Alexandria Engineering Journal 95 (2024) 59–71

Contents lists available at ScienceDirect

Alexandria Engineering Journal

journal homepage: www.elsevier.com/locate/aej

Original article

User-centric secured smart virtual assistants framework for disables

Fayez Alfayez [a,*], Surbhi Bhatia Khan [b,c]

[a] Department of Computer Science and Information, College of Science, Majmaah University, Saudi Arabia
[b] Department of Data Science, School of Science, Engineering and Environment, University of Salford, United Kingdom
[c] Department of Electrical and Computer Engineering, Lebanese American University, Byblos, Lebanon

ARTICLE INFO

Keywords:
Blockchain
Authentication
Privacy
LSTM
Global updation
Operational efficiency
Disabilities

ABSTRACT

Research on intelligent secured virtual assistant (ISVA) systems for disabled people is essential in order to meet the special requirements and overcome the difficulties they confront. The delicate nature of user interactions makes security and privacy considerations paramount in virtual assistant platforms. The gaps and weaknesses in existing systems can be identified by researching the context of current practice concerning their features, usability, limits in security procedures, and privacy restrictions. Therefore, we present a framework that combines blockchain-based security with federated learning (FL) to address the current shortcomings of virtual assistant technology. The examination focuses on two primary facets of cutting-edge virtual assistants. Firstly, it evaluates existing IoT-based virtual personal assistant systems designed for persons with disabilities, examining their features, usability, and limitations. The aim is to identify the specific needs and requirements of individuals with disabilities, considering their unique challenges and preferences in utilizing virtual assistant technologies. Second, considering the sensitivity of the information sent between users and virtual assistants, it explores the issues of security and privacy that arise while using such systems. The investigation covers authentication, data encryption, access control, and data privacy rules to provide a snapshot of the prevailing state protecting virtual assistants. Besides this, the framework strengthens the privacy and security of virtual assistants using blockchain technology. Through several empirical trials, it is found that the framework maintains better performance and usability, along with the provision of robust security mechanisms to safeguard user data and guarantee privacy.

1. Introduction

Virtual assistants [24] are becoming more adept at understanding the context of user interactions. They can recognize and remember previous commands or conversations, enabling more seamless and personalized interactions for individuals with disabilities. Virtual assistants are now more integrated with a wide range of smart home devices and IoT technologies[9]. A smart virtual assistant relying on the Internet of Things (IoT) [1] refers to an intelligent virtual assistant system that leverages IoT technologies to connect and interact with various devices and services. It utilizes IoT capabilities to gather data, control devices, and provide personalized assistance to users through voice commands or other interfaces. This integration enables individuals with disabilities to control various aspects of their environment. Virtual assistants are constantly expanding their skillsets and applications to better serve disabled individuals.

While virtual assistant technology has seen significant advancements, there is a need to evaluate existing IoT-based virtual personal assistant systems specifically designed for persons with disabilities [3]. This evaluation should focus on their features, usability, and limitations, and identify the specific needs and requirements of individuals with disabilities (Gerges et al., 2023). Additionally, there is a gap in addressing the security and privacy challenges associated with virtual assistant systems, particularly in the context of sensitive personal information involved in user interactions. This research aims to improve the accessibility and inclusivity of virtual assistant systems for individuals with disabilities (Ibrahim et al., 2021). By evaluating existing systems and understanding the unique challenges and preferences of this user group, it provides insights to enhance the design and functionality of virtual assistant technologies, ensuring they meet the specific needs of disabled individuals.

Concerning virtual assistants, the study investigates the crucial aspects of privacy and security. There is an immediate need to strengthen the safeguards against possible exposures in these systems in light of the rising tide of data breaches and privacy invasions. This research looks at state-of-the-art security protocols and presents a new framework that uses the strength of blockchain [4] and the smarts of FL techniques. In an ever-more-connected world, it is crucial to strengthen user data

* Corresponding author.
E-mail address: f.alfayez@mu.edu.sa (F. Alfayez).

https://doi.org/10.1016/j.aej.2024.03.033
Received 25 October 2023; Received in revised form 31 January 2024; Accepted 13 March 2024
Available online 29 March 2024

protection and maintain strict privacy requirements for virtual assistant platforms. Only then can sensitive information be assured of security.

The integration of blockchain-based security [22] and Federated Learning (FL) (Lim et al., 2020) plays a significant role in designing a novel framework for virtual assistant systems to benefit disabled persons. Blockchain's distributed and unchangeable ledger improves the safety and confidentiality of AI assistants. Blockchain technology allows for the secure storage of private user information and interactions, guaranteeing openness, data integrity, and security against manipulation or disclosure ([12]; Wehbi et lal., 2023). FL is a confidentiality preservation machine learning approach that allows participatory model training while avoiding exposing raw user data. FL enables private data to remain on-device while individual user devices participate in model training in the context of virtual assistant systems [25]. This method improves the efficiency and precision of virtual aids for disabled individuals without compromising their right to privacy.

Thus, such procedures enhance user trust, enable better customization of the virtual assistant's behavior, and empower users with insights into how the system assists them. The framework's integration of blockchain and FL not only enhances security and privacy but also showcases the potential of combining these technologies to create more robust and trustworthy virtual assistant systems. The motivation behind intelligent secured virtual assistant (ISVA) systems for disabled individuals lies in addressing their unique needs and challenges, ensuring enhanced accessibility and user experience (Othman, 2023). With disabled users often sharing sensitive information with virtual assistants, the emphasis on security and privacy becomes paramount. Existing systems have revealed gaps in features, usability, and especially in security protocols. To bridge these gaps, the proposed framework amalgamates the robustness of blockchain security [13]with the adaptability of federated learning. The scope encompasses an in-depth evaluation of IoT-based virtual assistants tailored for the disabled, spotlighting their capabilities and constraints. Moreover, it delves into intricate security aspects, from authentication and encryption to access controls[19], ensuring a holistic protection approach for virtual assistants. The ultimate goal is to create a system that offers impeccable usability while ensuring uncompromised data protection and user privacy.

The success of blockchain and federated learning in protecting and securing data motivated us to propose a new system for protecting the virtual system developed for assisting disabled persons (Li, 2023; Zhang, 2022). In the same way, it is true that deep learning is powerful in solving complex issues in the fields of image processing and security. This characteristic inspired us to explore LSTM for implementing the concepts of blockchain and federated learning in this work.

The key contributions are as follows.

- Exploring the combination of blockchain and federated learning for authenticating the virtual system of disabled people is new compared to the state-of-the-art methods.
- Adapting LSTM to implement the concepts of blockchain and federated learning is new.
- The way the proposed work combines different concepts in a novel is new.

The layout of this study is delineated as follows: Section 2 reviews the most relevant studies based on the suggested methodologies in the existing work. Section 3 summarizes the inclusion of the framework and its procedures. Section 4 elaborates on the observed outcomes and their analysis. Finally, Section 5 provides conclusive notes on the research study based on potential technical aspects and future work.

2. Related works

Visual Rahman et al. [21] recently introduced a revolutionary home treatment management system that uses MEC (Mobile Edge Computing) and the IoT. This technology takes a novel approach to help people with physical limitations by collecting and distributing real-time information about their joint range of motion. Those born with or who develop impairments over time will have quick access to diagnostic and analytical data thanks to the framework's use of MEC's strengths. The system protects medicinal data's confidentiality, ownership, and dissemination with blockchain-Tor hybrid security architecture. Preliminary testing has shown that it can handle a high volume of users without negatively affecting performance.

Felix et al. [6] presented Android mobile software that employs cutting-edge technologies like AI, ML, Image/Text Recognition, and more to increase mobility and independence for the visually handicapped. The suggested system provides various features, including voice assistance, item and money identification, digital book comprehension, and conversational relations, to help the visually handicapped navigate new areas with limited access to visual information. The app's voice-activated features make scanning barcodes and reading text from printed materials possible. This technical intervention aims to level the playing field for those with visual impairments so that they, too, may enjoy the outcomes of technological advancement.

Ha et al. [8] performed two studies using the principle of communication privacy management. The preliminary investigation showed that the level of sensitivity of the data and the IVAs (Intelligent Virtual Assistants) had a substantial impact on users' concerns regarding privacy. The second trial indicated that consumers were more concerned about confidentiality while interacting with a partner-role IVA while handling susceptible material but were more likely to rely on a partner-role IVA over a servant-role IVA in situations involving less sensitive information. The results provide light on the theoretical foundations and real-world uses of IVAs.

Namoun et al. [15] provided 2-phase ML framework (2MLF) that comprises comprehensive impairment ontology for enhanced service-based decision-making, create semi-synthetic databases on disabilities-related services, and build an ML system for responsive service decisions. This ML system has two phases: first, it evaluates atomic workloads according to user objectives and profiles, and second, it refines the directory of service proposers according to QoS (quality-of-service) characteristics in light of the individual's impairment. User attributes such as disability background, preferences, surroundings, and accessible technological assets are considered by the technique. This study adds to previous efforts by including accessibility elements into current datasets such as WS-DREAM and QWS V2.0. The suggested method is more accurate in service selection while still meeting accessibility requirements than the more common multifaceted decision-making model like PROMETHEE, SAW, TOPSIS and AHP.

Ngan Van et al. [16] proposed a PriFL-Chain framework, an innovative architecture that protects data owners' confidentiality while using their information in training models. Rather than sharing raw data, individuals could instead share predictive models trained on their information via the approach's utilization of differential confidentiality (DP) and FL. Because of this, the confidentiality of information is increased. All user transactions are recorded on a Blockchain for suitability concerns. Employing InterPlanetary File System (IPFS) and MEC additionally enhances the system's effectiveness by lowering the burden on the primary server and the cost of data transmission. The results of these experiments suggest that combining IPFS, MEC, Blockchain, and FL reduces the high costs associated with learning models and successfully protects individual privacy while drawing from a rich pool of community knowledge.

Qahtan et al. [18] presented a new Multifaceted Assessment and Decision-Making approach known as S-FWZIC (Spherical fuzzy weighted with zero inconsistency) for establishing the importance of security and confidentiality in IoT medical facilities through the use of the blockchain. To do this, they first employed the S-FWZIC technique to assign weights for every resource according to the relationship between the components of blockchain IoT medical facilities and their safety and

confidentiality attributes (such as user login, accessibility, etc.). The Bald Eagle Searching and GRA-TOPSIS (grey relational analysis–technique for order of preference by similarity to ideal solution) optimization methods are used to implement the appropriate weights and evaluate the platforms. Based on the results, it seems that the "access control" feature is the most important (with a weighted value of 0.2070), whereas the "integrity" component is the least important (with a strength of 0.0646). The reliability of the assessment was verified using a sensitivity analysis. The research is meant to aid healthcare organizations in making informed system selections and to point developers toward strengthening system privacy.

Deebak & Hwang. (2023) presented L2FAK (Lightweight Two-Factor Authentication Framework), a novel two-factor verification method built from the ground up for more ingenious eHealth apps. The mobile endpoints and other privacy measures are integral to this architecture. Both official and informal evaluations have validated its resilience against a wide range of threats, including connection hijacking, communication manipulation, and interruption of operation. Implementing FL layered verification to comprehend data attributes at the level of physical security is an exciting aspect of L2FAK. The TensorFlow Collaborative environment was employed to analyze the approach, and it performed well on the FashionMNIST and MNIST datasets. Results indicate that in contrast to previous techniques, FL layered verification successfully guarantees privacy while maintaining accuracy. The communication productivity and overrun proportions of L2FAK have been shown experimentally to be much better than those of contemporary systems.

Goswami et al. [7] explored how technology could be used to level

Table 2
showing the comprehensive analysis by comparing with the recent published 5 papers at least, title, techniques, dataset, and performance, compare the same with your proposed model.

Reference	Dataset	Methodology Algorithm	Strength	Weaknesses
Rahman et al. [21]	Real Time Sensory data	Tor process is a one-time padding process that is used for each transaction address to execute the block chain process.	Developed a framework Mobile Edge Computing with IOT by collecting and distributing real-time information about their joint range of motion	IoT nodes that are participated are mobile edge node and the client node in the therapy process will not allow the third party API system or tools.
Felix et al. [6]	Real time capturing of images	The methodology is reading the features from the real time capturing device and are broadly divide into four categories like M1, M2,M3 and M4.The M1 is the personal,M2 is the mobile app that works for visually disabled persons,M3 is the object detection.M4 is the character Detection	Voice assistance with digitalized narrations with its relations called chat bot which is used to Scan the barcodes and reading the textual information generated by the devices. The camera will take the pictures and explain the scenes inside the picture	Works with only Images or Text only. Not able to work on multi-lingual. The computation power is very less it will work on the images serially no image stitching is possible to understand and combine the scenes clearly.
Namoun et al. [15]	The dataset that are used is WS-DREAM and QWS V2.0	Decision based system which works on two phase • User profilealong with Disabilityand Abilitieswith their user goals. • Context based contains the location, time and the status. Auto sub services selector works on multi task and preprocessing of SPs ranker to preprocess the historical data with XML - IR Indexer.	Created thesynthetic dataset for disability services based on their profiles and the individual impairments.Applying the machine learning on the synthetic data in order to train the multifaceted based decision making machine learning model generates the profiles for the individual impairments	Limited predicted variables that are used. The disabled users and the service providers are not included in the context aware service selection
[16]			• The information will not be shared to create an ML model based on block chainto store the data. It protects the data generated form the owners which undergo for the training.The predictive models will be created hence there is no contact of the raw data. • IPFS,MEC,FL and blockchain reduce the cost	
Qahtan et al. [18]	Real Time Data	The author introduced the weights for each device or hardware by using S-FWZIC methodology.	• The informed system selection process starts by establishing a strong security with the resources which contains weights in relation to confidential-ityintegrity and authentication. • Creating custom weights to each and every resource so that the perception will be created to construct imaginary view to the user.To optimize the resources will be easily done by optimizing the weights	Fuzzy logic needs some computational cost. There are some devices which will be acts like a actual to get weight but it was cloned by the external users.
Deebak& Hwanget al. (2023)	• MNIST • FashionMNIST	Introduced the cloud centric architecture using federated learning layered Architecture -L2FAK with IOT	The Access Points are categorizing the nodes that are present in the architecture • Patient • Expert • Data Center Reducing the computation cost, the L2FAK with IOT was introduced and it has a lightweight operations and it also preserves the privacy attributes of the data authentication.	Evaluation of the instances that are registering to the cloud was not investigated. There is no separate policy to check the privacy and security mechanisms of the instances.
Ha et al. [8]	-	Created a partner-role IVA which primarily focuses on Levels of the sensitivity of the data. Authorization of the partner roles with servant roles	The inspection of the data transmission that is being assigned to the roles of the users like partner and the servant role.	Assigning and Revoking the permissions to the users and maintaining are also difficult

the playing field for people with physical impairments in online education. The article starts with a survey of available aids in online classrooms. It then presents a voice-activated, AI-driven framework with comprehension, instruction, and test-taking modules tailored to the needs of students with special needs. This system can produce fill-in-the-blank and question-and-answer tests as part of its ongoing reviews. The framework is evaluated using Python-based computational resources and the DIKSHA online education platform that hosts electronic publications from the National Organization of Learning and Research. Early findings show promise and improvements for the future are explored. Annexure I information represented in Table 2 comprises the specific details of the reviewed research work for better understanding. On utilizing the following APIs listed in Table 1, the connectivity and performance of the model was assessed.

The realm of intelligent secured virtual assistants (ISVA) for disabled individuals, though burgeoning, is fraught with potential pitfalls in terms of security, usability, and adaptability to unique needs. Despite the surge in IoT-based virtual personal assistant systems tailored for this demographic, there remains a discernible gap in understanding the intricate requirements and challenges faced by disabled users. These challenges encompass not only the functional and usability aspects but also the overarching concerns regarding data security and privacy. The current virtual assistant frameworks often fall short in providing holistic security measures, particularly in areas of authentication, data encryption, access control, and adherence to stringent data privacy norms [10]. The proposition of integrating block chain-based security with federated learning offers a novel approach to address these lacunae. However, the empirical validation of such a fusion in ensuring enhanced performance, user-centric design, and fortified security remains a crucial area awaiting exploration. The pressing need is to develop a system that seamlessly merges the benefits of advanced security technologies with the bespoke requirements of disabled users, ensuring a safe, efficient, and inclusive user experience.

The realm of intelligent secured virtual assistants (ISVA) for disabled individuals, though burgeoning, is fraught with potential pitfalls in terms of security, usability, and adaptability to unique needs. Despite the surge in IoT-based virtual personal assistant systems tailored for this demographic, there remains a discernible gap in understanding the intricate requirements and challenges faced by disabled users. These challenges encompass not only the functional and usability aspects but also the overarching concerns regarding data security and privacy. The current virtual assistant frameworks often fall short in providing holistic security measures, particularly in areas of authentication, data encryption, access control, and adherence to stringent data privacy norms. The proposition of integrating blockchain-based security with federated learning offers a novel approach to address these lacunae. However, the empirical validation of such a fusion in ensuring enhanced performance, user-centric design, and fortified security remains a crucial area awaiting exploration. The pressing need is to develop a system that seamlessly merges the benefits of advanced security technologies with the bespoke requirements of disabled users, ensuring a safe, efficient, and inclusive user experience.

3. Proposed methodology

As discussed in the previous section, the scope of the proposed work is to develop a model to authenticate the virtual system developed for disabled persons [27]. To protect the virtual system from the attack, the proposed work explores new techniques called blockchain and federated learning in this work. More details are presented in the flowchart given in Fig. 1.

3.1. Formulating the problem

To formulate the problem definition mathematically, we focused on the core aspects: the security and privacy of virtual assistants using both block-chain technology and FL.

Axiom 1. *For any set of users U interacting with an ISVA and producing data D, the integration of blockchain B and FL ensures data integrity, security, and privacy, such that the system maintains* usability constraints in terms of latency and data size.

*Data Integrity and Security:*Given that every block B_i in the blockchain contains the hash of the previous block $H(B_{i-1})$, it ensures that the data in B_{i-1} cannot be changed without altering all subsequent blocks. This maintains data integrity. For security, since every transaction in B_i is encrypted and only the owner of the private key can add data to the blockchain, unauthorized access and tampering are prevented.

FL Ensures Privacy: The global model $\ddot{M}$ is updated using:

$$\ddot{M} = M + \sum_{u_i \in U} w_u \Delta M_u \tag{1}$$

Here, only the updates ΔM_u are shared, not the actual D. This ensures that individual user data remains private.

Blockchain ensures Privacy: For any transaction in B involving U, only$\ddot{a}(U)$, the anonymized identify, is visible. Thus, the identity and data of the user remain private in the B_i.

Axiom 2. *Given a virtual assistant system V and a disabled user U, the usability constraint C_U for the user U is defined as:*

$$C_U(V) = (1/|F(V)|) \sum_{f \in F(V)} C(U,f) \tag{2}$$

where, $|F(V)|$ represents the feature counts in V, $C(U,f)$ is the usability

Table 1
List of APIs and its vital components for Integrating ISVA model.

Endpoint	Description	Method	Parameters	Applicability
/api/register	Register a new user on the blockchain	POST	username, password, platform (NVDA/Wheelmap/ SesameEnable)	All
/api/login	Authenticate a user	POST	username, password, platform	All
/api/verifyTransaction	Verify the authenticity of a transaction	GET	transactionId	All
/api/initiateTransaction	Initiate a new transaction on the blockchain	POST	fromUser, toUser, amount, description	All
/api/getUserTransactions	Retrieve all transactions for a user	GET	username, platform	All
/api/ getPlatformTransactions	Retrieve all transactions for a specific platform	GET	platform	All
/api/logout	Log a user out and end the session	POST	sessionId	All
/api/encryptData	Encrypt data using blockchain's public key	POST	data, platform	All
/api/decryptData	Decrypt data using blockchain's private key	POST	encryptedData, platform	All
/api/accessibilitySettings	Retrieve or set accessibility settings for the API	GET/ POST	platform, settings (optional for POST)	All
/api/updatePlatform	Update the platform information (e.g., new version)	POST	platform, version, description	All
/api/checkPlatformStatus	Check the status and version of the platform	GET	platform	All

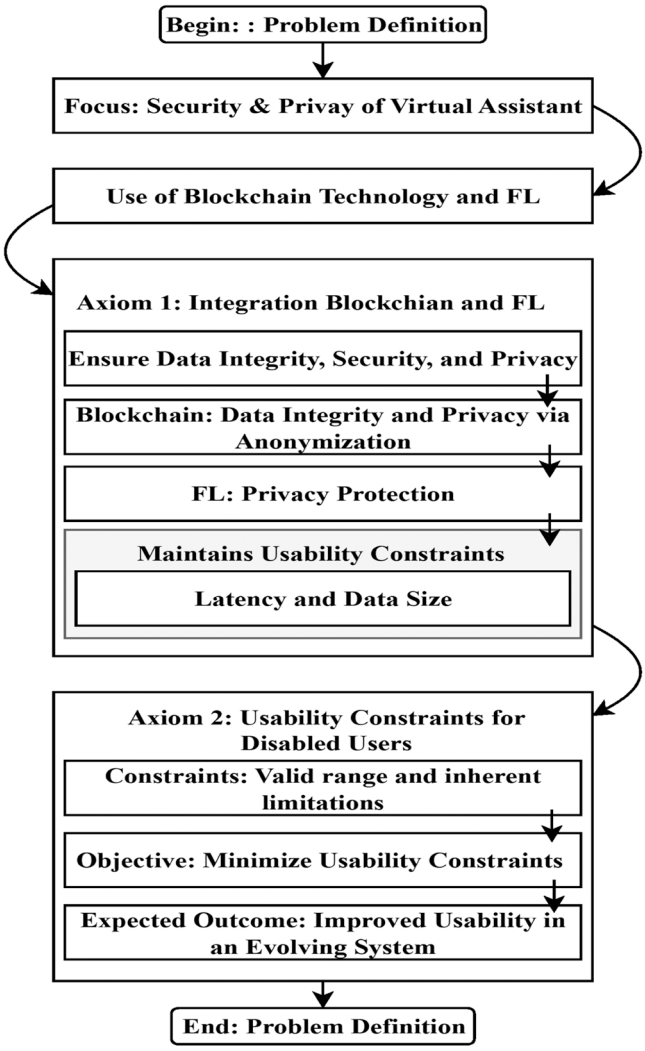

Fig. 1. Flowchart of the research problem.

constraints faced by U when using feature f. The objective is to minimize $C(U,f)$ for all U in D. That is, the goal is to design or modify V such that the usability constraints faced by all disabled users are minimized.

Constraints:

- $0 \leq C(U,f) \leq 1$, *for all d in D and for all f in F(V) — This ensures that the usability constraint values are within the valid range.*
- *For certain disabilities, some features might inherently have usability constraints that cannot be reduced to 0.*

Thus, the expected outcome of a virtual assistant system V' for every user U in D is expressed as, $C_U(V') \leq C_U(V)$,where new system V' has equal or better usability for all disabled users compared to the original system V.

3.2. Overview of ISVA system

The proposed work enhances ISVA system by integrating the proposed secured software, resulting in a new ISVA system for assisting disabled persons. The ISVA system is designed for those with disabilities, it's crucial to consider the range of communication methods, which include voice, touch, gesture, and other specialized means. Equally important is the system's ability to integrate seamlessly with other smart devices and IoT platforms, and whether it offers customization options to cater to individual needs. Furthermore, the presence of built-in accessibility tools, such as screen readers and magnifiers, adds significant value. On the usability front, the ease with which a person with disabilities can set up the system, the intuitiveness of its interface, especially for novices, the clarity and accessibility of its feedback mechanisms, and its proficiency in error handling and troubleshooting are paramount. Potential limitations come in the form of specific hardware prerequisites, any constraints related to software compatibility or updates, the frequency of required maintenance, and the overall cost, which must be reasonable for the majority of users with disabilities. Thus, we integrated the proposed secured framework into the popular open-source application like NVDA, Wheel map, and Sesame Enable. Fig. 2 represents the framework block diagram for the ISVA system.

3.2.1. ISVA operational flow

This data, combined with interaction logs showcasing user commands, ISVA responses, and encountered errors, as well as feedback from user surveys, can be invaluable. Analyzing this data enables us to compute descriptive statistics, discern correlations between user attributes and system interactions derive usability scores based on feedback, and employ machine learning techniques[11], such as decision trees, to pinpoint the most impactful features. Fig. 3 depicts the operational flow of the system.

3.3. The LSTM for authentication

Sequence-to-Sequence LSTM (S2S-Long Short-Term Memory) is employed to handle the varied input and output lengths, end-to-end learning, and customization for disable needs. Therefore, the computational process of S2S-LSTM provides efficient solution for virtual assistant systems designed to cater to the unique needs of individuals with disabilities. These models can handle the variability and complexity of human communication, ensuring that assistive technologies are more effective and inclusive.An LSTM cell processes sequences step-by-step, maintaining a cell state and a hidden state across the sequences. Formally all the four gates are processed accordingly. For a given input I_t at time t, the previous hidden state h_{t-1}, and the previous cell state β_{t-1}, the computation of input, forget, cell-state update, and output gate are represented as follows.

$$\text{Input Gate} : I_G = \varsigma\left(\left[h_{(t-1)}, I_t\right] \bullet w_I + \vartheta_I\right) \tag{3}$$

$$Forget \quad Gate : F_G = \varsigma\left(\left[h_{(t-1)}, I_t\right] \bullet w_f + \vartheta_f\right) \tag{4}$$

$$Cell-state \quad Updation : \beta_G = \varsigma\left(\left[h_{(t-1)}, I_t\right] \bullet w_\beta + \vartheta_\beta\right) \tag{5}$$

$$Output \quad Gate : O_G = \varsigma\left(\left[h_{(t-1)}, I_t\right] \bullet w_O + \vartheta_O\right) \tag{6}$$

$$h_t = O_t \bullet \tanh\tanh \quad (\beta_t) \tag{7}$$

where, ς denotes the sigmoidal function, w_I, w_f, w_β, $w_O$represents the weights of input, forget, cell-state, and output gates, respectively. Similarly, ν_I, ν_f, ν_β, ν_O represent the bias of input, forget, cell-state, and output gates, respectively.

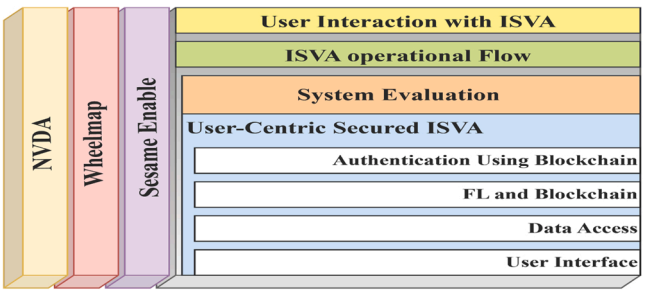

Fig. 2. *: ISVA Framework.*

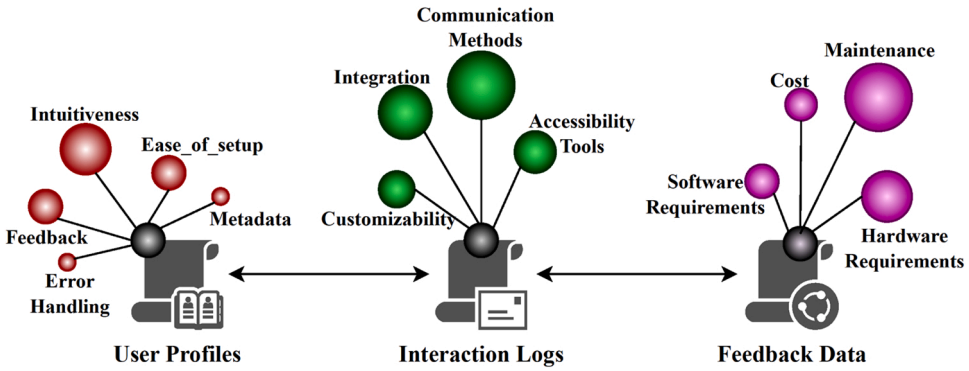

Fig. 3. *Operational Flow of the ISVA System.*

The sequence-to-sequence model performs transformation of one sequence into another. LSTMs, with their inherent ability to handle sequences and remember long-term dependencies, are an ideal choice for this task. The primary S2S model has two primary components: the encoder (ecr) and the decoder (dcr). Both parts are typically composed of LSTM layers. The ecr takes a sequence as input and compresses the information into a memory vector. The last ɦ state of the LSTM is usually used as this context vector, which is expressed as,

$$ɦ_{ecr} = LSTM_{ecr}\left(I_{sequence}\right) \tag{8}$$

Whereas dcr utilizes the context vector from the encoder and generates the output sequence. It starts producing the output sequence one element at a time, using its previous outputs as additional inputs (along with the memory vector).

$$O_{sequence} = LSTM_{dcr}\left(ɦ_{ecr}, ₸_{sequence_i}\right) \tag{9}$$

where $₸_{sequence_i}$ denotes the start of the sequence token.

Federated Learning: The central server initiates a global S2S-LSTM model. Clients (gadgets of disables) download this model, train it locally, and compute updates. These model changes are sent back to the server, which aggregates them, often by averaging. The server then updates the global model with these aggregated changes.

This cycle of local training and global updating continues through several communication rounds until the model converges. Fig. 4 illustrates the working flow FL strategy in accordance with S2S-LSTM.

3.4. Integrating federated learning and blockchain

Authentication using Blockchain: Authentication here refers to the process of verifying a user's identity. We utilized a Decentralized Identifiers (*DIDs*). In this technique, the user is given a unique, self-sovereign identity which is stored on the blockchain. This identity can be used to verify the user without the need for centralized authority.

A technique named "Decentralized Public Key Infrastructure (*DPKI*)" is employed that uses blockchain technology to decentralize trust. This method provides a secure way for users to authenticate themselves. It utilizes asymmetric cryptography where a pair of keys (public and

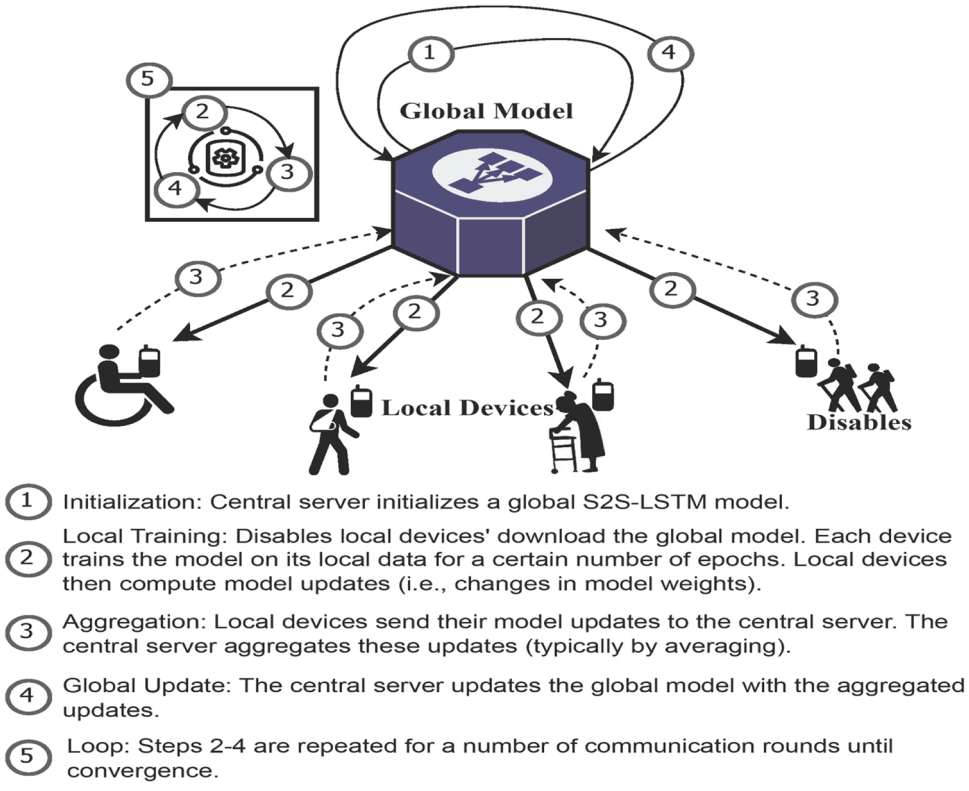

Fig. 4. *: Working Mechanism of FL.*

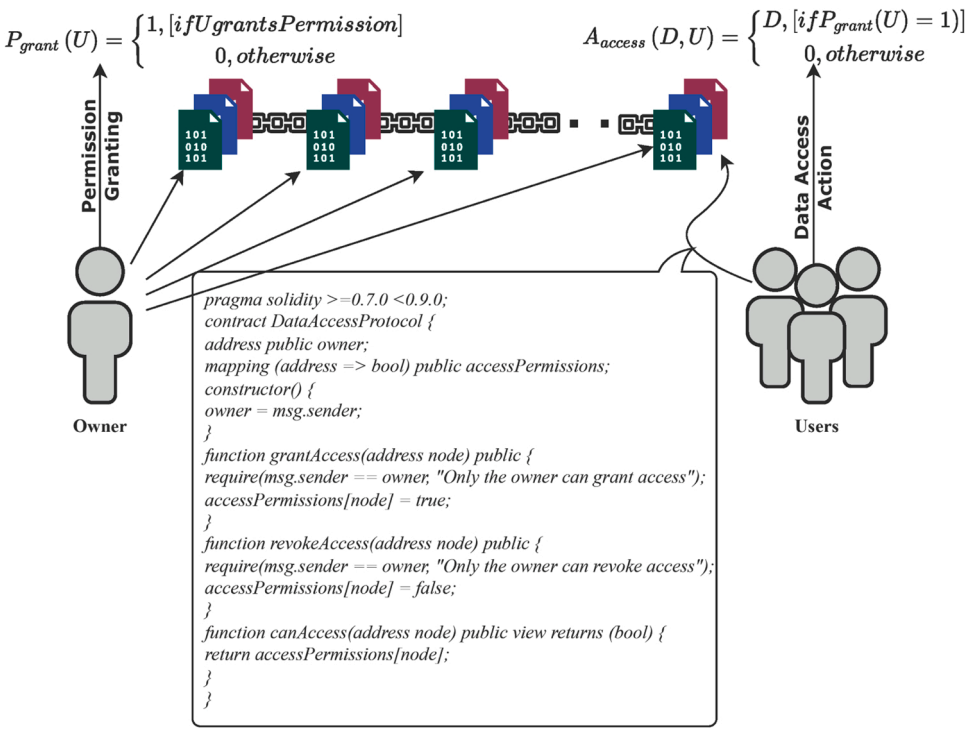

Fig. 5. *Data Access Smart Contract.*

private key) is

$$r = (\Upsilon_{ID}, pk_U) \tag{10}$$

Whenever a specific 'U_i' wishes to authenticate, they sign a message (m) (e.g., timestamp or a nonce for preventing replay attacks [20]) with their $\text{þ}k_U$. This creates a signature, ψ_U.

$$\psi_U = SIGN(\text{þ}k_U, m) \tag{11}$$

Then the U_i sends their Υ_{ID}, m, and the ψ_U to the verifier.

The verifier ($\mathcal{Z}$), upon receiving the Υ_{ID}, m, and the ψ_U, retrieves the corresponding pk_U from the blockchain. They then use this pk_U to check if the ψ_U was generated by the associated $\text{þ}k_U$y, confirming the user's identity.

$$\mathcal{Z} = f_{verify}(\Upsilon_{ID}, m, \psi_U) \tag{12}$$

$$U_i = \{1, \mathcal{Z} == true 0, \mathcal{Z} == false \tag{13}$$

If $\mathcal{Z}$ is true, the U_i is authenticated. Otherwise, theauthentication fails. This method offers a secure and block chain to store the 'hash' of the updated weights of the ISVA involvesutilized. The public key is stored on the blockchain and associated with the user's *DID*, while the private key remains confidential to the user.

Federated Learning and Blockchain: Federated learning involve training ISVA models on a network of devices while keeping data localized. A novel approach could involve using a blockchain to store the 'hash' of the updated weights of the ISVA model. This would allow for a traceable and tamper-proof record of updates, thus enhancing trust and transparency in the FL process. Table 3 signifies the operation flow of fl with blockchain procedures.

Each node i initializes its own model M_i with weightsw_i. A trusted authority initializes the blockchain $B_i$with the genesis block. Each node I performs training on its local dataset $D_i$and produces an updated set of model weights, $w_i^{'}$. Each i computes a cryptographic hash of its new weights, $H_{w_i^{'}}$. The node then signs the H using its private key, creating a signature S_i. Each i broadcasts its hash $H_{w_i^{'}}$ and signature S_i to all other nodes. When a node j receives a hash $H_{w_i^{'}}$ and signature S_i from node i, it verifies the signature using node i's public key. If the signature is valid, node j records $H_{w_i^{'}}$ and S_i in its local copy of the B_i. Once a node has received and verified hashes and signatures from all other nodes, it aggregates the new weights using a specified aggregation function. This results in a new set of aggregated model weights, ϖ_i. The node computes a hash of the aggregated weights H_{ϖ_i} and creates a new block containing H_{ϖ_i} and all received $H_{w_i^{'}}$ and S_i. It then appends this block to its local copy of the blockchain. The node broadcasts its new block to all other nodes. When a node j receives a new block from another node, it verifies the block by checking the hash of the aggregated weights and the individual signatures. If the block is valid, it is added to the blockchain. Consensus is achieved when more than half of the nodes agree on the same blockchain. After the blockchain has been updated, each node i updates its model M_i with the new aggregated weights, ϖ_i. All the procedures are then repeated for each new round of training. This approach ensures that each model update is stored on the blockchain, providing a tamper-proof record of the training process. This enhances trust and transparency in the FL process.

Data Access: A smart contract is implemented for data access control mechanism, where the contract owner can grant or revoke access for specific nodes. Other users can use the canAccess() to check if they have been granted access to the contract. The contract is written in Solidity version 0.7.0 but below version 0.9.0 due to the specified pragma statement at the beginning. Fig. 4 elaborates the data access smart contract procedures.

The execution of the smart contract Θ can be described by the following function:

$$\Theta(D, \mathfrak{c}) = \{A, if \mathfrak{c} is \quad true 0, otherwise \tag{14}$$

where, $\Theta(D, \mathfrak{c})$represents the smart contract function that takes D and certain condition ($\mathfrak{c}$) as parameters, 'A'denotes the specific action that gets executed if $\mathfrak{c}$ is met.

Upon deployment, these contracts contain predefined rules detailing data access and sharing permissions. When data is input into the system, it's encrypted, and any third-party access or processing request is verified against the contract's rules. Successful verification allows data

Table 3
Operation Flow of FL with Blockchain Procedures.

Input: $n_i \in N$ *// a network with N decentralized nodes participating in FL.*
Output: $M_i \mapsto n_i$ *// model updation*

1: Initialization
∀ $(n_i)Do$
initialize( )
$M_i \Leftrightarrow w_i$ *//model and its associated weights*
$T_A \rightarrow B_i$;*// trust authority initialize the block*
End *Do*
2: Local Training
for *i* in range(*1, N+1*):
$w_i \rightarrow initialize(\ )$;
$D_i \rightarrow Load\_local\_data(\ )$; $/D_i = \{d_1, d_2 \cdots d_N\}$
$w_i' \leftarrow train(w_i, D_i)$;
3: Compute and Sign the Hash
for *i* in range(*1, N+1*):
$H \leftarrow hashlib.SHA\_256(\ )$;
$H.update(w_i'.tobyte(\ ))$;*// Conversion to bytes might be necessary depending on the weights format*
$H_{w_i'} = H.digest(\ )$;
$S_i = ₱k_i\left(H_{w_i'}, padding\right)$;
End for
4: Broadcasting
∀ $(n_i)Do$
$broadcast\left(H_{w_i'}, S_i\right)$;
End *Do*
5: Verification
for *j* in range(*1, N+1*):
for *i* in range(*1, N+1*):
$if(i \neq j)$:
// receive the hash and signature from node i
$n_j \leftarrow \left(H_{w_i'}, S_i\right) \in n_i$
// verify the signature using node i's public key
$if\ Ƹ\left[(pk), (S_i), \left(H_{w_i'}\right)\right] = isValid(\ )$
$BC.update\left[(S_i), \left(H_{w_i'}\right)\right]$

// if the signature is valid, record the hash and signature in the local blockchain
End for
End for
6: Aggregation
$\varpi_i = aggragate\left(w_{i_{new}}\right)$;
7: Commit B_i
$H \leftarrow hashlib.SHA\_256(\ )$;
$H.update(\varpi_i.tobyte(\ ))$;
$H_{\varpi_i} = H.digest(\ )$;
$B_{i_{new}} \leftarrow \left[H_{\varpi_i}, BC\right]$;
$BC.update\left(B_{i_{new}}\right)$;
8: $broadcast\left(n_j, B_{i_{new}}\right) \rightarrow n_\infty$;
9. Consensus verification
$Ƹ(₵) \rightarrow BC.appended\left(B_{i_{new}}\right)$;
10: Model Update
for *i* in range(*1, N+1*):
$M(n_i) \rightarrow update\left(M_i \Leftrightarrow H_{\varpi_i}\right)$;
End for

decryption and use, while failed verification denies the request. All interactions are transparently recorded on the blockchain for audit purposes. The goal of the smart contract is to ensure that any third-party data request is always within the bounds of the contract's permissible data set.

$$d_r \subseteq s_R \tag{15}$$

Eq. (6) exhibits that the data requested by third parties (d_r) should always be a subset of the data that is allowed to be processed based on the rules of the smart contract (s_R).

User Interface: A novel user interface could include 'Interactive Visualization Panels' that dynamically helping user to understand the model's decision-making process. The proposed secured model is incorporated with three open-source VPI applications; they are NVDA,

Wheelmap, and Sesame Enable.

Non-Visual Desktop Access (NVDA) ([17].) is a free and open-source screen reader for windows that provides feedback via synthetic speech and Braille. Wheelmap is an open-source app that helps wheelchair users finds accessible places in their surroundings [14]. Sesame Enable (Sesame Enable, n.d.) is an open-source app designed for people with mobility impairments, Sesame Enable lets users control their smartphones with head movements [23]. On utilizing the following APIs listed in Table 4, the connectivity and performance of the model is assessed.

4. Experimental results

4.1. Dataset

To evaluate the proposed model, we consider AudioSet (AudioSet, n.d.), which is a versatile dataset that can assist systems for people with disabilities [2]. Some key attributes of the training datasets are listed in Table 4.

The empirical setup and detailed discussion on the evaluation metrics is conducted further.The performance of the proposed ISVA framework is compared with few relevant competitive approaches (L2FAK, S-FWZIC, PriFL, and 2MLF) that were discussed in previous section.

4.2. Implementation details

Table 5 provides the details of hyperparameters used in the proposed work.

4.3. Evaluating effectiveness of the proposed system

To evaluate the proposed framework that combines blockchain-based security with FL for an ISVA system, we considered a combination of performance, usability, security, and privacy metrics. Here are unique performance metrics along with their computations:

Latency in Data Processing and Retrieval (LDPR): Time taken to fetch, process, and return the required information/data which is computed as,

$$LDPR = time_{end} - time_{start} \tag{16}$$

The observed results from Fig. 6 indicate a clear relationship between the size of the dataset utilized and the average latency of each method. Generally, as the dataset size increases, one would expect latency to increase as well due to the complexity and volume of data being processed. However, this trend isn't consistently seen in the provided data. For instance, the L2FAK method, despite having the smallest dataset size of 50, has a latency of 43.45 ms, which is higher than the PriFL method that utilizes a dataset thrice its size. This can be attributed to the intrinsic efficiency and optimization of certain methods over others. Most notably, the ISVA framework, which is the focal point of the research, exhibits the lowest average latency (23.18 ms) even when applied to the largest dataset (250).

This superior performance can be rationalized based on the integration of blockchain-based security with FL in the ISVA system. The distributed nature of blockchain and the decentralized learning approach of FL can lead to faster processing and reduced latency. Moreover, the system might have been optimized to handle larger datasets efficiently, given its design focus on security and privacy. The impact of the ISVA outcome on the experimental domain is profound. It not only showcases the viability of the proposed framework in terms of efficiency and speed but also reinforces the premise that enhanced security and privacy, when implemented thoughtfully, do not have to come at the cost of system performance. The ISVA's results emphasize the potential for a new standard in virtual assistant systems, especially for persons with disabilities, balancing usability with robust security and privacy.

Number of Successful Authentications (NSA): It is measured in terms of count of successful user authentications over a specific time frame. consider a set of discrete time intervals, say $\{t_1, t_2, \cdots, t_n\}$, and let $a(t_i)$ be the number of successful authentications in the time interval ti, then the NSA over all these discrete time intervals (n) is given as,

$$NSA = \sum_{i=1}^{n} a(t_i) \tag{17}$$

From the observed results depicted in Fig. 7, we verified the authentication process across various experimental time frames for five different models. ISVA consistently shows the highest authentication success rates across all time frames, peaking at 98.13% in the 250-hour mark. This high performance might be attributed to the system's design, which is tailored for persons with disabilities, ensuring usability given their unique challenges and preferences. PriFL also performs consistently well, with success rates mostly above 80%, though it dips to 79.32% at 250 hours. L2FAK and S-FWZIC display more variable performance. While L2FAK has a dip at 150 hours (69.19%), S-FWZIC's lowest is at 100 hours (67.21%). Both methods recover in subsequent time frames. 2MLF shows a generally increasing trend in success rates over time, starting from 69.45% at 50 hours and reaching 79.14% by

Table 4
Characteristics of AudioSet Dataset.

Dataset Characteristics	Description/Values
Total Clips	Over 2 million
Clip Duration	10 seconds each
Audio Event Classes	632 classes
Recordings	22, 000
Feature Size	2.4 Gigabytes
Hierarchy	Yes, classes are hierarchically structured
Source	YouTube videos
Annotation	Manually labeled by humans
Audio Format	YouTube IDs with start/end time offsets (No direct audio files)
Balanced Subset	127 classes, ~10k clips (chosen to balance class distribution)
Unbalanced Subset	All 2 million+ clips
Embeddings	VGGish audio embeddings are available (128-D)
Ontology	Provided as a JSON structure

Table 5
Model Hyperparameters.

Hyperparameters		Values/Ranges
S2S-LSTM	Number of LSTM layers	3
	Number of units (neurons) per LSTM layer	100
	Dropout rate(prevent overfit)	0.5
	Recurrent dropout rate	0.5
	Learning rate	0.001
	Batch Size	128
	Epochs	50
	Optimizer	ADAM (Ajani & Bharadwaj, 2019)
	Loss function	MSE
	Gradient clipping threshold	0.5
	Sequence length	3000 – 6000 time step
	Embedding dimension	100
	Initializer for gates	Random Uniform
FL	No. of clients (disables) participating/round	10–50
	Communication Rounds	(CR) 200
	Local Epoch	10
	Local Batch Size	128
	Learning Rate	0.001
	Aggregation Method	FedAvg [28]
Blockchain	Block Size	2 Megabytes
	Block Creation Time min	5
	Network Size	~1000 nodes
	Hash Function	SHA256 [26].

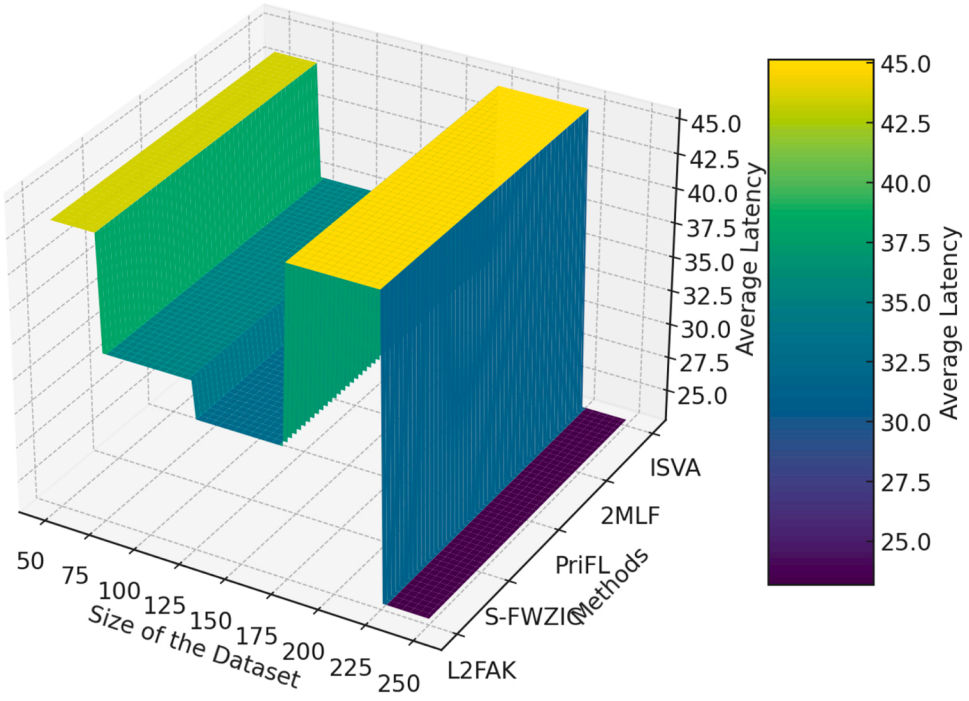

Fig. 6. Analysis of LDPR in the Proposed Context.

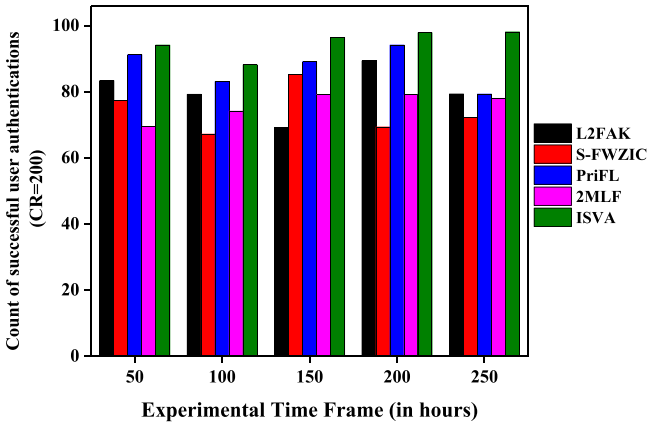

Fig. 7. NSA Assessment and Discussion.

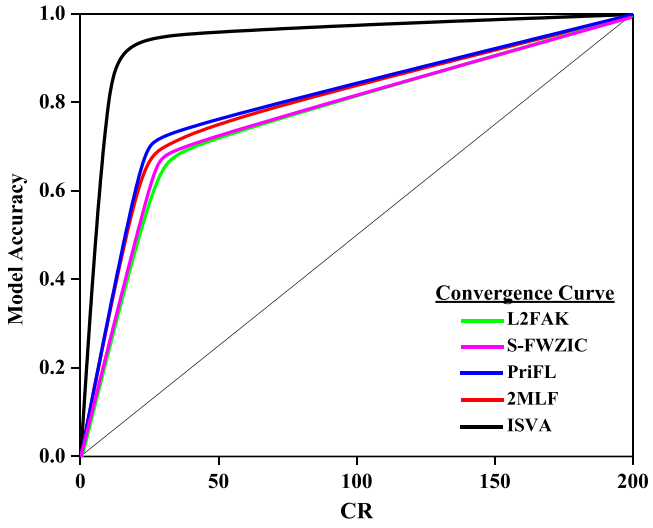

Fig. 8. NSA Assessment and Discussion.

200 hours.

4.4. Evaluating usefulness of the proposed system

Federated Learning Convergence Time (FLCT): Time taken for the FL model to converge or reach a satisfactory accuracy level which is expressed as,

$$FLCT = time_{convergence} - time_{initial} \tag{18}$$

From the outcome represented in Fig. 8, the convergence points indicate the efficiency of each method in achieving a consensus or stable state over 200 communication rounds. L2FAK, with the lowest convergence point of 63.24, suggests optimal performance in terms of speed and, potentially, resource utilization. This is especially crucial for IoT-based virtual personal assistant systems where computational resources may be limited. However, rapid convergence must not compromise the blockchain's inherent security features and FL's decentralized nature. While ISVA's highest convergence point of 98.21 might imply a more prolonged communication or more extensive data processing, it could also hint at a deeper, more thorough security verification process, balancing speed with robustness. The other methods, S-FWZIC, 2MLF, and PriFL, offer varying degrees of efficiency, emphasizing the need to strike a balance between fast convergences and maintaining rigorous security and privacy standards, especially for the sensitive user group in focus.

Privacy Breach Incidents (PBI) Vs Data Transaction Throughput on Blockchain (DTTB): Both PBI and DTTB is analyzed in Fig. 8. Count of reported incidents over a specific time frame where user privacy was compromised. For each model, the proportion of incidents related to user privacy compromise compared to the total number of incidents across 200 CR. Number of data transactions processed per second on the blockchain which is measured in transactions per second (TPS). Methods with higher transaction throughput tend to have fewer privacy breach incidents. Conversely, methods with lower transaction throughput have more privacy breach incidents.

Fig. 9 showcases the correlation between transaction throughput and privacy breach incidents for various methods. The number of transactions processed per second (TPS) increases, the number of privacy breaches appears to decrease.The methods are as following: Layer-2 Framework for Anonymous Key Generation (L2FAK) has a throughput of 1200 TPS and has experienced 10 privacy breaches.Secure Function With Zero-Information Leakage and Computational Leakage (S-FWZIC) which is a multi-party computation (MPC) protocol.has a throughput of 1400 TPS and has experienced 8 privacy breaches.Privacy-preserving Federated Learning(PriFL) has a throughput of 1600 TPS and has experienced 5 privacy breaches.Two-Party Machine Learning Framework (2MLF)has a throughput of 1800 TPS and has experienced 4 privacy breaches.and Inductors, Superconductors, and Voltage Amplifiers (ISVA)has the highest throughput of 2000 TPS and has experienced the fewest privacy breaches, with only 3. These findings underscore the criticality of security and privacy in virtual assistant technologies, particularly when integrated into IoT-based solutions for persons with disabilities. The graph's evident decline in privacy breach incidents with a concomitant rise in data transaction throughput supports the abstract's claim about the proposed blockchain-based framework's capability to bolster the security and privacy of virtual assistants. This proficiency is notably displayed in the exemplary performance and stringent security mechanisms of ISVA methods. This method not only provides the highest throughput but also minimizes breach incidents, underscoring its proficiency in safeguarding user data and ensuring privacy. Consequently, the graph serves as a tangible testament to the framework's effectiveness in curtailing privacy breaches while preserving high transactional efficiency, signifying its viability for tangible applications.

User Engagement Score (UES): score based on the frequency and duration of user interactions with the ISVA. It is the average engagement time or frequency from user logs. To calculate the UES based on the frequency and duration of user interactions with the ISVA, we can break this down into two components:

Frequency of Interactions (FI): This refers to how often a user interacts with the ISVA during a specific period. It can be calculated by counting the number of interactions (e.g., number of commands, questions, or any other form of communication) from the user logs.

Duration of Interactions (DI): This measures the average length of time a user spends in a single interaction with the ISVA. To compute this, we can sum the duration of all interactions and then divide by the total number of interactions. Given these two components, the UES is computed as a weighted average of FI and DI:

$$UES = (w_1 \times FI) + (w_2 \times DI) \tag{19}$$

where, w_1 and w_2 is the weight assigned to the FI and DI, respectively. $w_1 + w_2 = 1$ to ensure the weights sum up to 1. In practice, the weights w_1 and w_2 is adjusted based on the importance of each factor in determining user engagement.

Fig. 10 presents a visualization of the User Engagement Score (UES) across various methods: L2FAK, S-FWZIC, PriFL, 2MLF, and ISVA. These methods represent different approaches to implementing virtual assistant technology. The x-axis signifies the Frequency of Interactions (FI) with values ranging approximately from 5 to 30, while the y-axis represents the Duration of Interactions (DI) with similar range values. The contour shading indicates the User Satisfaction (US) levels, with darker shades indicating higher satisfaction.

From the outcome, it's evident that the ISVA method, with FI and DI values approximately at 27 and 28 respectively, achieves the highest user satisfaction, represented by the darkest shade. This could be attributed to its superior features, usability, and robust security mechanisms, ensuring data privacy and protection. On the other hand, methods like L2FAK, with FI and DI values roughly at 7 and 8, lie in regions of lower user satisfaction. This might imply potential limitations or shortcomings in their approach to addressing the unique challenges faced by users with disabilities.

In essence, the results reinforce the idea that combining blockchain security with federated learning, as possibly employed in the ISVA method, ensures not only enhanced user engagement but also robust security and privacy, addressing the critical concerns of the modern virtual assistant ecosystem.

5. Discussion

The proposed work that combines blockchain-based security with federated learning (FL) appears to bolster ISVA's robustness. Such high rates of successful authentication suggest that the mechanism provides both security (through blockchain and FL) and usability, which is crucial for virtual assistants catering to individuals with disabilities. The fluctuating success rates in other methods may be attributed to various factors, such as the granularity of insights, system capacity, and historical data. However, ISVA's consistently superior performance underscores the importance of designing systems with the end user in mind, especially when catering to individuals with specific needs and challenges. Furthermore, the integration of blockchain technology not

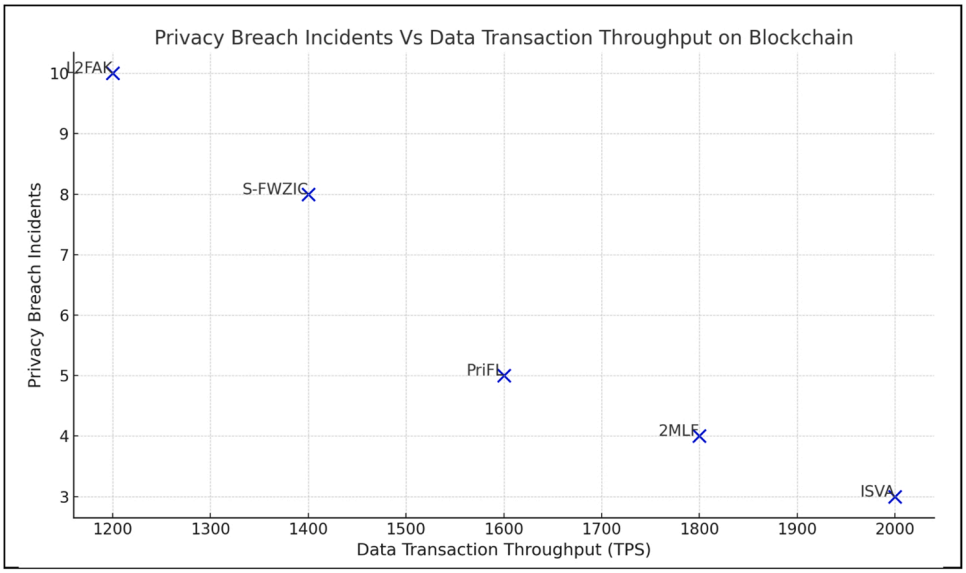

Fig. 9. Analysis of PBI Vs DTTB.

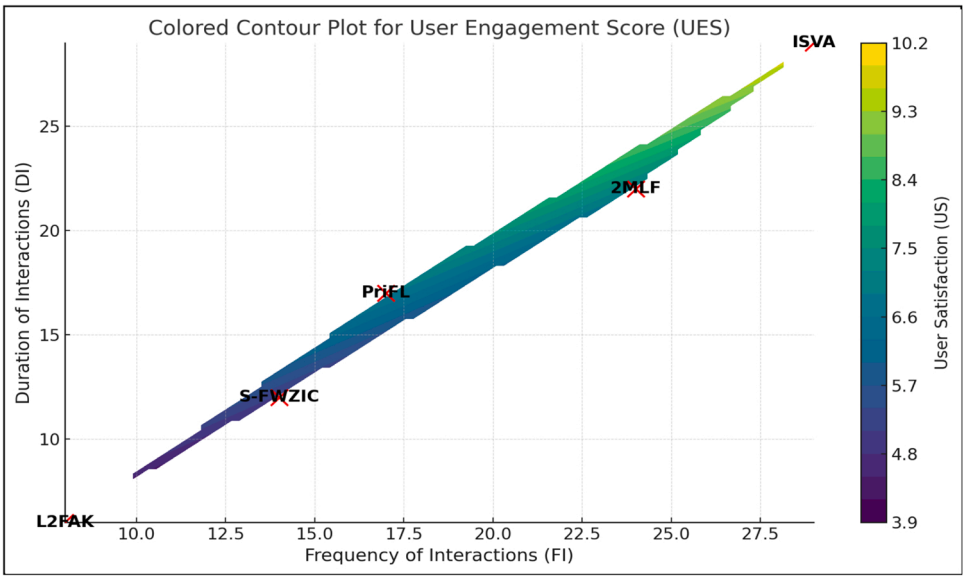

Fig. 10. *Analysis of UES.*

only enhances security but also ensures data privacy, making it a preferred choice for users concerned about their information's safety.

This study on improving virtual assistant systems with blockchain technology and FL has several important implications for managers:

- Virtual assistant systems that combine blockchain with FL improve upon existing security flaws and provide better privacy management. This means a more robust guarantee of data privacy and security for managers, which is vital for retaining customer confidence, particularly in industries dealing with sensitive information.
- Research emphasizes the significance of user-centric design, especially for people with impairments, leading to an improved user experience and accessibility. Managers can think about this strategy if they want to make their products more accessible and inclusive, which might increase sales and happiness among customers.
- The study points to a forthcoming technology change in its future predictions, particularly about quantum computing and edge computing. To take advantage of new possibilities and reduce risks, managers need to keep themselves informed and ready for these developments.
- Businesses may follow the suggested framework's lead in providing customized user experiences and incorporating continuous feedback loops into their services or products. More personalized customer experiences and incremental product enhancements driven by user input are possible outcomes of this research.

The suggested architecture employs smart contracts for data management, integrates Federated Learning with Blockchain, and provides a balanced analysis of the drawbacks and benefits of performance, usability, and security.

When it comes to safety, the foundation is exceptional. By creating an immutable record, blockchain technology dramatically improves data reliability and user confidence. Implementing a Decentralized Public Key Infrastructure (DPKI) further strengthens this by providing a more secure authentication mechanism, lowering the risks of unwanted access and identity theft. Furthermore, data access is tightly managed and complies with privacy requirements thanks to the integration of encryption and smart contracts for data privacy rule enforcement.

When it comes to performance, the framework is designed to be efficient. Data transport and central processing may be resource-intensive; federated learning enables decentralized data processing to alleviate this. In addition to improving efficiency and accuracy, local processing makes model training and updates more responsive and data-specific at each node. However, delays introduced by the complexity of blockchain operations, the overheads needed in maintaining the ledger, and executing smart contracts might impact real-time data processing and decision-making (M. [5]).

In this perspective, usability has both positive and negative aspects. One positive aspect for users who are concerning privacy and data management is that the system could be more robust and less reliant on central authority due to its decentralized design. Users without a solid technical background may find the learning curve of blockchain technology and FL relatively high. The intricacy of the framework may affect the user experience, which might restrict its adoption to people with a greater level of technical skill.

6. Conclusion and future work

The proposed research framework, which incorporates the strengths of blockchain security with FL, addresses the pressing inadequacies of contemporary security issues in virtual assistant technologies. The results drawn from various trials underline significant findings. For instance, despite the intuitive expectation of increased latency with larger datasets, certain methods like L2FAK and PriFL buck this trend. Remarkably, the enhanced ISVA framework, the centerpiece of this research, consistently outperforms in terms of reduced latency, even with the most extensive dataset, which is because of the fusion of blockchain and FL. Results also highlight ISVA's remarkable authentication success rates, peaking at an impressive 98.13%, which can be attributed to its user-centric design and robust blockchain infrastructure. The convergence points further emphasize the efficiency of these methods, with ISVA's slightly higher value possibly hinting at a deeper security verification process. Moreover, the correlation between transaction throughput and privacy breach incidents brought to light ISVA's unmatched ability to combine high throughput with minimal breaches. Lastly, the UES contour visualization underscores ISVA's superior user engagement, achieving the pinnacle of user satisfaction with FI and DI values around 27 and 28. However, there is scope for extending the proposed system to address the problem of complex situations. For example, fusing and integrating different techniques on different datasets of the systems.

Moving forward, we envision harnessing the power of quantum computing to further bolster the security infrastructure of virtual assistants. Advanced ML algorithms, coupled with edge computing, can enhance real-time processing capabilities. Additionally, integrating adaptive user interfaces will ensure a more personalized user experience, especially for individuals with disabilities. Continuous feedback loops and AI-driven insights will be pivotal in refining and evolving the system to cater to emerging user needs.

Declaration of Competing Interest

We declare that we have no conflict of interests that may have influenced the research or the interpretation of the results presented in this manuscript that stated as "High-End User-Centric Secured Smart Virtual Assistants Framework for Persons with Disabilities"

Acknowledgment

The authors extend their appreciation to the King Salman center For Disability Research for funding this work through Research Group no KSRG-2023-513.

References

[1] C. Angulo, A. Chacón, P. Ponsa, et al., Towards a cognitive assistant supporting human operators in the Artificial Intelligence of Things, Internet Things 21 (2023) 100673, https://doi.org/10.1016/j.iot.2022.100673.
[2] AudioSet. (n.d.). Research.google.com. Retrieved August 12, 2023, from ⟨https://research.google.com/audioset/index.html⟩.
[3] M. Bolaños, C. Collazos, F. Gutiérrez, et al., Adapting a Virtual Assistant Device to Support the Interaction with Elderly People, Proc. 6th Int. Conf. Inf. Commun. Technol. Ageing Well E-Health (2020), https://doi.org/10.5220/0009840102910298.
[4] B. Cao, X. Wang, W. Zhang, H. Song, Z. Lv, A many-objective optimization model of industrial internet of things based on private blockchain, IEEE Netw. 34 (5) (2020) 78–83, https://doi.org/10.1109/MNET.011.1900536.
[5] M. Chahoud, H. Sami, A. Mourad, S. Otoum, H. Otrok, J. Bentahar, M. Guizani, ON-DEMAND-FL: a dynamic and efficient multi-criteria federated learning client deployment scheme, IEEE Internet Things J. vol. 10 (18) (2023) 15822–15834, https://doi.org/10.1109/JIOT.2023.3265564.
[6] S.M. Felix, S. Kumar, A. Veeramuthu, et al., A Smart Personal AI Assistant for Visually Impaired People, 2nd Int. Conf. Trends Electron. Inform. (ICOEI) 2018 (2018), https://doi.org/10.1109/icoei.2018.8553750.
[7] T. Goswami, S.R. Javaji, K.K. Nagwanshi, et al., Framework for voice-controlled ai teaching assistant for specially-abled, 3rd Int. Conf. Artif. Intell. Signal Process. (AISP) 2023 (2023), https://doi.org/10.1109/aisp57993.2023.10135015.
[8] Q.-A. Ha, J.V. Chen, H.U. Uy, E.P. Capistrano, et al., Exploring the privacy concerns in using intelligent virtual assistants under perspectives of information sensitivity and anthropomorphism, Int. J. Hum. –Comput. Interact. 37 (6) (2020) 512–527, https://doi.org/10.1080/10447318.2020.1834728.
[9] N. Hu, Z. Tian, H. Lu, X. Du, M. Guizani, A multiple-kernel clustering based intrusion detection scheme for 5G and IoT networks, Int. J. Mach. Learn. Cybern. 12 (11) (2021) 3129–3144, https://doi.org/10.1007/s13042-020-01253-w.
[10] H. Li, Q. Huang, J. Huang, W. Susilo, Public-key authenticated encryption with keyword search supporting constant trapdoor generation and fast search, IEEE Trans. Inf. Forensics Secur. 18 (2023) 396–410, https://doi.org/10.1109/TIFS.2022.3224308.
[11] S. Li, Q. Zhang, X. Wu, W. Han, Z. Tian, Attribution classification method of APT malware in iot using machine learning techniques, Secur. Commun. Netw. 2021 (2021) 1–12, https://doi.org/10.1155/2021/9396141.
[12] Z. Lian, Q. Zeng, W. Wang, T.R. Gadekallu, C. Su, Blockchain-based two-stage federated learning with non-IID data in IoMT system, IEEE Trans. Comput. Soc. Syst. 10 (2022) 1701–1710, https://doi.org/10.1109/TCSS.2022.3216802.
[13] Y. Liu, C. Zhang, Y. Yan, X. Zhou, Z. Tian, J. Zhang, A Semi-centralized trust management model based on blockchain for data exchange in IoT system, IEEE Trans. Serv. Comput. 16 (2) (2023) 858–871, https://doi.org/10.1109/tsc.2022.3181668.
[14] A. Mobasheri, J. Deister, H. Dieterich, Wheelmap: the wheelchair accessibility crowdsourcing platform, Open Geospatial Data, Softw. Stand. 2 (1) (2017), https://doi.org/10.1186/s40965-017-0040-5.
[15] A. Namoun, A.A. Abi Sen, A. Tufail, A. Alshanqiti, W. Nawaz, O. BenRhouma, et al., A Two-Phase Machine Learning Framework for Context-Aware Service Selection to Empower People with Disabilities, Sensors 22 (14) (2022) 5142, https://doi.org/10.3390/s22145142.
[16] L. Ngan Van, A. Hoang Tuan, D. Phan The, T.-K. Vo, V.-H. Pham, A privacy-preserving approach for building learning models in smart healthcare using blockchain and federated learning, 11th Int. Symp. . Inf. Commun. Technol. (2022), https://doi.org/10.1145/3568562.3568665.
[17] NV Access. (n.d.). NV Access. ⟨https://www.nvaccess.org/⟩.
[18] S. Qahtan, K.Y. Sharif, A.A. Zaidan, H.A. Alsattar, O.S. Albahri, B.B. Zaidan, H. Zulzalil, M.H. Osman, A.H. Alamoodi, R.T. Mohammed, Novel multi security and privacy benchmarking framework for blockchain-based IoT healthcare industry 4.0 Systems, IEEE Trans. Ind. Inform. 18 (9) (2022) 6415–6423, https://doi.org/10.1109/tii.2022.3143619.
[19] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, B. Fang, A survey on access control in the age of internet of things, IEEE Internet Things J. 7 (6) (2020) 4682–4696, https://doi.org/10.1109/jiot.2020.2969326.
[20] K.M.K. Raghunath, V.V. Kumar, M. Venkatesan, K.K. Singh, T.R. Mahesh, A. Singh, XGBoost regression classifier (XRC) model for cyber attack detection and classification using inception V4, J. Web Eng. (2022), https://doi.org/10.13052/jwe1540-9589.21413.
[21] M.D.A. Rahman, M.S. Hossain, G. Loukas, E. Hassanain, S.S. Rahman, M. F. Alhamid, M. &Guizani, Blockchain-based mobile edge computing framework for secure therapy applications, IEEE Access 6 (2018) 72469–72478, https://doi.org/10.1109/access.2018.2881246.
[22] S. Rani, H. Babbar, G. Srivastava, T.R. Gadekallu, G. Dhiman, Security framework for internet of things based software defined networks using blockchain, IEEE Internet Things J. 10 (2022) 6074–6081, https://doi.org/10.1109/JIOT.2022.3223576.
[23] Sesame Enable. (n.d.). Sesame Enable. ⟨https://www.sesame-enable.com/⟩.
[24] A. Soofastaei, Introductory chapter: virtual assistants, Virtual Assist. (2021), https://doi.org/10.5772/intechopen.100248.
[25] Y. Wan, Y. Qu, L. Gao, Y. Xiang, Privacy-preserving blockchain-enabled federated learning for B5G-driven edge computing, Comput. Netw. 204 (2022) 108671, https://doi.org/10.1016/j.comnet.2021.108671.
[26] Wang, M., Duan, M., & Zhu, J. (2018). Research on the Security Criteria of Hash Functions in the Blockchain. Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts - BCC '18. https://doi.org/10.1145/3205230.3205238.
[27] X. Zhao, Y. Zhang, Y. Yang, J. Pan, Diabetes-related avoidable hospitalisations and its relationship with primary healthcare resourcing in China: A cross-sectional study from Sichuan Province, Health Soc. Care Community 30 (4) (2022) e1143–e1156, https://doi.org/10.1111/hsc.13522.
[28] Y. Zhou, Q. Ye, J. Lv, Communication-efficient federated learning with compensated overlap-fedAvg, IEEE Trans. Parallel Distrib. Syst. 33 (1) (2022) 192–205, https://doi.org/10.1109/tpds.2021.309033.