The classification parameters are then shared with neighboring edge nodes, rather than relying on a coordinating node that would impact all connected edge nodes. This approach reduces the system's vulnerability to risks associated with hacking or unauthorized manipulation, as any compromise would only affect the neighboring node, which is comparatively easier to address. The BB similarity score that is created will largely be employed for the purpose of enhanced authentication. In this process, the similarity threshold will be synchronized with BT. Consequently, any decrease in the similarity score below the threshold will be promptly detected. The outcome of the created comparison will serve as the input for the access determination module, which will assess whether the user should be allowed to continue using the device or be locked out from further access.

The BBB-EAL network, which is being proposed, is built upon the Ethereum Blockchain. The platform of this network comprises the following components: Ethereum encompasses two types of accounts: managed accounts and smart contract accounts. These accounts are distinguished by a 25-byte address. A smart contract is a software program that is kept within the blockchain and operates in a manner that is analogous to traditional contracts, with the purpose of achieving predetermined objectives. The system possesses Application Binary Interfaces (ABIs) that let users to interact with its operations through the transmission of transactions or messages from Ethereum accounts. In the context of a blockchain ledger, it is important to note that each node inside the network possesses a localized version of the blockchain.

The suggested method entails the division of the procedure at the Blockchain layer into three distinct steps, namely:

a) Registration phase.
b) Static authenticating phase.
c) Enhanced authentication phase.

The smart contract can receive and respond to queries from end-users or edge nodes to execute various operations, such as registration, static authorization, and ongoing verification.

Instruments

The experimental project will use the Anaconda system for data pre-processing and implementing a recognition machine learning model utilizing the Python programming language. Jupiter Notebook serves as the Integrated Development Environment (IDE) for development purposes, offering a dynamic and interactive platform for the display and execution of code. The implementation of distributed computing in TensorFlow will include using the distributed strategy, enabling the nodes to modify the model variables after data training. The database will be partitioned into multiple segments, and a TensorFlow distribution method will be employed to facilitate variable trade and updates among nodes. Each node will independently train the current information segment and store the resulting variables. These variables will then be exchanged with the subsequent node, utilizing the obtained variables to introduce the following data segment. Using the Azure Workbench, the ML strategy will be implemented as a web service inside the Azure cloud infrastructure. Microsoft has made significant investments in the growth of the Azure Blockchain services and the Ethereum networking within the Blockchain networking level. The Microsoft Azure Blockchain Growth Kit for Ethereum is utilized to construct the Blockchain network and facilitate the deployment of the intelligent agreement on this network. The Azure Blockchain Workbench Application Programming Interface (API) can initiate requests to the record and transmit information from another system to a designated contract. It is important to note that the Blockchain networks and the intelligent agreement cannot retrieve data from sources outside their networks. The Azure Blockchain Development Kit also offers a readily available testing environment and presents a visually intuitive interface for executing Ethereum test cases and investigating the Blockchain system. The Azure Monitoring service has a collection of efficiency charts that specifically focus on various Key Performance Indicators (KPIs) to assess the overall network efficiency or effectiveness at the individual node level.

Software Architecture

The system is comprised of three main elements:

(a) The visual user interface is designed to capture the dynamics of user keystrokes and mouse movements during information entry.
(b) The information pre-processing unit produces distinct user trends (features) from the keystroke and mouse movement dynamics.
(c) The ML unit acquires knowledge from the characteristics to provide predictions for novel input data.

The software application collects and stores the unique characteristics of a user so that during the authentication procedure, new data is collected and compared to the previously held information. Confirming recognition happens when the information is determined to be coherent, whereas rejecting occurs if the information is determined to be incoherent. The BBB-EAL architecture illustrates the implementation and management of an ML system that enables the production of predictions on new data. The model requires the collection of ten knowledge examples from persons who possess the cards legitimately (accurate research) and ten information examples from those involved in fraudulent actions (false knowledge). Hence, it was ensured that the BBB-EAL scheme was furnished with ten pre-processed spurious data sets acquired from several users who input fabricated card information shown on the graphical user terminals.

The current user must enter the same fictitious card data 1,000 times on the graphical user interface. This procedure enables the production of genuine data, combined with pre-existing synthetic data, to

train and maintain an algorithm. The method employs a sequential application of the same artificially generated card data, irrespective of the user, as test data to develop judgments on the validity of the user's input.

- **User Interface**

The user interface has been developed to replicate the structure and appearance of a conventional online payment application. The Kivy2 Python module recorded user actions about KMT behavior from the form's input fields. The information is saved in the JavaScript Object Notation (JSON) layout, which offers simplicity in Python programming owing to its built-in compatibility with JSON. JSON documents comprising 1760 examples of raw KMT dynamics have been available. The data was obtained from 1,000 persons who willingly participated in the study. The male and female participants were at least 18 years old. During the experiment, they were asked to input fabricated card information into the BBB-EAL web page.

- **Data Pre-processing**

A diverse range of keyboard and mouse behaviors are recorded throughout user sessions, including critical presses and updates, mouse movements, left and right button presses and updates, and scrolling in both upward and downward directions. The analysis of KMT dynamics extends to many user interface forms, including touch displays. The collected KMT movements were converted into a condensed collection of characteristics by computing several functions, including the lowest, highest, and mean, for each test session. Based on the information, the research has ascertained the most suitable subset of characteristics using a well-recognized approach called choosing features. The factors that were chosen were later utilized for training for forecasting.

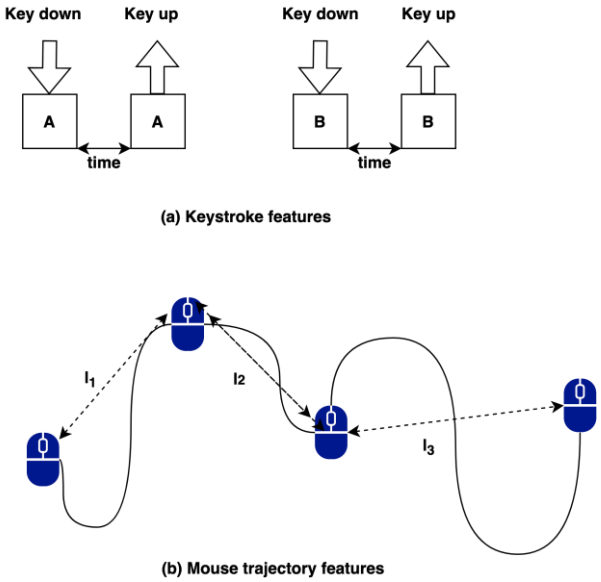

Figure 3: (a) Keystroke Features, (b) Mouse Trajectory Features

The chosen variables consist of the average duration of keyboard stay and the average time of flight period, as seen in Figure 3(a). The middle path of mouse movements in each session of KMT movement testing is represented in Figure 3(b). As seen in Figure 3(b), the average mouse path is determined by calculating the total length covered ($l_1 + l_2 + l_3$) and dividing it by the number of pauses that exceed

500 ms from the initial point to the final point, inclusive. This calculation is performed three times. The chosen characteristics are placed in a Pandas Data Frame, prepared for training and testing ML methods.

- **Machine Learning**

In the present iteration of BBB-EAL, the categorization job was performed using the sci-kit-learn4 implementations of an SVM classification with default parameters. To showcase the functionality of BBB-EAL classification for authentication by users, the research focused only on the three chosen characteristics. These attributes were obtained from a total of 1,000 user data-entering sessions.

Software Demonstration

The user interface exhibits the particulars of an imaginary card, accompanied by directives to input these particulars inside the payment form. The BBB-EAL system is initially equipped with 1,000 fabricated user KMT dynamic examples. These instances are obtained by gathering data from persons who input simulated card information on the user interface. During the initial creation process, the program prompts the legitimate user to input their card data on ten occasions. A timer appears on the consumer's interface throughout the accurate entry of information (e.g., 'Training information provided: 1/1000). The Reset button serves the purpose of clearing the input fields in the event of user error or mistakes. The Delete and Save Modeling buttons will stay inactive until a minimum of ten accurate user training information submissions have been performed. The dynamics of KMT characteristics are derived from the entries and the pre-existing fabricated user data. The features are then utilized for training the classification approach, which is stored in the Sparse Allele Vectors (SAV) file type using the Save Modeling button.

- **Classification Module**

The proposed framework will partition the dataset, allocating 80% for training and reserving the remaining 20% for testing. This approach aligns with the widely accepted best practice in data science. Within the classification component, the feature vector derived from the input face picture is compared to the feature vectors of enrolled behavioral biometrics stored in the template database. This process aims to authenticate the behavioral biometrics by confirming a match with a satisfactory level of likelihood. If no match is discovered, the behavioral biometric is classified as unknown. Categorization methods have emerged as the most suitable option for implementing ongoing authentication compliance. Among these methods, the SVM classification has gained significant popularity and shown superior accuracy and quicker prediction capabilities than other classifiers. Numerous studies have been conducted on using SVMs in behavior biometric identification, with promising outcomes described. SVM classifier demonstrates optimal memory use by using a subset of the training data known as support vectors in its decision mechanism. Essentially, the algorithm determines the optimum width of the hyperplane that effectively partitions the data points into different categories.

One of the primary issues associated with the SVM classification is the need to identify the key factors that significantly impact how well it performs. These factors include selecting a suitable kernel feature and determining the optimal value for the soft boundary variable C, which is crucial in ensuring precise classification. To mitigate their influence, BBB-EAL intends to use an improved SVM classifying methodology by substituting the decision-making function of the hyperplane that separates with the Euclidean space algorithm. Figure 4 depicts the Euclidean-based classification method.

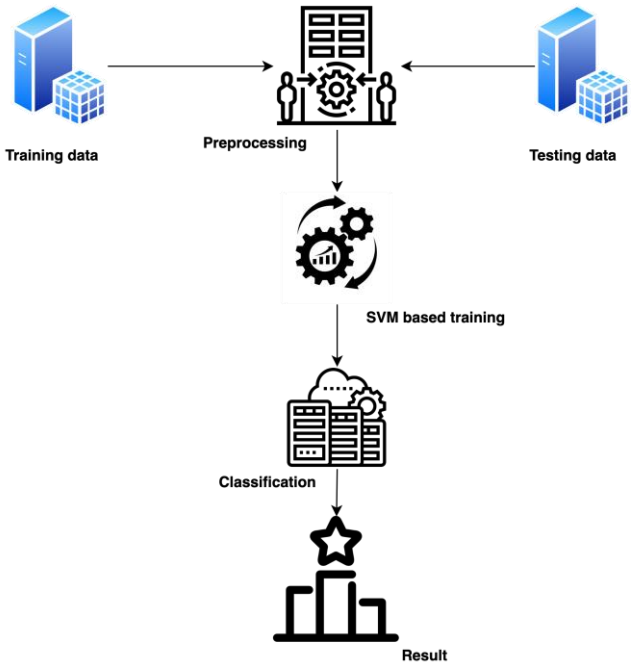

Figure 4: Classification Method for the Behavior Biometrics

To facilitate training and categorization tasks, it is necessary to preprocess and transform the face photos database into numerical form. This conversion enables the mapping of the pictures into vector spaces. The information will undergo dimensionality reduction to reduce the computational time required for calculating, as previously stated in the feature extraction component.

In the training stage, the SVM method will be used to fit the instruction points used for training and then map them into support vectors for every group. Any data points that cannot be recognized will be discarded. In the classification stage, an unorganized data point undergoes preprocessing and is incorporated into the categorization component. Instead of the traditional SVM decision operation, the Euclidean distance operation is employed, as depicted in Equation (1). In this equation, p_x and q_x represent the coordinates of $P\ or\ Q$ in an n-dimensional space.

$$D = \sqrt[2]{(p_1 - q_1)^2 + (p_2 - q_2)^2 + \cdots + (p_n - q_n)^2} \quad (1)$$

The information point will be assigned a label based on the grouping with the shortest distance to the collection of support vectors, which will be determined by calculating the mean distance between the information point and the support vectors for every grouping.

- **Authentication**

The suggested approach utilizes token-based authentication, whereby a token is created by the intelligent agreement to verify the individual's identity. Although the consumer's token is employed in static verification as a one-shot verification method, its suitability for this duty is negated by its continuous monitoring feature. BBB-EAL organization is now pursuing a methodology that relies on biometric traits. In the context of the ongoing verification structure, recognizing an impostor being identified has more significance than detecting an imposter. The primary objective of the BBB-EAL is to identify instances of illegal connection with minimal delay.

Finding anomalies is a common approach in data science, using various statistical methods and machine learning techniques. Nevertheless, within the IoT realm, the proliferation of data being created has presented a heightened level of difficulty in addressing this particular undertaking. The BBB-EAL framework has a trust module that enables ongoing verification of users. The access authorization of a user is reassessed by using the acquired facial picture of the present user and comparing it with the reference template of the authorized user. A trust-level appreciation (T_L) will be assigned, varying from 0.0 (no trust) to 1.0 (finished trust), to assess the credibility of the present user. If the trust level falls below a predetermined threshold, the computer system will require the execution of static obtrusive confirmation to maintain access. The user must meet the necessary access requirements to enter the device. The continuous calculation of a shift in trust-level value, denoted as δT_L, is contingent upon the face similarity rating, E_f, derived by the face recognition machine learning model at the fog nodes level. Applying a threshold to the degree of similarity of each behavioral biometrics collected throughout the session will increase the False Acceptance Rate (FAR) and the False Rejection Rate (FRR). This thresholding process will significantly reduce the level of detail and precision in the verification operation. Consequently, the e_m and e_{red} functions about the behavior biometric resemblance assessment will be used to either increase or decrease the T_L value.

The level of trust should be subject to variation over the period between encounters. Two primary functions will determine this change, notably e_m and e_{red}.. The primary objective of the e_{red} function is to regulate the system's behavior if behavioral biometrics is not recognized. In security, the system exhibits a higher level of protection when multiple uses occur without any identified facial activity during device inactivity, as opposed to instances when the gadget is actively used. The operation is defined with a single variable, T_{LO}, which determines the duration after which the user will be automatically logged out if no face picture is recognized.

The function e_{red} determines the rate of change of the T_L value at any given moment, as described by Equations (2) and (3). The quadratic component is indicative of a cubic decrease in login trust. Once the legal user's identity has been validated, the trust level should gradually decrease without a recognized facial picture. This loss in confidence should occur at a quicker rate as more time elapses. To prevent an excessive and rapid decline in trust, the rate of change of the e_{red} variable is limited to -0.1 per minute.

$$e_{red}(t) = \begin{cases} \frac{t^2}{10t_s(t_s-1)} & t < t_s \\ \frac{1}{10} & else \end{cases} \quad (2)$$

$$t_s = \frac{3}{2}t_{LO} + 1/3(t_L - 6) \quad (3)$$

In the context of continuous verification in BBB-EAL, the behavior biometric similarity score E_f is used to modify the T_L value in active discussions by increasing or decreasing it. Specific guidelines are used to ascertain the impact of a facial similarity score derived from a session on the corresponding login rating.

The obtained fit operation, denoted as e_m, utilizes the behavioral biometrics resemblance score E_f variables as shown in Equations (4) and (5).

$$e_m = \begin{cases} \frac{3}{10} & f(E_f) < 0.01 \\ f(E_f) & 0.01 < f(E_f) < 0.2 \\ -\frac{3}{10} & else \end{cases} \quad (4)$$

$$f(E_f) = \frac{(E_f)^3}{7} - \frac{(E_f)^2}{3} + \frac{E_f}{4} \quad (5)$$

The variables e_m and e_{red}, in conjunction with the duration of the preceding session t_{x-1}, are employed to calculate the T_L at period t_s , as demonstrated in Equation (6).

$$T_L(t_s) = T_L(t_{x-1}) + \int_{t_{x-1}}^{t_s} e_{red} dt + e_m(E_f) \quad (6)$$

As the duration of t_d increases, the likelihood of e_{red} resulting in a T_L score under zero during intervals between sessions grows more pronounced. To mitigate the risk of unauthorized access to the device over an extended period, a projected value of T_L at a subsequent time (t_{x+1}) is determined using the variables t_d and t_e, as illustrated in Equations (7) and (8).

$$T_L(t_{x+1}) = T_L(t_s) + \int_{t_s}^{t_{x+1}} e_{red} \quad (7)$$

$$t_{x+1} = t_s + t_d + t_e \quad (8)$$

The score at time t_{x+1} is contrasted with the log in limit T_c, which is dynamically changed based on the genuine user pattern. If the degree of confidence falls below a certain level, it indicates a significant disparity between the present user and the authorized user. The system will become locked and need the implementation of intrusive authentication procedures to regain access. The process of accessing the system will continue.

This section presents the BBB-EAL framework, a unique approach to addressing security concerns in the context of IAP. BBB-EAL establishes the safe first authentication method by seamlessly integrating behavioral biometrics and blockchain technology. This procedure promotes the establishment of secure communication channels between end-users and edge servers, assisted by using access tokens issued by smart contracts, hence removing the need for intermediaries. This section illustrates how the framework can improve online security using advanced techniques to provide a strong and effective authentication system.

4 Simulation Analysis

Behavioral biometrics refers to the field of study that focuses on analyzing and measuring human behavioral patterns for identification. The Multi-device and multi-activity data from the Same users (BB-MAS) dataset encompasses data obtained from several devices used by a cohort of more than 1,000 individuals (Dataset). These users were involved in various activities, including typing, swiping, and tapping. The data set comprises information obtained from four distinct device categories: smartphones, tablets, laptops, and desktops. Each user is associated with a total of 10,000 occurrences of activity. The provided dataset is a valuable and extensive resource for studying cross-device behavioral biometrics.

The Python-based simulation program SciKit-Learn was used to examine the BB-MAS dataset. The investigation was performed on a workstation with an Intel Core i7 CPU operating at a frequency of 3.5 GHz, 16GB of RAM, and 512GB of solid-state drive storage capacity. The simulation used parallel processing, using all available cores with an average memory of 8GB. The dataset was partitioned into training and testing subsets, with a ratio of 80% for training and 20% for testing, to evaluate the performance of the ML model.

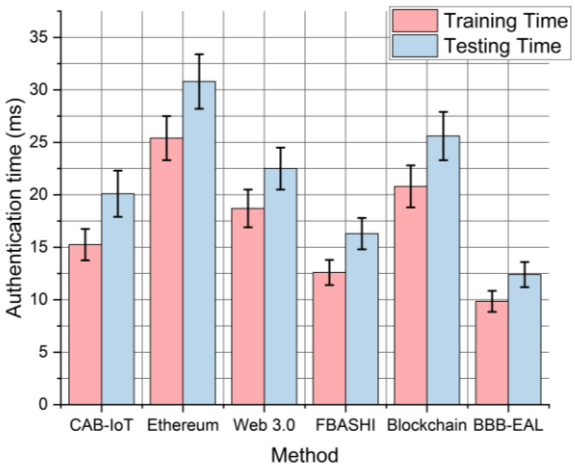

Figure 5: Authentication Time Analysis of Behavioral Biometrics

The average authentication analysis of behavioral biometrics of different systems is shown in Figure 5. The mean authentication durations for the various techniques were recorded as follows: CAB-IoT (17.675 ms), Ethereum (28.1 ms), Web 3.0 (20.6 ms), FBASHI (14.45 ms), Blockchain (23.2 ms), and BBB-EAL (11.625 ms). The BBB-EAL technique demonstrated superior performance to other approaches in the training and testing stages. It achieved the lowest average authentication time, owing to its effective use of static authentication and blockchain-enhanced mechanisms. Using its distinctive architecture and behavioral biometric approach in this technique leads to decreased processing time and improved overall performance.

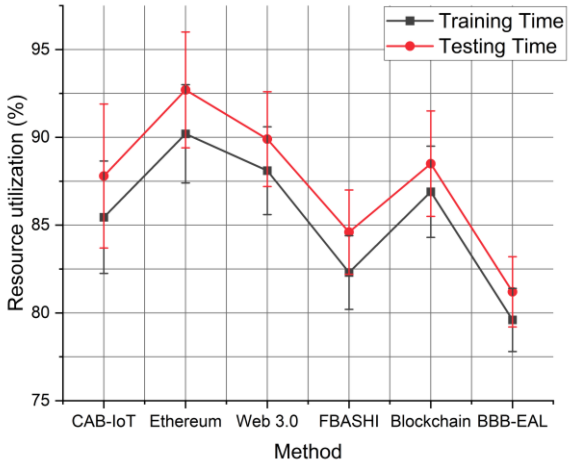

Figure 6: Resource Utilization Analysis of Behavioral Biometrics

The resource utilization analysis of behavioral biometrics of different methods is shown in Figure 6. The mean resource usage percentages for the approaches were as follows: CAB-IoT (86.625%), Ethereum (91.475%), Web 3.0 (88.5%), FBASHI (83.45%), Blockchain (87.7%), and BBB-EAL (80.4%). Although BBB-EAL demonstrated somewhat greater resource use than specific approaches, it consistently maintained efficient utilization of resources. The capability is ascribed to its optimized architectural design, seamlessly incorporating behavioral biometrics and blockchain technology. This integration enables safe authentication processes while efficiently controlling resource requirements.

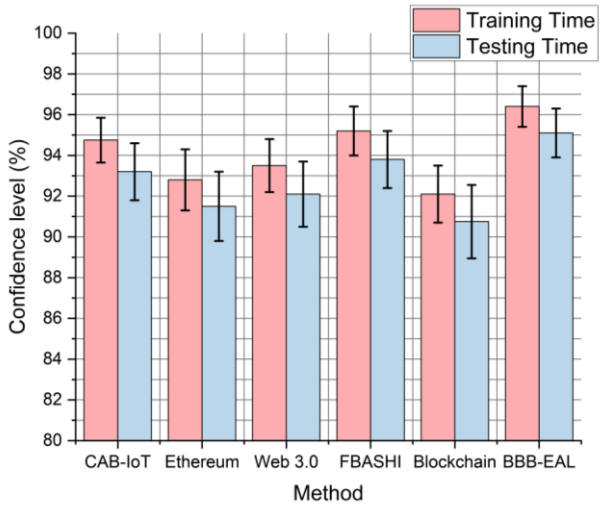

Figure 7: Confidence Level Analysis of Behavioral Biometrics

The confidence level analysis of behavioral biometrics of different methods is shown in Figure 7. The mean confidence levels for the different techniques were as follows: CAB-IoT (93.7875%), Ethereum (92.225%), Web 3.0 (92.95%), FBASHI (94.5%), Blockchain (91.425%), and BBB-EAL (95.75%). The BBB-EAL model had the most excellent mean confidence levels throughout the training and testing. The system's improved capability to reliably evaluate and authenticate users' identities is primarily due to the combination of behavioral biometric data with blockchain-enhanced authentication, leading to increased trust levels.

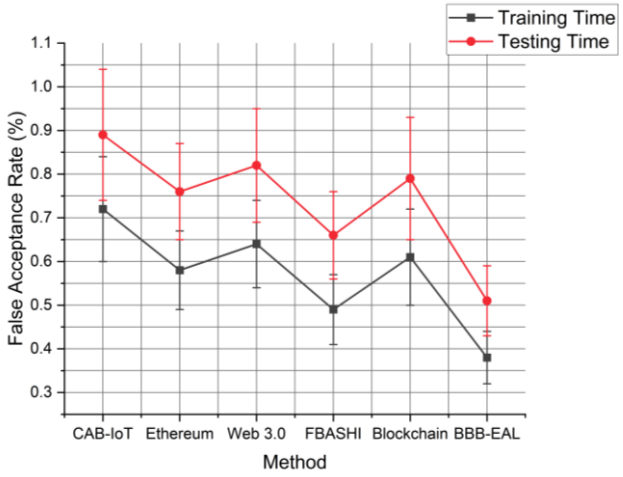

Figure 8: FAR Analysis of Behavioral Biometrics

FAR analysis of behavioral biometrics of different methods is depicted in Figure 8. The FAR for the different approaches were calculated and found to be as follows: CAB-IoT (0.805%), Ethereum (0.67%), Web 3.0 (0.73%), FBASHI (0.575%), Blockchain (0.7%), and BBB-EAL (0.445%). The BBB-EAL, as suggested, demonstrated the most favorable average false acceptance rate (FAR) values throughout both the training and testing phases, thereby highlighting its efficacy as a biometric authentication system. The greater accuracy of this technology in identifying legitimate users from illegal ones is ascribed to the precision of its behavioral biometric recognition model.

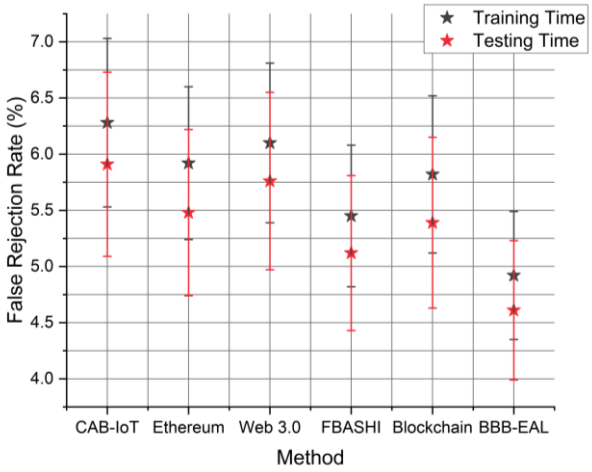

Figure 9: FRR Analysis of Behavioral Biometrics

The FRR analysis of behavioral biometrics of different methods is depicted in Figure 9. The techniques exhibited varying average FRR. FRRs for CAB-IoT, Ethereum, Web 3.0, FBASHI, Blockchain, and BBB-EAL were 6.095%, 5.86%, 5.98%, 5.285%, 5.605%, and 4.765% respectively. The BBB-EAL, as suggested, demonstrated the lowest average FRR values throughout the training and testing phases. This observation emphasizes the robustness of the BBB-EAL in effectively identifying and admitting real users. The model's ability to accurately identify user behavioral biometric patterns has been credited for this accomplishment, resulting in a decrease in valid users being erroneously denied access.

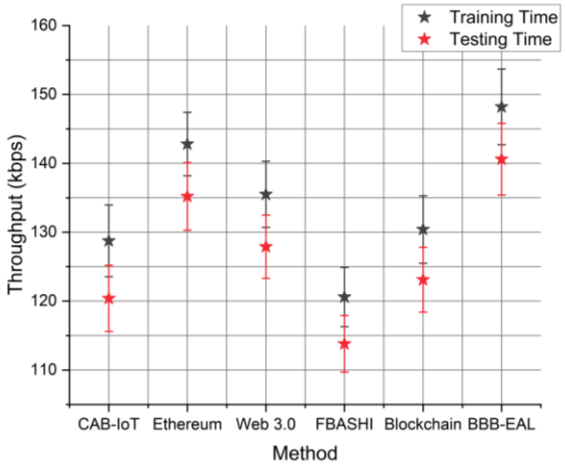

Figure 10: Throughput Analysis of Behavioral Biometrics

Throughput analysis of behavioral biometrics of different methods is shown in Figure 10. The mean throughput numbers (in kilobits per second) for the respective techniques were as follows: CAB-IoT (124.575 kbps), Ethereum (139.5 kbps), Web 3.0 (131.7 kbps), FBASHI (117.2 kbps), Blockchain (126.75 kbps), and BBB-EAL (144.4 kbps). The BBB-EAL demonstrated superior average throughput values throughout the training and testing periods. The enhanced performance of this system is ascribed to its optimized architectural design and streamlined data processing capabilities, leading to accelerated data transfer rates. Integrating behavioral biometric authentication and blockchain upgrading is expected to boost data management efficiency within the technique.

The simulation findings demonstrate that the BBB-EAL approach consistently performed more than other strategies across all measures. The BBB-EAL system showed an average authentication time of 11.625 milliseconds, with training and testing utilization rates of 80.4% and 81.2%, respectively. The average confidence levels were measured at 96.4% and 95.1%, while the false acceptance rates were 0.38% and 0.51%. The false rejection rates were also determined to be 4.92% and 4.61%. The training and testing throughput were recorded as 148.2 kilobits per second and 140.6 kilobits per second, respectively. The result highlights the efficacy of BBB-EAL in providing prompt and reliable authentication by using behavioral biometrics and integrating blockchain technology to reduce mistakes and enhance resource utilization.

5 Conclusion and Future Study

In an age characterized by the Internet's pervasive presence, the need to safeguard its security has emerged as a primary preoccupation. The demand for resilient solutions has increased with the rising incidence of data breaches, unlawful entry, and service interruptions. The present study aimed to tackle these difficulties by introducing a novel authentication layer called the Behavioural Biometric Block Chain-Enhanced Authentication (BBB-EAL). The emergence of this unique framework is attributed to the identified limitations present in current models. Many current models often encounter complex challenges that arise from the heterogeneous nature of Internet Architecture and Protocols. The proliferation of networked devices and platforms has created a multifaceted ecosystem susceptible to cyber-attacks. Achieving a balance between security advances and user experience has proven a formidable problem, necessitating exploring adaptable and innovative methodologies.

The BBB-EAL framework has emerged as a promising solution, successfully integrating behavioral biometrics and blockchain technology. The integrated system implemented an initial static authentication step to create secure communication channels between end users and edge servers. Significantly, this methodology produced access tokens through smart contracts, reducing reliance on intermediaries and promoting heightened security. The simulation findings provided a valuable perspective on the capabilities of the system. BBB-EAL demonstrated exceptional performance across various metrics. It achieved an average authentication time of 11.625 ms, with training and testing utilization rates of 80.4% and 81.2%, respectively. The confidence levels for training and testing were 96.4% and 95.1% respectively. The false acceptance rates were 0.38% and 0.51%, while the false rejection rates were 4.92% and 4.61%. The training and testing throughput was measured at 148.2 kbps and 140.6 kbps, respectively. The results highlight the efficacy of BBB-EAL in attaining reliable and expeditious authentication.

Nevertheless, like every groundbreaking scientific endeavor, other problems and concerns arose. The issue of privacy about behavioral biometric data and the possibility of data faking necessitated thorough scrutiny. The continuing focus was to ensure the framework's flexibility to change cyber threats. The future trajectory requires expanding this study to incorporate more comprehensive investigation and enhancement. The following research will focus on enhancing mechanisms for privacy protection, better safeguarding the components of the blockchain, and studying strategies to adapt to the ever-shifting threat environment. In light of the ongoing evolution of technology, research endeavors need to maintain flexibility and adaptability to tackle new difficulties effectively and influence the future trajectory of Internet security.

References

[1] Alkhateeb, A., Catal, C., Kar, G., & Mishra, A. (2022). Hybrid blockchain platforms for the Internet of Things (IoT): A systematic literature review. *Sensors*, *22*(4), 1-19.

[2] Al-Naji, F.H., & Zagrouba, R. (2022). CAB-IoT: Continuous authentication architecture based on Blockchain for the Internet of Things. *Journal of King Saud University-Computer and Information Sciences*, *34*(6), 2497-2514.

[3] Alsaadi, I. M. (2021). Study on most popular behavioral biometrics, advantages, disadvantages and recent applications: A review. *International Journal of Scientific & Technology Research*, *10*(1), 15-21.

[4] Berentsen, A., & Schär, F. (2019). Stablecoins: The quest for a low-volatility cryptocurrency. *The economics of Fintech and digital currencies*, 65-75.

[5] Boakes, M., Guest, R., & Deravi, F. (2021). Adapting to Movement Patterns for Face Recognition on Mobile Devices. In *Pattern Recognition. ICPR International Workshops and Challenges: Virtual Event, Proceedings, Part VIII*, 209-228. Springer International Publishing.

[6] Boucher, C., & Kooli, M. (2022). Anatomy of money-losing IPOs. *Research in International Business and Finance*, *60*.

[7] Delgado-Mohatar, O., Fierrez, J., Tolosana, R., & Vera-Rodriguez, R. (2020). Blockchain and biometrics: A first look into opportunities and challenges. *In Blockchain and Applications: International Congress*, 169-177. Springer International Publishing.

[8] Hakiri, A., Sellami, B., Yahia, S.B., & Berthou, P. (2020). A Blockchain architecture for SDN-enabled tamper-resistant IoT networks. *In IEEE Global Information Infrastructure and Networking Symposium (GIIS)*, 1-4.

[9] Hisseine, M.A., Chen, D., & Yang, X. (2022). The application of blockchain in social media: a systematic literature review. *Applied Sciences*, *12*(13), 1-25.

[10] https://paperswithcode.com/dataset/bb-mas

[11] Hu, T., Liu, X., Niu, W., Ding, K., Wang, Y., & Zhang, X. (2020). Securing the private key in your blockchain wallet: a continuous authentication approach based on behavioral biometrics. In *Journal of Physics: Conference Series*, *1631*(1). IOP Publishing.

[12] Jung, S.W. (2022). Universal Redactable Blockchain. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, *13*(4), 81-93.

[13] Kassab, M., DeFranco, J., Malas, T., Laplante, P., Destefanis, G., & Neto, V.V.G. (2019). Exploring research in blockchain for healthcare and a roadmap for the future. *IEEE Transactions on Emerging Topics in Computing*, *9*(4), 1835-1852.

[14] Luo, H., Chen, Z., Cui, J., Zhang, H., Zukerman, M., & Qiao, C. (2014). CoLoR: an information-centric internet architecture for innovations. *IEEE Network*, *28*(3), 4-10.

[15] Mason, J., Dave, R., Chatterjee, P., Graham-Allen, I., Esterline, A., & Roy, K. (2020). An investigation of biometric authentication in the healthcare environment. *Array*, *8*.

[16] Mohanta, B.K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet of Things*, *11*.

[17] Oak, R. (2018). A literature survey on authentication using Behavioural biometric techniques. In *Intelligent Computing and Information and Communication: Proceedings of 2nd International Conference, ICICC*, 173-181. Springer Singapore.

[18] Petcu, A., Pahontu, B., Frunzete, M., & Stoichescu, D.A. (2023). A Secure and Decentralized Authentication Mechanism Based on Web 3.0 and Ethereum Blockchain Technology. *Applied Sciences*, *13*(4), 1-17.

[19] Pop, C., Cioara, T., Antal, M., Anghel, I., Salomie, I., & Bertoncini, M. (2018). Blockchain-based decentralized management of demand response programs in smart energy grids. *Sensors*, *18*(1), 1-21.

[20] Sabu, S., Ramalingam, H.M., Vishaka, M., Swapna, H.R., & Hegde, S. (2021). Implementation of a Secure and privacy-aware E-Health record and IoT data Sharing using Blockchain. *Global Transitions Proceedings*, *2*(2), 429-433.
[21] Sundararajan, A., Sarwat, A.I., & Pons, A. (2019). A survey on modality characteristics, performance evaluation metrics, and security for traditional and wearable biometric systems. *ACM Computing Surveys (CSUR)*, *52*(2), 1-36.
[22] Tripathi, K.P. (2011). A comparative study of biometric technologies concerning human interface. *International Journal of Computer Applications*, *14*(5), 10-15.
[23] Thooyamani K.P., et.al (2014). Crypto-devices algorithms test techniques and fault detection, World Applied Sciences Journal, 29(14), 221-227.
[24] Vasa, J., & Thakkar, A. (2023). Deep learning: Differential privacy preservation in the era of big data. *Journal of Computer Information Systems*, *63*(3), 608-631.
[25] Yang, W., Aghasian, E., Garg, S., Herbert, D., Disiuta, L., & Kang, B. (2019). A survey on blockchain-based internet service architecture: requirements, challenges, trends, and future. *IEEE Access*, *7*, 75845-75872.
[26] Zulkifl, Z., Khan, F., Tahir, S., Afzal, M., Iqbal, W., Rehman, A., & Almuhaideb, A.M. (2022). FBASHI: Fuzzy and blockchain-based adaptive security for healthcare IoTs. *IEEE Access*, *10*, 15644-15656.

Authors Biography

Jhimmy Alberth Quisocala Herrera
Doctoral Studies in Mechanical and Electrical Engineering Sciences. With M.Sc, in Mechanical and Electrical Engineering Sciences with a major in Environmental Energy Management. Undergraduate and graduate professor at Universidad Nacional del Altiplano. Dedicated to the construction, operation, regulation and training of the energy sector, and research.

Fernando Antonio Flores Limo
Researcher with several articles published in scientific journals as well as books on marketing management research with extensive experience in thesis advising of master's and doctoral students from several universities Professor of Research Epistemology and Ethics.

Abel Alejandro Tasayco-Jala
Doctor in administration and Educational and Tutorial Psychology. With a Master's Degree in Research and University Teaching. Professor of undergraduate courses at the National University of Cañete and Cesar Vallejo University. Dedicated to higher teaching and research.

Isabel Menacho Vargas
doctor in education administration and public management and governance. With a Master's degree in evaluation of educational quality. Professor at undergraduate and postgraduate courses at the Universidad Nacional Mayor de San Marcos. Dedicated to intellectual property and research.

Wilfredo Barrientos Farias

Doctor in Environmental Sciences Universidad Nacional de Tumbes, Master in Public Management Universidad Cesar Vallejo, Bachelor in Communication Sciences Universidad Nacional San Luis Gonzaga de Ica, Appointed University Professor Universidad Nacional San Luis Gonzaga de Ica, Appointed University Professor Universidad Nacional de Tumbes. Professor Universidad Jaime Bausate y Meza, Former regional director of Comercio Exterior y Turismo Tumbes, general secretary of the Latin American Federation of Social Communication Workers, member of the order of the College of Journalists and national leader of the National Association of Journalists of Peru.

Zoila Mercedes Collantes Inga

I am a university professor, systems and computer engineer and I am a professional passionate about technology and systems engineering. I teach in different universities such as Universidad Nacional de San Marcos, Universidad Nacional Federico Villareal, Universidad Nacional Federico Villareal.

Eber L. Herrera Palacios

Bachelor in Forestry and Environmental Engineering from Universidad Nacional de Tumbes. Degree in Forestry and Environmental Engineering from Universidad Nacional de Tumbes. Master in Education Administration from Universidad Cesar Vallejo. Doctor in Environmental Sciences, Universidad Nacional de Tumbes.