Cluster Computing
https://doi.org/10.1007/s10586-024-04515-2

Comprehensive framework for implementing blockchain-enabled federated learning and full homomorphic encryption for chatbot security system

Nasir Ahmad Jalali[1] · Chen Hongsong[1]

Received: 14 January 2024 / Revised: 8 April 2024 / Accepted: 16 April 2024

Abstract
Chatbot is an artificial intelligence application that can provide a conversational environment between humans and machines. Most organizations and industries are willing to lay out their services through chatbots because they can provide 24/7 customer support. Meanwhile, it raises security and privacy challenges like access control, data leakage during transmission, SQL injection attacks, and language model attacks, which make the users concerned about their data, performance, and accuracy. Therefore, this research paper proposes a comprehensive framework integrating blockchain, federated learning, and a fully homomorphic encryption algorithm with face recognition to solve the above-mentioned chatbot's challenges. The experimental result shows that a distributed system improves chatbot accuracy (90%) and that more transactions in less time with more clients do not affect the performance. In contrast, more iterations and clients will decrease the accuracy, performance, and transactions in a centralized system. In addition, fully homomorphic encryption improves and speeds up the data encryption process. It encrypted more data (1792 MB) in a small amount of 1240 times per second, and conversations and transactions can be transferred via a secure network to ensure the confidentiality, integrity, and authenticity of users' data. The implementation of such a comprehensive framework in real-life situations can improve chatbot security when it actively works as a customer agent in an organization.

Index Terms Chatbot · Security/Privacy · Federated learning · Full homomorphic encryption · Blockchain

1 Introduction

Technological advancement, with the involvement of businesses, has led the world to develop chatbots to help businesses and industries provide assistance to their end users. [1] Chatbot is composed of the two words chat and robot, which is an automated computer program that can mimic human communication patterns to interact with humans via text and voice conversation (conversation of humans with machines). Chatbots are computer-related artificial programs that are developed in a conversational manner through various communication channels such as text messaging, voice, and mobile applications. Chatbots are virtual assistants that must play various roles and receive natural language input to generate intelligent responses and services, access data, and help users complete a specific task [2].

Chatbots try to understand users' requests and provide a specific answer without human interference. Whenever the users' query or conversation intersects with the chatbot's current knowledge, then the conversation will be passed to the human operator to provide the answer. Recently, modern chatbots can learn through machine learning algorithms during conversations with users [3]. People feel less comfortable talking to chatbots than talking to humans because they have less experience dealing with chatbots; some of them even drop out of the conversation if they feel they are not talking to a real person. However, studies have shown that modern chatbots are based on conversation data associated with multiple data sources, making the

✉ Chen Hongsong
Chenhs@ustb.edu.cn

Nasir Ahmad Jalali
nasir.zehand@gmail.com

[1] Department of Computer Science, University of Science and Technology Beijing (USTB), Beijing 100083, China

Published online: 12 May 2024

conversation more natural than if they were talking to a real person [4].

In general, chatbots are just input/output computer programs, as shown in Fig. 1, pre-programmed by natural language processing (NLP) to be used instead of humans for classical conversations such as health advice, e-banking, e-shopping, etc., to avoid wasting time. On the other hand, people are cautious when it comes to their personal data because chatbots collect, learn, and deal with users' personal data, so this kind of chatbot leads to security challenges. Users do not know how to store, use, share, and handle their sensitive personal identity information (PII). The main goal of this paper is to investigate and discuss security, privacy, transparency, and data protection issues in order to find ways to minimize the above security issues through a systematic investigation in the era of chatbots to help organizations improve the security of chatbots they are using as agents to offer services.

A financial chatbot is also a kind of chatbot in which the financial organization provides its services to its users through a chatbot. It can conduct transactions and provide financial advice to users via chat or voice. They need to improve the security and privacy of chatbots to prevent fraud in the financial system [5].

1.1 Contribution

Nowadays, artificial intelligence-based chatbots play an important role in business and industry. Natural language processing (NLP) underpins their operations, enabling them to provide services and provide specific answers in response to user requests. Since chatbots communicate over an Internet connection and collect a huge amount of data for conversations, it raises data security and privacy challenges during user communication and the exchange of data for service inquiries. Therefore, we list our further contribution as follows:

- We developed a framework for chatbot security and privacy.
  1. Secure login access to the chatbot
  2. Secure data transmission between user and chatbot
  3. Secure storage and processing of data in the backend of the chatbot
- The framework has integrated blockchain-enabled federated learning and homomorphic encryption algorithms with facial recognition as new technologies for security and privacy.
- Concentration on chatbots security systems's defects and how to enhance users' trust, as well as chatbots accuracy and performance in the future.

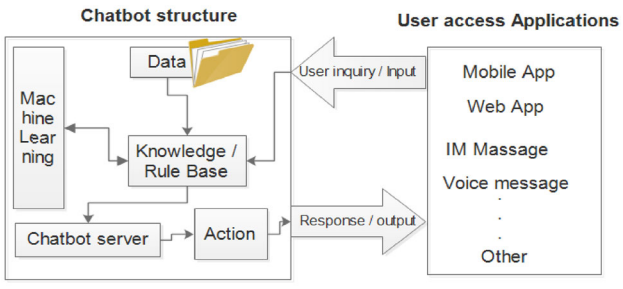


Fig. 1 Chatbot general system [5]

1.2 Research novelty

The novelty of this research is that it proposes the first comprehensive framework to improve chatbot security that consists of various security procedures. The framework integrated face recognition technology to ensure that the chatbot is connected to an authorized user and a full homomorphic encryption algorithm to secure and guarantee end-to-end data security during chatbot interaction with the user; furthermore, the framework embodied blockchain-enabled federated learning at the backend of chatbots to introduce a new distributed technique for training chatbots while preserving user privacy to ensure that the user's sensitive data is not exposed during the training process; and a decentralized identity management system to guarantee data integrity, transparency, performance, and accuracy.

1.3 Paper organization

The paper is organized as follows: Sect. 2 explains related work on the topic. Section 3 explains the architecture and application of chatbot systems. Section 4 explains the research methodology. Section 5 describes the result and the discussion. Section 6 describes the results and future work.

2 Related work

Professionals, particularly researchers, have recently focused their attention on chatbots and the security and privacy of the information they collect or exchange with users. While there are several researchers who have attempted to study information security and privacy issues in chatbots, users are still concerned about the security and privacy, transparency, integrity, and confidentiality of information collected by chatbots. According to our knowledge, there is currently no work that tackles the security and privacy of access or login, data transfer, or data in the backend of the chatbot. Previous work has only

analyzed the security and privacy of data transmission, access control, or security in the rest of the system, but not the complete security and privacy triad such as access or login control, secure data transmission, and security in the backend of chatbots.

The author of [6] studied security and privacy issues in his work and recommended the authentication and encryption method to improve security and privacy only in the transmission part between chatbot and user. The goal of [7] 's study is to develop chatbots that support various functionalities and provide restrictive security measures to protect users' personal data during data transmission in healthcare scenarios. The research in [8] examined various aspects of chatbots, including security and privacy issues, and found that chatbots faced some security challenges, such as threats, vulnerabilities, data tampering, and data theft. Therefore, they recommended some solutions such as two-factor authentication, e.g., username and password, and sending a confirmation email or message containing security questions to overcome the above challenges, but these solutions are not responsive for chatbot security. The authors [9] stated in their research article that chatbots collect a huge amount of data during a conversation with users and store it. Users are concerned about losing control of their data after conversing with the chatbot, third-party access to personal information, and inappropriate use of sensitive data. The solution based on their survey paper recommended that all technical parts of the chatbot should be improved for security and protection of users' sensitive data. Another author [10] studied web-based chatbots to increase sales and provide timely and punctual responses to their customers to gain insight into customer behavior, but in terms of security, they did not receive a guarantee because they had vulnerabilities such as tracking cookies and sharing data with third parties. After completing their survey, the authors found that despite the many websites promising privacy and security to customers, users are unknowingly exposed to insufficient security guarantees by companies selling their services using chatbots.The author's goal [11] was to get an overview of the security issues related to ChatGPT, such as malicious text, private data disclosure, fraudulent services, and unethical content production, so the author presented an empirical study to investigate the effectiveness of ChatGPT's content filtering. The author also mentions in his conclusion that professionals, researchers, and policymakers should try to improve research on the complex security challenges of ChatGPT, and the possible mitigation is to push content filtering, tag data, scan the output, or use artificial intelligence (AI) to filter AI content. The work of the author [12] emphasized the security attacks and vulnerabilities that are associated with the general working modules of chatbots listed in Table 1. The structure of a chatbot involves four main modules. The first module is the client module, which enables users to interact with the chatbot. The second module is the network module, which is responsible for sending messages to the response generation module and the database module. The third module is the response generation module, which generates answers to the input messages initiated by the users. Finally, the fourth module is the database module, which saves all the records generated by the clients and chatbots. Table 2 summarizes the viewpoints of various researchers on chatbots and security issues with their solutions and compares them with our research scheme.

3 Architecture design and application of chatbots system

Artificial intelligence has developed and become popular rapidly in the recent era of technology, like chatbot systems, which are the most popular AI-based technology to support and provide information to end users. It is an intelligent agent that can mimic human communication to interact with users and provide them with services, as well as a set of appropriate answers to their questions and queries [13].Chatbots are an important technological system that can support, enhance, and promote individual learning experiences in education, business, industry, or banking services for customers [14].

The system architecture of chatbots mostly depends on the domain in which they are deployed, but AI chatbots consist of various components, as shown in Fig. 2, such as the user interface, node server, environment, question and answer system, service system, and intelligent automation [15]. It describes that the user's request via message or voice is forwarded through the interface to the Node Server to find an appropriate response. In this scenario, the Node Server interacts with various components; the environment serves as the primary hub for the natural language process that explains context, and it includes several sub-components. 1: The NLP engine is the main part of the environment that interprets what the user says in conversation time and converts it into structured data for further processing; the intent classifier takes the user request, identifies its meaning, and tracks it back to one of the chatbots supporting intents; the entity extractor extracts the main information of the user request. The Dialog Management Agent manages the current context of the dialog between the user and the chatbot to learn more from the user feedback for future user satisfaction. Question and answer is the main part of the chatbot system that interprets users' frequently asked questions to give users an accurate answer based on its knowledge. This part can give the answer based on two common methods: manual training, where the

Table 1 Chabot's vulnerabilities and cyber attacks

Chatbot module	Type of attack	Impacts	Descriptions	Counter measures
Client module [18, 19]	• Fake response • Access control attack	• Data leakage and loss trust • Session hijack and information loss	• Attackers can manipulate chatbots by providing them with false and misleading information, causing them to perform malicious actions • Unauthorized access to chatbots can result in the disclosure of sensitive information	• Response filtering • Regular testing • Strong authentication • Input validation
Network module [20, 21]	• Dos Attacks • MiTM Attack	• Services interruption • Identity theft and data manipulation	• The chatbot interaction is stopped by a denial-of-service attack that floods the server with requests • The adversaries intercepts the communication between two parties and replaces it with malicious content	• Strong Encryption • Load balancing
Response module [22, 23]	• Language model attack • Adversarial test simple • Adversarial responding feedback	• PII theft and trust loss • Wrong information • Reconstruct ML model to perform malicious tasks	• Attackers make malicious attempts to steal information • The input messages are crafted to lead fake response • An attacker can replicate the response generation module's content to execute malicious attack task without modifying the model parameters	• Verification Language model • Hate speech detector (future update) • "Network interpretations and data transformation with Style Transformer."
Database Module [24]	• SQL injection • Knowledge graph attack	• Data deletion, alteration or theft • Loss of accuracy	• An attacker can submit a harmful SQL statement, which can result in gaining unauthorized access to sensitive data • An attacker can manipulate the knowledge graph of a chatbot in order to provide incorrect information	• Input validation • Storage mechanism • Identification detection • Access control • Strong encryption

company provides a list of questions and answers (Q&A) for the chatbot to find the answer from this list and send it back to the user, and automated training, where the company provides all the related documents and then the chatbot trains through machine learning based on the documents and provides the answer to the user query [17].

3.1 Chatbots as a service

Today's connected world has changed the way businesses and consumers communicate based on applications that are commonly known as artificially intelligent applications called chatbots. It is one of the most important forms of communication that can manage the relationship between service providers and customers through a conversational interface such as Facebook, WhatsApp, WeChat, etc., as shown in Fig. 3. Which is integrated using natural language processing [35]. In education, health, industry, banking, and government, chatbots are used to provide real-time communication services to their customers to improve communication and save time and cost because chatbots need to collect and store a large amount of data about the user and the associated conversation [36].

It shows that a user generates a request process through a massaging interface via a speech or text input application and sends it to a natural language parser to convert it into the programming language of the conversation learning engine, or the conversation engine analyzes the user request and sends it to the backend of the system, which is connected to many different databases that provide the response to user requests. Most messaging platforms are supported by third-party chatbots, and they collect and store a large amount of data related to users. Also, they need permission to add more features to enhance the conversation to complete the task on behalf of the user, so the security and privacy of such huge data is a critical issue in the chatbot system; therefore, users and businesses need to be aware of data sharing protection [37].

3.2 Chatbot system security challenges

In the previous section, we explained the architecture of chatbots. Chatbots collect and store a large amount of data by communicating with users over the Internet to provide services, as well as exchanging specific data between the user and chatbot system application during the

Table 2 The comparison of prior work with our developed framework

Chatbot name	Research study topic	Part of chatbot	Limitation	Our developed framework
Deep learning mechanism [25, 26]	Chatbots using Deep Learning	Architecture	• Take more time for training • Costly techniques • No Standard Framework	We developed a comprehensive blockchain enabled federated learning framework with the integration of fully homomorphic encryption and facial recognition algorithm that can improve privacy/security, accuracy, performance and data management or transparency during three different stages such as login access, data security in transmission, and data privacy/security at the backend of chatbots
Health Care chatbot [6, 27]	Design of chatbot using Depp Learning	Architecture	• Data wasn't trained on time • Slow processing • Lack of security framework	
Diagnostic chatbot [28, 29]	Design and development of diagnostic chatbot for supporting primary healthcare system	Application	• Less accuracy the human doctor • Contain small database to store 150 diseases • Weak of machine learning part	
PriBot [30, 31]	PriBot: conversation privacy with Chatbots	Application/ Security	• Risk of malicious users to make the bot useless • The bot is closer to personal privacy assistant than to a smarter searching interface • Users less trust on PriBot about their data usage	
Chatbots [32, 33]	Chatbots: security, privacy, data protection, and social aspects	Security/ Privacy	• Data manipulation on provider side	
Speech review chatbot system [34]	An reinforcement leaning-based speech censorship chatbot system	Security/ Privacy	• The impact of data imbalance and attack detection and aggressive response detection considering multiple rounds of dialogue	

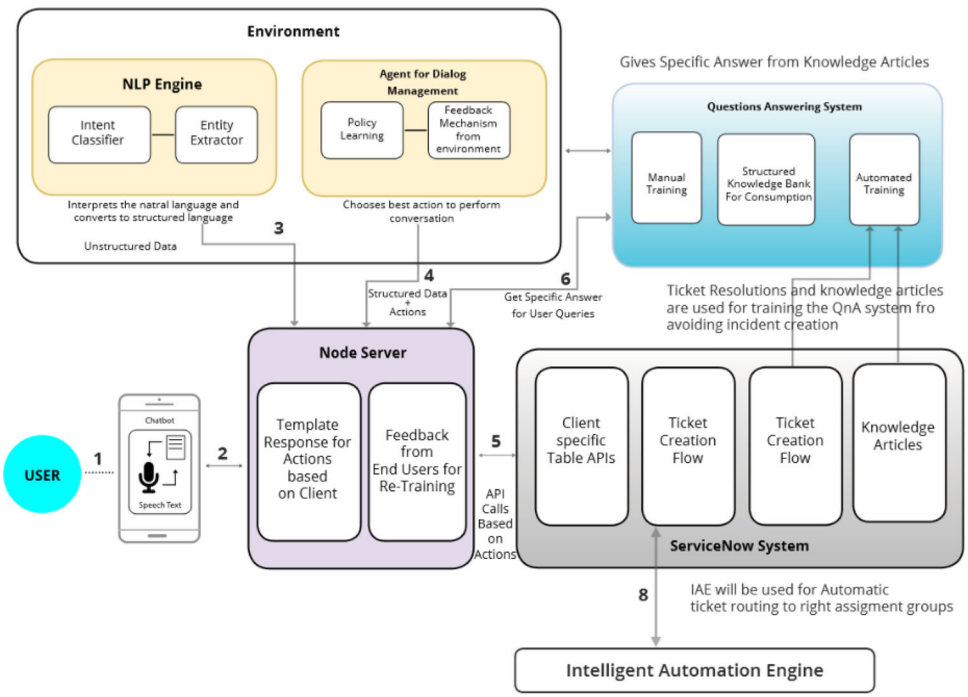


Fig. 2 AI Based conversational chatbot architecture adapted from [16]

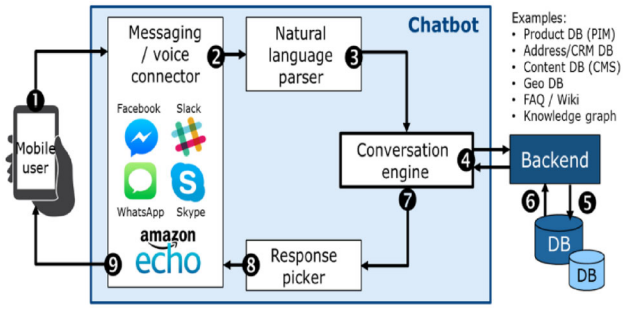


Fig. 3 Chatbot as a service general structure adopted [36]

communication. Since chatbots communicate with people over the Internet, they are vulnerable to cybersecurity and malicious activities. As a result, it is critical to investigate data security and confidentiality during transmission and throughout the system in order to increase users' confidence in the future use of chatbots [38].

3.2.1 Security and privacy challenges

Information security is the customer's willingness to preserve and control their personal identity information (PII), so privacy protection consists of three stages. First, the collection of personal data; second, control over the data; and third, knowledge of laws and regulations related to data processing and privacy [39]. Various application areas use chatbots to process large amounts of data. Therefore, security and privacy are critical issues for chatbot systems, especially for the organization that chatbots use for critical tasks such as financial information, data analytics, etc. Here, we can highlight that secure communication and authentication, data integrity, confidentiality, system availability, transparency, and accountability are security challenges for chatbot systems [40]. First of all, it should be ensured that only authenticated users can communicate with chatbots to query or transmit their sensitive information related to financial issues. Secondly, we must ensure the integrity and confidentiality of the data. The transmitted data can be viewed only by authorized participants and should be protected from any kind of violation or corruption. Third is availability, which protects the system from interruptions and keeps it available to users. Transparency and accountability increase the trustworthiness of the chatbot system. The privacy and security issues arise from the lack of a comprehensive security framework to control the data transferred between the user and the chatbot system [37].

3.2.2 AI based chatbots security threats

With the development of AI technologies, chatbots are able to reproduce human aspects such as conversation through speech and text with high accuracy, like humans. This opens the door to malicious activities and gives a chance to social engineering, man-in-the-middle, and phishing attacks for compromising sensitive information, like hackers using bots as tools to imitate humans to trick them into submitting their payment details [40] Unknowingly trusting chatbot requests, the victim is unaware that the chatbot is under the control of a cybercriminal group, allowing hackers to collect a significant amount of personal data from users through numerous daily conversations with chatbots [41].

3.2.3 Chatbots vulnerabilities

Adversaries exploit chatbot vulnerabilities to compromise the security of the system. These vulnerabilities arise from inadequate code, carelessness in code and infrastructure, unprotected and pornographic human errors, and make the chatbot system vulnerable to cyber-attacks. Many chatbots use cloud computing services, which have their own threats and vulnerabilities, to store and process the data. So, it is the responsibility of the bot manufacturer to ensure all security processes related to chatbots, who are responsible for restoring the architecture and data flow, which should be encrypted both in transit and at rest in the system environment [42].

3.2.4 End-to-End encryption issue in chatbot

This phase performs two functions: first, the transmission of user requests to the responding agent; and second, the transmission of user requests from the responding agent to the database for providing the information. Communication with chatbots is associated with the upper layer of the Open System Interconnection (OSI) model, so we can concentrate on the OSI upper layer (transport-application) [43]. The upper layer of the OSI model also faces security threats. In some cases, adversaries use various tools to launch attacks, such as Man-in-the-Middle (MitM), which intercepts the legal conversation and modifies it with his malicious message or accesses encrypted data to extract sensitive information [44]. Most of the time, denial of service attacks also occur via the communication phase, where the adversary's access to legal conversation is altered with their own information to participate in communication as a legal client for communication disruption with the server [45, 46].

3.3 Data collection and management problems in chatbots

Chatbots process a huge amount of data and store it in the system, whether the data is structured or unstructured, but

data management is a major concern for users because they do not know what the chatbot does with the collected and stored data. How can we share data without compromising its integrity and transparency? These are the two most common privacy questions that make users concerned about the security and protection of their data in the system [47]. Security techniques such as encryption, authentication, and verification can improve the protection of such large amounts of data. Therefore, data scientists have recommended and applied natural language processing (NLP) to address and overcome the security challenges in chatbots because NLP is an artificial intelligence field that can analyse how computers interpret and manage speech and text to collect information according to the concept of human language and provide a suitable mechanism for computer systems to manage human language and perform various related tasks [48]. Despite the advantages of natural language processing, it is also vulnerable to attack by test-time attackers. These vulnerabilities allow attackers to modify input in order to address model flaws. The universal attacker tries to find typically ungrammatical phrases to use as inputs for predicting bugs as well as for training-time attacks, such as poisoning attacks, where an attacker injects some malicious codes into the victim's dataset, as shown in Fig. 4 [49, 50].

Figure 4 explores the idea that adversaries inject malicious code or applications into the dataset while it is training the data model, making a backdoor for adversaries to do more malicious activities in the future for effecting user data and sending them triggered data instead of normal and corrected sentences [51].

3.4 Chatbots computation privacy

Chatbots are artificial intelligence-based computer programs that can process human conversations, both spoken and written, and allow people to interact with them as if they were real people. According to this nature of chatbots, they perform simple tasks, such as answering simple predefined questions, and complicated tasks, such as digital assistants. Natural language processing performs all processes, regardless of chatbot type. On the other hand, computation is the critical part of a chatbot, and its privacy is very important to process the data and answer the users accurately. Therefore, the developers and owners of chatbots should pay attention to improving the protection of data processing by implementing security and privacy technologies and algorithms [52]. We will briefly explain some of them:

3.4.1 Homomorphic encryption

The collection, handling, and processing of sensitive data in chatbots or other AI-powered applications is very important and sensitive for both data and system owners, who must apply strict rules and processing algorithms. Homomorphic encryption is the appropriate and cost-effective solution to ensure confidentiality and prevent unauthorized access to personal and business data [53]. Homomorphic encryption is a collection of encryption algorithms that mimic and implement homomorphic properties, which perform a certain type of operation directly on the encrypted text and provide the same response as on the original message after decryption [54], as depicted in Fig. 5. Homomorphic encryption is a type of encryption scheme in cryptography that allows third parties to perform computations on encrypted data. Therefore, encryption is an essential mechanism for maintaining the confidentiality of sensitive information, while conventional encryption mechanisms cannot perform this process on encrypted data [55].

3.4.2 Secure multi-party computing

This is a technique that allows multiple parties to perform computations together while keeping their input secret. Secure multiparty computation is the solution to various problems in joint computation without compromising data confidentiality, and it ensures data confidentiality, independence, and accuracy for all parties involved in the computation [56, 57]. Secure multiparty computation can perform

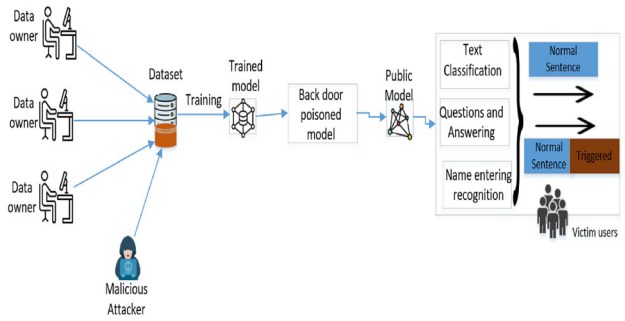


Fig. 4 Overview of poisoning with backdoor attack model training in NLP [51]

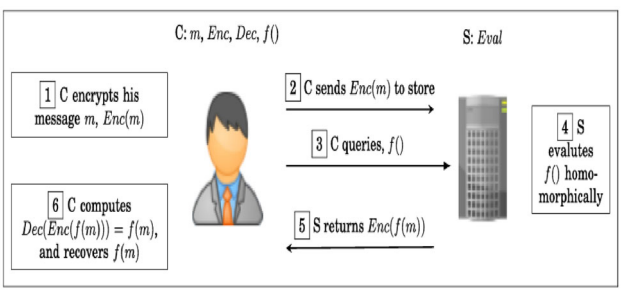


Fig. 5 Homomorphic encryption general scheme [55]

inference on encrypted data but is less suitable for training large language models such as chatbots because it includes a single dataset owned by a single entity, and SMPC leads to increased computation and communication overhead, which has a significant impact on system performance [58].

3.4.3 Federated learning

Artificial intelligence applications such as chatbots collect, store, and process massive amounts of data, which impacts performance, computing power and time, quality of service, and most importantly, privacy and security of user data. Due to privacy and security concerns, most data owners and users are not interested in sharing data with chatbots because chatbots are data-driven applications and collect user data from text, voice, or multimedia conversations [59]. Privacy and security of user data during the training of deep learning models may be violated by shared datasets. As mentioned earlier, there are many approaches to data security and privacy, but all of them require access to user data. In contrast, federated learning is an approach to improving data security and privacy where data is not collected in a central location, but the user's data remains in its own location. Federated learning updates the information through a deep learning model that is trained over the client's private dataset, as shown in Fig. 6. This way, federated learning protects data privacy and security [60, 61].

3.4.4 Blockchain

Blockchain technology employs a public distributed database and ledger for authorized transactions to prevent tampering by partial consensus. The primary idea behind blockchain technology is to provide a secure environment for anyone who communicates to exchange information through a public connection [62, 63]. Blockchain operates on a peer-to-peer network where each node has a permanent and immutable copy of the ledger that keeps track of the entire map and the number of chained blocks using a hash technique [64, 65] Blockchain technology transmits information through a decentralized network of records, restricting unauthorized administrators and allowing limited authorized monitoring of nodes. Unlike traditional centralized systems, which are controlled by a single entity, every computer (node) performs the function based on a peer-to-peer architecture where each node keeps a copy of all transactions [66]. If a new user or node wants to join and create a block of transactions in the system, then various consensus procedures like proof of work and proof of stake are used to validate and provide the agreement of network nodes (miners) about the new adding node and block for transactions [67]. Blockchain employs cryptographic techniques to safeguard transactions and regulate the generation of new units, as depicted in Fig. 7. We use public and private keys to secure transactions and restrict access to the blockchain. Once you upload a block to the blockchain, it becomes extremely difficult to alter or remove the data within it. The blockchain's purpose is to provide data privacy, achieve immutability through cryptographic hashing, and use the consensus method to avoid fraud and provide a tamper-resistant ledger [68, 69].

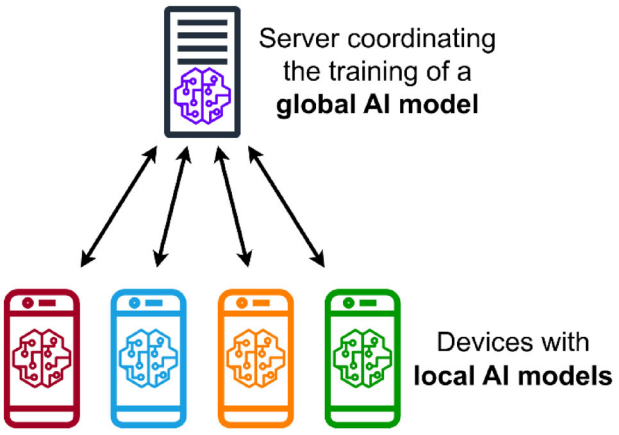


Fig. 6 Federated learning system and training structure [61]

3.5 Addressing the security and privacy challenges in chatbots systems

As mentioned earlier, chatbots are automated computer applications that affect people in various aspects, like providing personal assistance, providing information, offering services, and so on. Whenever a human-like dialog system has been developed, known as chatbots, attention must be paid to potential security and privacy challenges and vulnerabilities that can lead to data leakage and exploitation. There are various types of security and privacy challenges that affect different parts of a chatbot according to its architecture [70]. To better understand, we have divided chatbot architecture into three parts, where

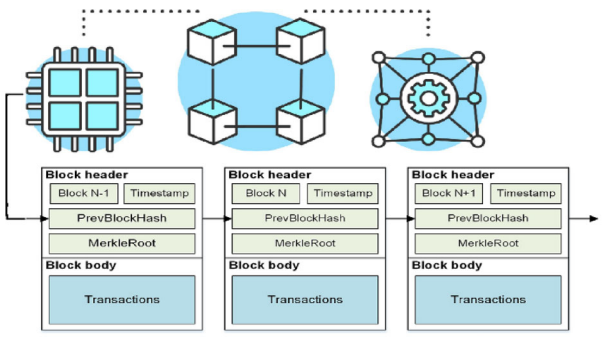


Fig. 7 blockchain and data blocks structure [67]

every part experiences various security and privacy challenges with their own solutions:

3.5.1 Access control and authentication

The widespread use of chatbots increases security and privacy risks, especially for financial service providers, which is harmful for both users and systems. The first layer to improve the security and privacy of the chatbot is controlling login access to prevent illegal logins to the chatbot [32]. Access control can improve data integrity and confidentiality because it strongly restricts unauthorized users access to chatbots [71]. Therefore, to have strong login access control, we recommend a layer combined with username/password and facial recognition because it allows the chatbot to be connected only with authorized and legal users who will also be accountable for their future actions [72].

3.5.2 Data transmission security/privacy

Artificial intelligence-based chatbots communicate with users and exchange data over a public internet connection. End-to-end encryption is a type of communication where only the legal and authorized parties (source and destination) can see, read, and decrypt the message without anyone else. Therefore, it is very important to secure the communication between the user and chatbot to ensure that adversaries cannot access user data during transmission, but only legal users can encrypt and decrypt keys to read the messages [73]. We would like to use a new and secure algorithm (full homomorphic encryption) to improve the security of data during transmission because it allows the process to be performed over encrypted data in contrast to other encryption methods and algorithms.

Traditional encryption algorithms spread the concept of distributed keys, where public and private keys are exchanged over the internet during communication because they need to process decrypted data. In contrast, the full homomorphic encryption algorithm (FHE) allows a complex mathematical operation to be performed on encrypted data during transmission without decryption [74]. FHE consists of three steps for the data encryption process: key generation, encryption, and decryption. The key generation step is randomized to take security parameters as input and

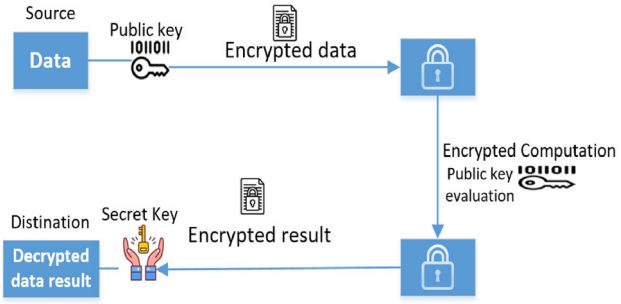


Fig. 8 Homomorphic encryption operational structure [73, 77]

generate public (PK) and secret (SK) keys to encrypt data. The encryption step is also randomized and takes PK and plaintext as input and generates the ciphertext, while decryption needs SK and ciphertext as input and generates plaintext [75], as depicted in Fig. 8. Even though the adversaries have access to data during transmission, they cannot decrypt and read the information, therefore reducing the risk of a man-in-the-middle attack. On the other hand, full homomorphic encryption can support encrypted image processing. For example, a chatbot get the image from the user and forward it to a deep learning model for further processing, and the result is transmitted back to the chatbot to be displayed to the user accordingly [76]. So the implementation of FHE can improve data security and privacy during transmission between the user and chatbot [77].

3.5.3 Data storage and security in backend

As earlier mentioned, chatbots collect a huge amount of data at a single point, so the processing of such huge data is a challenge and a big issue. Chatbots are used in various application domains, so they need to maintain data integrity, confidentiality, transparency, and accountability. On the other hand, users are also concerned about their data and how the chatbot deals with it and shares the data to maintain integrity and transparency [78]. To address these challenges and user concerns, we developed a framework that integrated blockchain-enabled federated learning to improve data security, privacy, and transparency in the backend of chatbots. Blockchain is a distributed ledger technology that maintains a continuously growing ledger on the network to provide a secure transaction with a

timestamp recording mechanism to support data security and privacy [79, 80]. Ledger is a systematic system for data structure that consists of many blocks chained by a cryptographic mechanism. Therefore, it uses chained blocks to store and transmit data with public and private keys to verify and sign the transactions because it is called a blockchain [81]. Ledger technology makes the smart contract and its execution immutable, irreversible, and undesirable. In addition, blockchain provides data persistence, distributed data control, data management, transparency, and accountability. Various fields utilize and deploy blockchain to establish a secure environment for data processing. Recently, it can also be used with natural language processing because blockchain stores and shares the data with other users through a distributed ledger [82]. Blockchain is used to store data as a smart contract in natural language processing to improve storage mechanisms for trustworthiness and prevent SQL injection attacks, which are important for secure computation. In addition, blockchain can store sentiment analysis data as a smart contract in natural language processing to allow users to access it as open source rather than a closed or preparatory source that is cheap and easy for small businesses [83]. Blockchain helps the artificially intelligent system process the data accurately and effectively by using smart contracts to connect different databases. Therefore, it makes data analysis true, and the decision-making process becomes better for the organization. Therefore, blockchain NLP allows users to compose a text through their voice or simply type the text using the keyboard, which is processed by an artificially intelligent model to protect it from language model attacks and malicious injections [84, 85].

3.6 Chatbots vs chatGPT

Chatbots are an integral part of the digital world, revolutionizing the way businesses interact with their customers. Therefore, the technological capabilities of chatbots are improving daily, from rule-based to complex conversational agents driven by artificial intelligence and machine learning algorithms. Although chatbots and ChatGPT are both conversational artificial intelligence technologies that have become increasingly popular in recent years, there are some security challenges, and both are conversational agents that communicate with humans through natural language processing techniques [86, 87]. However, there are some minor differences between them in terms of structure, obtaining information, and generating responses to user queries, as depicted in Table 3. Chatbots are computer programs that are designed to mimic human conversation through text or voice and are an application of artificial intelligence that creates an environment for communication between humans and machines in a conversational manner [33]. Chatbots focus on a specific domain, so they learn from decision trees or data predefined by the owner, as well as from user interactions. AI chatbots use natural language understanding and processing to generate human-like conversations. ChatGPT is a generative, pre-trained language model for chatbots developed by OpenAI. ChatGPT can handle a wide range of topics and domains because it uses deep learning and a transform architecture to train the model through a vast amount of textual data on the web, enabling it to understand and generate human-like conversations [88].

Table 3 Chatbot comparison with ChatGPT

Attributes	AI-Chatbots	ChatGPT
Architecture and design	Machine learning model	Generative pre-trained transformer
Flexibility	Flexibility based on predefined rule	High flexibility
Training	Trained on specialized dataset	Pre-trained on vast internet based data
Conversational depth	Offer depth based on training data	Offer more depth
Personalization	Can make personalized suggestions	Personalization is extended
Learning capabilities	Learning from specific training data	Learn from vast amount training data
Use cases	Task automation, customer support and information retrieval	Creative writing tools, virtual assistance, chat experience
Security and privacy	Vulnerable to data breaches – User data collection – Data leak – Sharing confidential data – Algorithmic bias	Vulnerable to data breaches – spread malicious software – business email compromise – user data collection – sharing confidential data – phishing emails

4 Proposed methodology

This research paper included both theoretical and experimental methods. First, we performed systematic research through various digital libraries to study related topics for carrying out challenges in the structure to shape a conceptual framework. Second, we tested some parts of the proposed framework to evaluate some parts, like its performance, accuracy, and privacy, in the real world.

The proposed framework has been developed to improve the security and privacy of chatbots so they can perform critical functionalities in a secure manner. This framework integrates blockchain-based federated learning and homomorphic encryption with face recognition to enhance the security and privacy of three correlative phases: (1) secure login access; (2) secure data transmission. (3) Data security, privacy, and transparency in the chatbot backend. Mainly, the framework included two main functions, as shown in Fig. 9. Front-end, where the user has direct access to login to perform the required options, and back-end, where data has indirect access for data storage and transactions, but a third party is operating between the front-end and back-end for secure transmission. While Fig. 10 shows the flow diagram of the proposed framework to describe the steps, order, and relationships between the front-end and back-end, Fig. 11 shows the sequence diagram based on the main framework to explain the operation and interaction among users and chatbots.

Federated learning is used at the backend of chatbots to improve the privacy of data by making the system distributed because the data has been kept on the user side and there is no need to transfer it to a central point for storage. Instead of real data, the updated data model exchanges between users and the chatbot system, as we earlier explained. Blockchain technology is used to improve the shortcomings of federated learning security countermeasures in chatbot systems, such as computation time, user access control, and vulnerability to security attacks that leak model parameters and single points of failure.

Blockchain uses hash algorithms for security purposes, immutability, and transparency among the participants in a chain system. Blockchain uses a consensus algorithm to register and validate the user before joining the chatbot to store data in a ledger, as well as a decentralized approach to decrease computation costs and prevent single points of failure.

Whenever the user wants to connect with the chatbot, he or she should be authenticated at the first security layer via

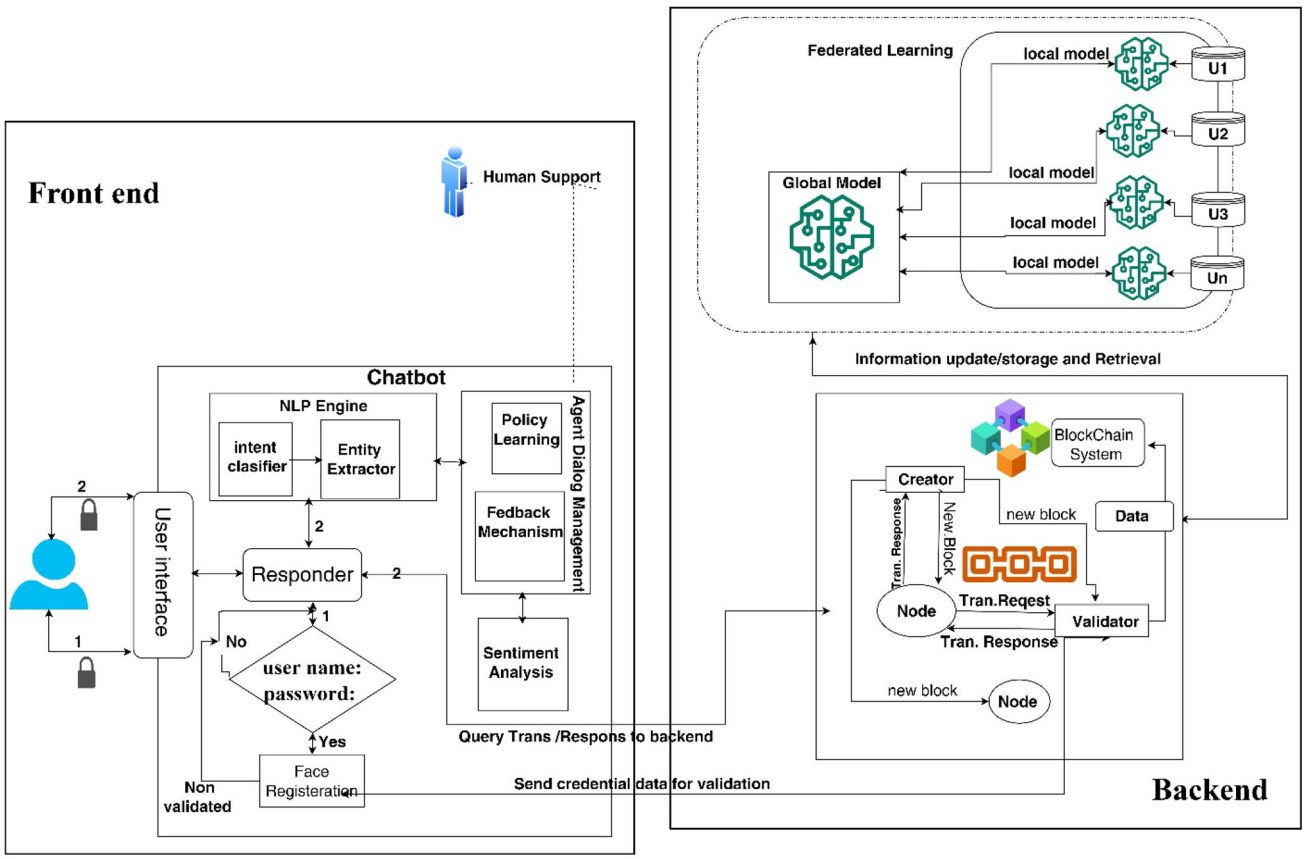


Fig. 9 Main framework to enhance chatbot security and privacy

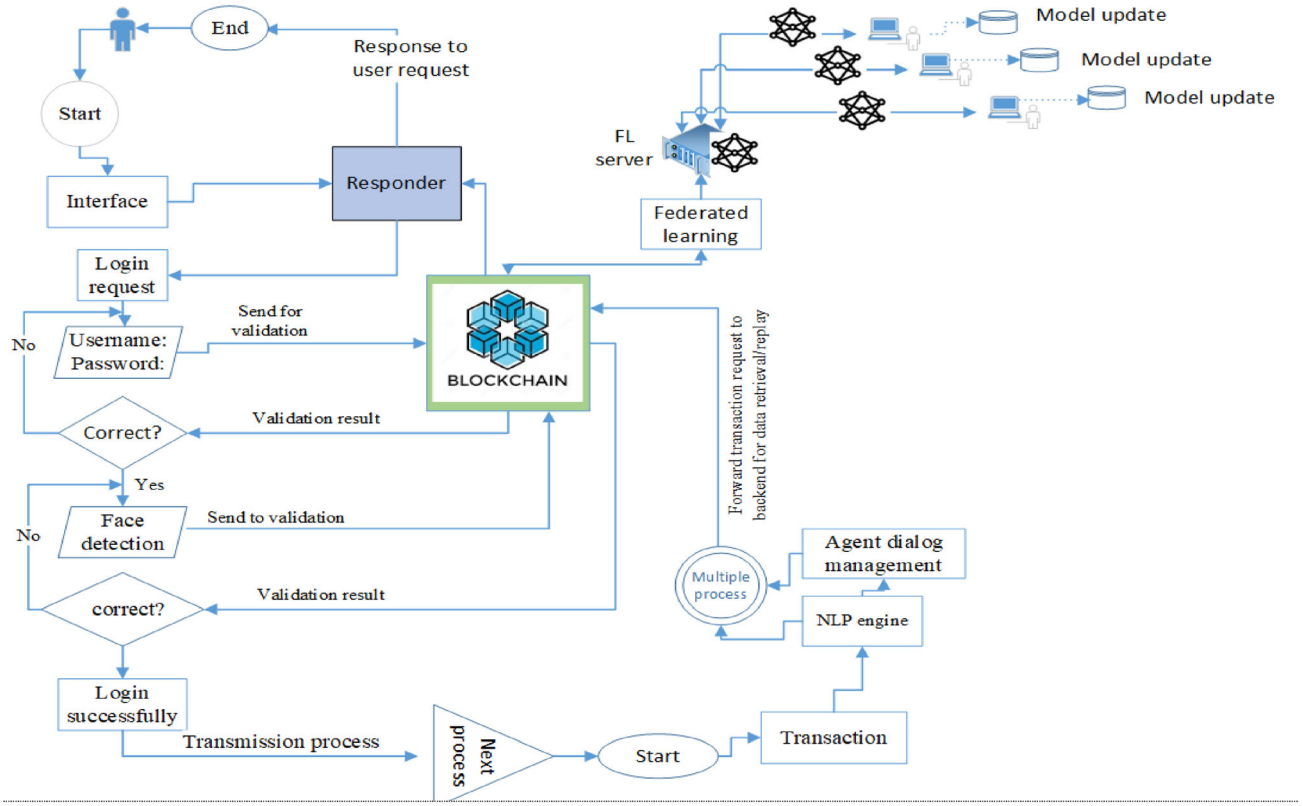


Fig. 10 flow diagram of main framework

common authentication (username, password) and face recognition to restrict the access of illegal users and ensure the chatbot has the authorization of a specific user. The validation of face recognition and common authentication is the responsibility of blockchain in a proposed framework, as you can see in Fig. 9. We used a full homomorphic encryption algorithm to transmit data in a secure and encrypted manner between the user and chatbot system.

4.1 Secure login

This is the first layer of chatbot security that consists of both common authentication (username and password) and face recognition to ensure that the chatbot is connected to an authorized and specific user who has access to sensitive data. The user needs to register his or her face with the chatbot system, which is enabled by blockchain to store and validate face-related data according to the block diagram as depicted in Fig. 12. The sequence diagram in Fig. 13 shows the whole process from start to finish. The registered face will be used for the login process, and a user will be held accountable for their actions in the future. Therefore, it improves data integrity and confidentiality because it restricts unauthorized user access. The proposed framework used the Viola-Jones algorithm for face detection, extracting all features to train the classifier, and we also recommended the convolutional neural network (CNN), which is a type of artificial neural network for picture classification, segmentation, processing, and accuracy, as depicted in Fig. 14. CNN can extract features from higher-layer data to recognize images, and it has the ability to develop internal representations of two dimensions of the image that allow the model to learn the position and scale of the image.

4.2 Secure data transmission

Once the user logs into the chatbot's system, the communication between the user and chatbot is through public internet connections, which raises security and data leakage risks; therefore, it needs to be secure from the access of unauthorized users to understand or alter the data. To do this, we used the full homomorphic encryption algorithm along with the proposed framework for secure data transmission between the user and chatbot system in a harsh environment. The encryption algorithm uses a technique that is suitable for handling the approximate arithmetic operation on floating-point numbers and stands out for its ability to perform an accurate and efficient operation on encrypted datasets without revealing any sensitive data. On

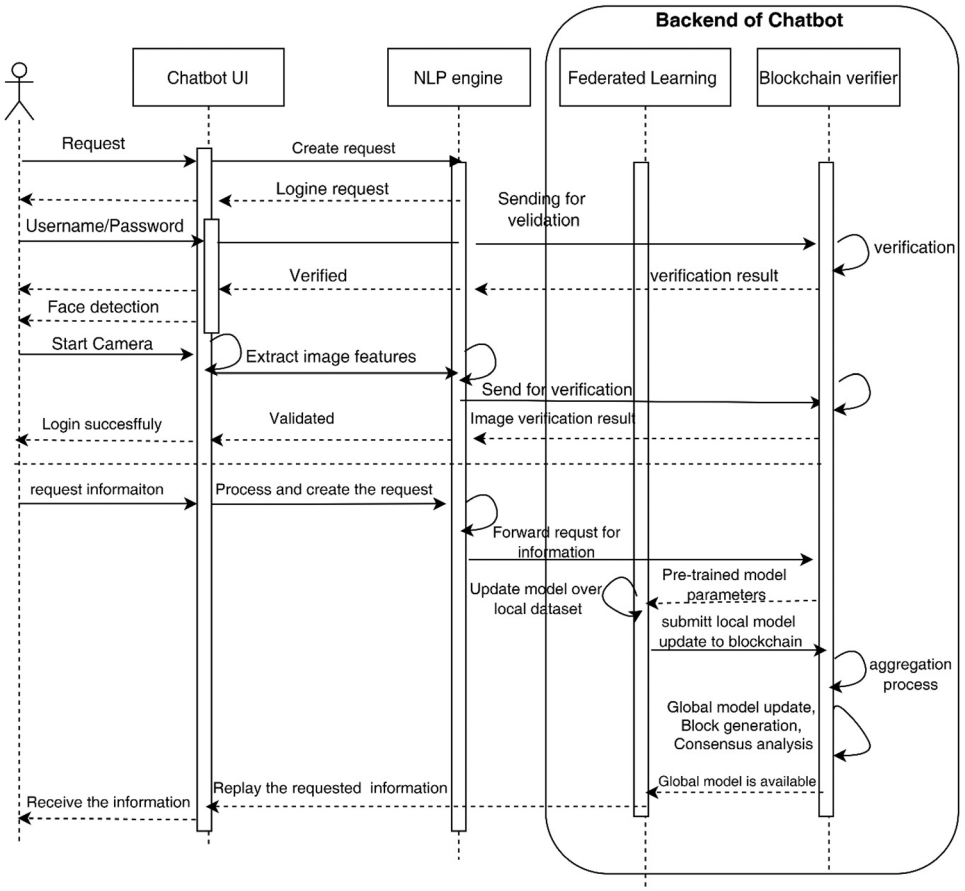


Fig. 11 Sequence diagram for the proposed framework

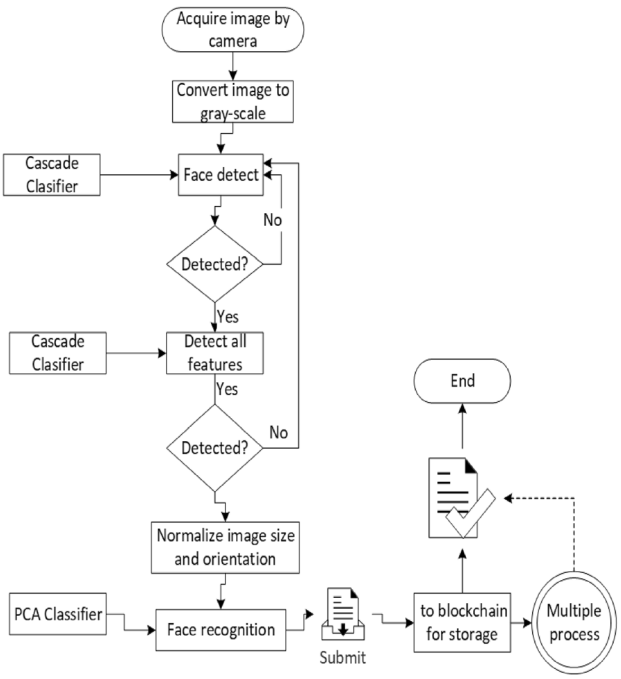
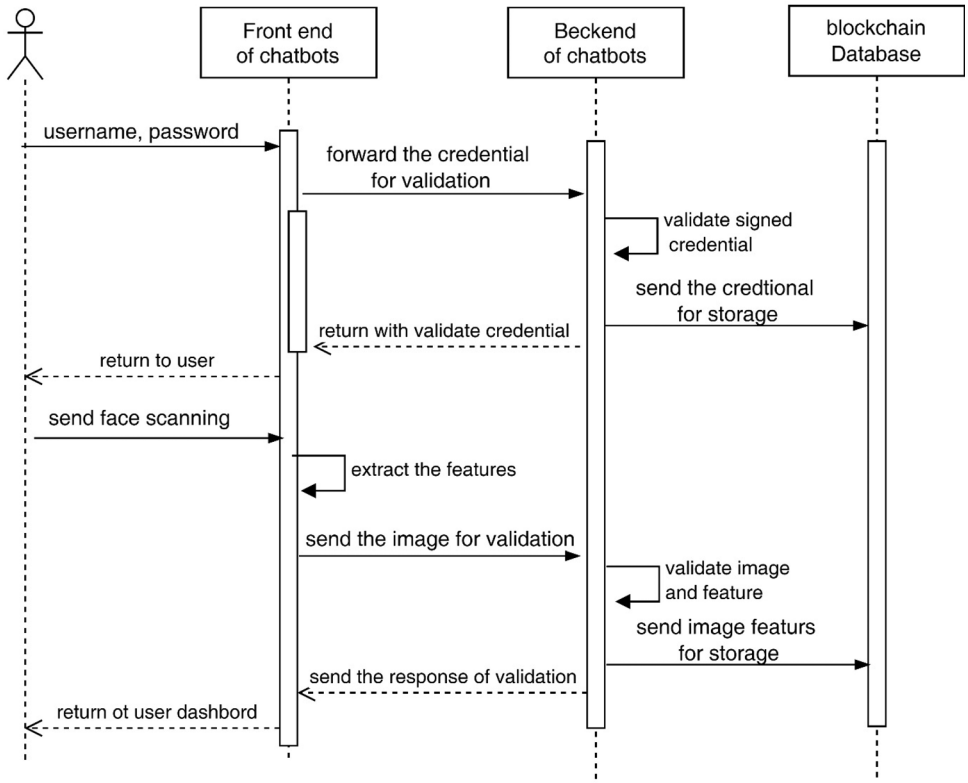


Fig. 12 face recognition block diagram

the other hand, the FHE algorithm is designed to support various arithmetic operations such as addition and multiplication on encrypted data that are the basis for complex computation. It also enables the management and mitigation of the growth of noise efficiently produced by these operations to ensure the result of computation is accurate and expressive after decryption.

The full homomorphic encryption algorithm technique includes the following steps for performing the operation on data during transmission:

- Plain text vector: this represents the plain text (message) that needs to be encrypted.
- Encoding: The plain text vector is transformed into a specific format that is appropriate for conducting homomorphic operations such as polynomials.
- Homomorphic operation: it performs various mathematical operations, such as addition and multiplication, on the encoded data.
- Encryption: this step encrypts the encoded data according to the homomorphic encryption scheme.
- Operation: the encrypted data is sent to chatbots for further processing, where the computations are performed on encrypted data without decrypting or revealing plaintext.



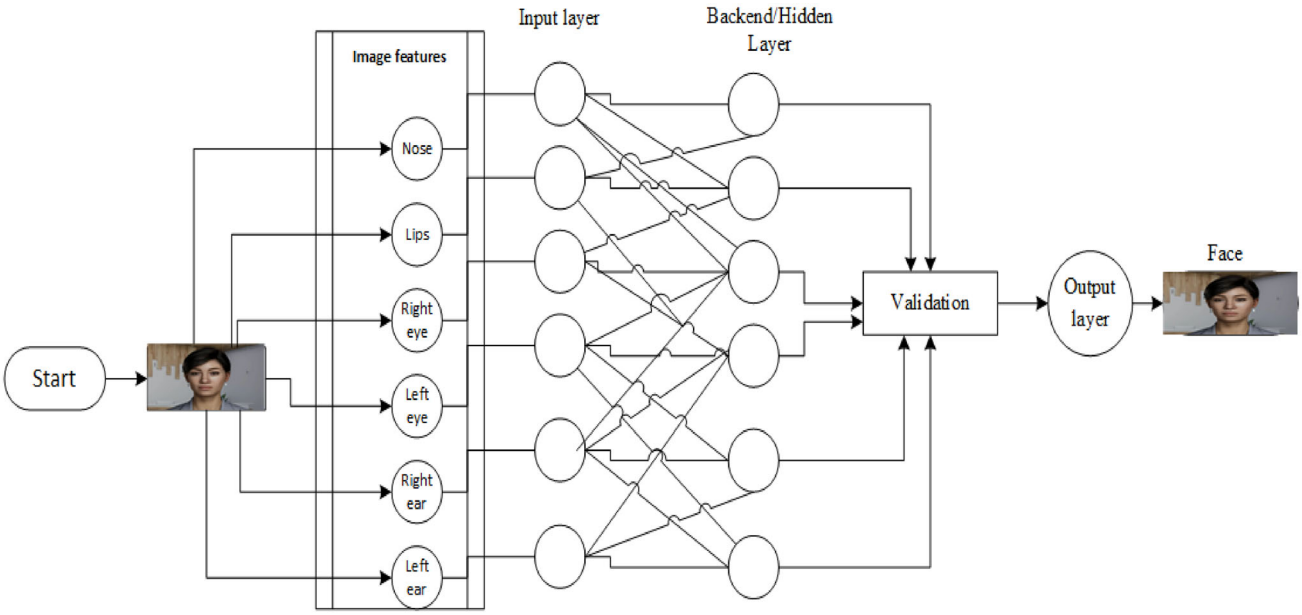


Fig. 13 User with Face registration sequence diagram

Fig. 14 CNN structure for image data processing and classification

- Decrypting: after performing all the above processes and computations, the destination will decrypt the data according to the decryption scheme of the full homomorphic algorithm.
- Decoding: the decryption result is decoding back to plaintext form for reading and understanding.

Algorithm 1 Homomorphic encryption algorithm scheme

- Generate K⟵ keyGen(λ)
- Input A ⟵ data m_0 m_1
- Generate cipher text C_0 and C_1: C_0⟵Enc(K, m_0) C_1⟵ Enc(K, m_1)
- Randomly selected b∈ {0,1} and send C_b to A
- The opponent A access the encryption prediction machine again offer multiple poling the guest b` of b is output.
- If b` = b {1} is output successfully otherwise 0 is output

Data Pre-Processing

- Plaintext m_1 converted to dimension d in vector p.
- Randomly number da – 1⟵ {ar_1, ar_2, …ar_{da-1}} (ari ∈R and I ∈ {1, da – 1}) compute $ar_{da} = m_1 - \sum_{i=1}^{da-1}$ ari . Generate da – 1 dimension vector p (ar_1, ar_2,…ar_{da-1}).

Key Generation

- Key space χ according to security parameter λ and generate non-zero random number set { x_1, x_2, …x_d} Generate d-order matrix $M=M^{-1}$, $m_{i,j} = \chi_i S_\pi(i), j$ and $M^{-1}{}_{i,j} = \chi^{-1}{}_j S^{-1}{}_{\pi(i),j}$ ⟶ K = (M, M^{-1}) Encryption /decryption

Encryption

- Input K ⟵ plain text dataset d = {m_1, m_2,….m_t}. m_1 is convert to d-dimension vector p = (ar_1,cr_1,ar_2 + cr_2,….ar_{da}) + cr_{da}, mr_1,mr_2 ….mr_{dn}, r_1, r_2 … r_{k-1}, $\sum_{i=1}^{da} cri$
- Select d (d-1)/2 non-zero random real integer and construct d-order matrix S= {s1, s2,…st}⟵vector p of the set of d can be generated.
- K= (M, M^{-1}) is using blinding matrix of S in order to get the chipper text C=Ms_t, M-1⟶ m1 and corresponding cipher text matrix set C=(c1, c2, …ct)

Computing

Input Computing function F (.)
Cipher text C={c1, c2, …ct}
Output result= F(c) for addition f (c) = {c1+c2+…ct} and multiplexing F(c)= {c1*c2*…..ct}

Decryption
Input key K= (M, M-1), compute result.

1. Remove blindness of result and compute the plaintext matrix result= M-1 (result)
2. Get addition result $\sum_{i=1}^{da}$(result[i][i] + $resutl[d][d]$
3. Get multiplication $\coprod_{i=da+1}^{da+dm} result\ [i][i]$

4.3 Data security and privacy at the backend of chatbot

Data mining and processing is a massive as well as important part of a chatbot system where the users have indirect access to it for ensuring security and privacy, as its flow diagram depicted in Fig. 10. Whenever the users are increasing their interaction with the chatbot, it collects and processes a huge amount of data centrally, which raises critical security and privacy risks. Therefore, it needs to be improved to inform the users about the data being processed by the chatbot. Therefore, we integrated blockchain-enabled federated learning technology at the backend of the chatbot in the proposed framework, as shown in the Fig. 9 to improve data privacy, transparency, accuracy, and performance of the chatbot system. First, a federated learning mechanism was implemented to change the central processing approach to a distributed processing methodology. Federated learning is able to exchange trained data over a private dataset model to update the information instead of collecting a huge amount of real data in a single central location. The users just need to train the local model parameters, which are determined and published by the federated server over their personal dataset, and send them back to the federated server for aggregation to create a global model. If we consider there are k clients over which the data has been partitioned P_k as a data set of indexes on k clients and f an indicated loss function, $fi(w)$ show the

loss function on weights on i^{th} iteration, while ∇k (local model, local data) is the gradient of loss function with respect to local model parameters. Therefore, on each client $\eta_k = |p_k|$. and local model training is conducted using local dataset as written in Eq. 1.

$$w_t^k = w_{t-1}^k - \eta \nabla w f(w_{t-1}^{(c)}) \tag{1}$$

After the local model update, it will be shared with the server for aggregation. The process is shown in Eq. 2.

$$F_k(w) = \frac{1}{\eta_k} \sum_{i=\rho_k} fi(w) \tag{2}$$

$$gk = F_k(w_t)$$

where w_t shows model weights in communication round t and w_t^k indicates model weights on communication round t on client k, learning rate has shown by η, and p_k shows set of data points on client k where η_k shows number of data points on client k. The Eq. 3 shows that central server aggregates all these gradients to apply the updates.

$$w_{t+1} \leftarrow w_t - \eta \sum_{k=1}^{k} \frac{n_k}{n} gk \tag{3}$$

Despite the advantages of federated learning that prevent the transfer of sensitive user data to a central server, there are still some concerns about data leakage and loss because federated learning also operates centrally and provides a single point of failure that will be full of risk from the perspective of data privacy and have a negative impact on computation, performance, and accuracy. The adversaries may also access model parameters that are trained over the user's private data, or they may attack the central server to leak and access users' related information. Second. We used blockchain to improve the shortcomings of federated learning in the context of privacy and security in the backend of chatbots because blockchain is a more secure technology and it operates in a decentralized manner. A blockchain can be defined as a decentralized database or ledger that contains an ever-expanding number of records called blocks that are interconnected and safeguarded through the use of cryptographic hash techniques. Chatbots keep the logs of conversations between users on a blockchain and provide a temper-proof record of interactions to ensure data integrity. Every block comprises a collection of transactions that have been validated by the blockchain network and includes a hash technique that is generated based on block content to ensure data integrity in the chatbot. It also contains the hash of the previous block to create the chain of blocks to ensure the immutability of the blockchain. The altering of one block would need to change all blocks, which is computationally not practically feasible in a distributed manner. Blockchain is a distributed ledger with cross-network nodes; hence, it doesn't need a central authority, and the transactions are validated by network nodes using cryptographic techniques. Once the transactions are verified, they are stored in a new block that is generated and added through a consensus process in a blockchain network.

The proposed system manages user requests using two smart contracts. The first smart contract (User_Manager) is in charge of user-related actions such as user registration, verification, and other user-related services required for the system to function. The main framework Fig. 9 illustrates the workflow of the User_Manager smart contract. The Chatbot interface validates the input data after the user enters the requested information, ensuring it meets the relevant criteria and limitations. Once the input data is confirmed by the chatbot, it interacts with the data and sends it to a blockchain-based smart contract that invokes a function responsible for user registration. Upon successful completion of the registration procedure, the smart contract alerts the user by sending out an event or returning a confirmation message. The chatbot receives confirmation from the smart contract and notifies the user that the registration procedure was successful. The second smart contract, named Data_Exchange, is developed by an entity with the responsibility of encoding the business logic for data transfers. Once the user has logged in, the chatbot offers the option to engage in data-related transactions and provides guidance throughout the transaction process. The user can initiate data transactions by selecting the relevant options, and the Chatbot verifies the user's request by checking access rights, user identity, and permissions to ensure that the necessary requirements and constraints are met. Once the user's request is verified by the Chatbot, it will communicate with the smart contract (Data_Exchange) to initiate the transaction and execute the functions that handle the processing of data transactions. A smart contract conducts essential verifications and validates transaction parameters to ensure the integrity of the transaction. If the validation is successful, the smart contract proceeds to execute the transaction logic, which may involve accessing, requesting, transferring, or exchanging data.

The blockchain employs the proof-of-authority (PoA) consensus mechanism to authenticate the transactions carried out by smart contracts. The proof-of-authority consensus technique involves the selection of network operators based on trustworthy validators or nodes who possess the authorization to produce new blocks and validate transactions. This selection is determined by their identification and authority inside the network. These

validators are typically referred to as trustworthy entities, such as organizations or persons who have a stake in the network's operation. The validator may possess a pre-established position bestowed by the network administrator, and their selection is contingent upon the reliability and standing of the nodes. Once the Chatbot-initiated transaction is verified by a preset group of authoritative nodes to guarantee its validity and integrity, it is recorded in a newly formed block by one of the authoritative nodes and appended to the blockchain. The chatbot can provide the user with confirmation that the transaction has been successfully uploaded to the blockchain as part of its answer.

Furthermore, we have incorporated a full homomorphic encryption technique into the proposed framework to enhance data privacy and security. As previously stated, full homomorphic encryption is a paradigm that encrypts the entire set of parameters and enables computation to be performed on encrypted data without the need for decryption. Once the processing of model training in federated learning is complete, the data will be sent to a blockchain miner to generate a block and store the information. This ensures that the data remains private throughout the whole process by encrypting it and storing it on the blockchain. Consequently, it improves data privacy and secrecy by ensuring that only authorized persons with the necessary decryption keys may access the original data. In addition, blockchain offers a tamper-resistant platform for sharing data among different parties. By integrating full homomorphic algorithms with the blockchain, data can be securely shared on the blockchain while keeping sensitive information encrypted. This protects the data from unauthorized access, creating a secure environment for collaboration and data exchange within the chatbot. On the other hand, blockchain offers a permanent record where all transactions are openly documented. By using a full homomorphic encryption technique, the authenticity and integrity of encrypted data and computations may be verified by a cryptographic proof kept in the blockchain. It enables auditors to evaluate data integrity operations autonomously, without depending on intermediaries, in order to promote openness and accountability inside the chatbot system. Furthermore, the integration of full homomorphic encryption with blockchain allows for decentralized data processing. This means that computations can be securely performed on encrypted data across a distributed network, resulting in improved scalability and robustness of data processing within a chatbot environment. Additionally, this integration ensures data privacy and security. For instance, from the perspective of a bank system, every user is expected to have an account in a bank system to perform financial activities such as balance inquiries and money transfers that are carried out by a bank system. To do so, we used a private blockchain system because public blockchain operates slowly, is open to all, and incurs significant costs to process and store data in smart- contracts like Ethereum. HyperLedger Fabrics is the most stable and popular private blockchain platform that supports smart contract functionality. This platform offers a novel notion of a channel that allows many blockchains to be controlled within a single network, creating a layer of confidentiality between various organizations to ensure that different activities remain private between different entities. Hyperledger Fabric uses several network entities, like node, creator, and validator, as shown in Fig. 9. Fabric refers to a smart contract as a chain, which transactions can invoke. A node submits a transaction to a validator, which is responsible for checking the validation of an entity for its permission to perform an activity in a ledger encoded during the transaction.

Furthermore, over the technical and security parts, the proposed framework also included sentiment analysis that can evaluate customer interactions with the chatbot. The lexican-based sentiment analysis technique is used to extract the emotional polarity from the chat or text that the user has with the chatbot. It examines all the words and sounds used by the customer during the interaction with the chatbot to understand the user's state, whether he is happy, sad, or angry. We can divide these statuses into three major categories, such as positive, negative, and neutral.

The flow diagram is depicted in Fig. 15, and algorithm 2 shows the entire steps of the sentiment analysis process. In addition, sentiment analysis is a form of cybersecurity perspective that refers to natural language processing and AI-based techniques to analyze users' states, attitudes, and

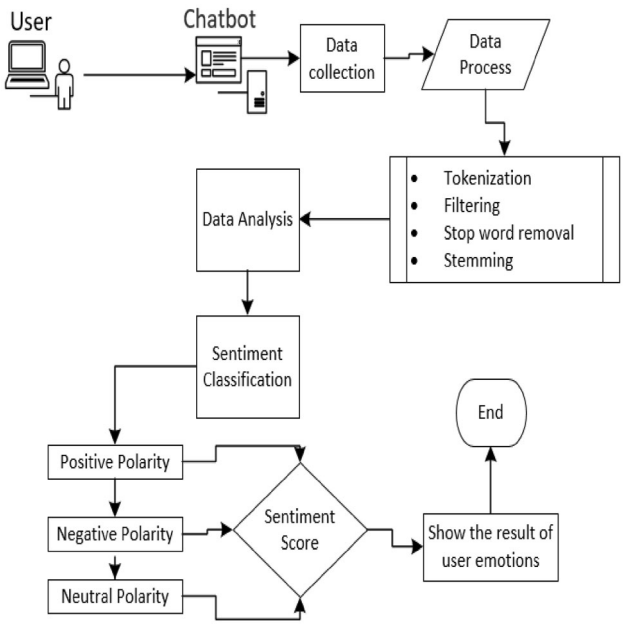


Fig. 15 Sentiment analysis flow diagram

opinions expressed in text and speech related to cybersecurity issues. Therefore, sentiment analysis can identify the areas that need improvement. Gathering information in the form of sentiment analysis that provides insight into how users think about services, specific products, or security issues is therefore key to improving the quality of services and security.

Algorithm 2 Sentiment Analysis Algorithm

INPUT: Text chat τ, the sentiment lexicon L.
OUTPUT: S_{mt} = {P, Ng, or N} and Straight S, where P: Positive
Ng: Negative, N:Neutral
INITIALIZATION: SumPos and SumNeg = 0, where
SumPos: accumulates the polarity of positive tokens $t_{i\text{-}smt}$ in T
SumNeg: accumulates the polarity of negative tokens $t_{i\text{-}smt}$ in T
Begin

```
For each ti ∈ T do
   Search for ti in L
   If ti ∈ Pos-list then
      SumPos ←— SumPos + ti-smt
   Else if ti ∈ Neg-list then
      SumNeg ←— SumNeg + ti-smt
   End if
End for
If SumPos > |SumNeg| then
   Smt = P
   S = SumPos/ (SumPos+SumNeg)
Else if SumPos < |SumNeg| then
   Smt = Neg
   S = SumNeg / (SumPos + SumNeg)
Else
   Smt = N
   S = SumPos/ (SumPos+SumNeg)
End If
```

End

4.4 Implementation environment

We implemented the framework on a high-performance platform that includes an Intel Core i7-8650U CPU at 2.10 GHz and 32 GB of RAM. We deployed certain aspects of the proposed framework on the Windows Server 2019 platform. On this system, we installed a chatbot virtual environment called RASA, which is an open-source framework based on machine learning to create a highly accurate text- and voice-based conversation chatbot environment. The RASA action server provides the environment to write code in Python 3.10 that is used to trigger the action of some parts, such as federated learning, full homomorphic encryption, and hyper-ledger fabric. We also employed a convolutional neural network to create a federated learning model with 15 participants, and the FedSGD techniques are used to allow many devices to train the model without exchanging private data. In addition, the blockchain was developed using the Solidity programming language and deployed using the Truffle framework. We also utilized the Mythril free-source security analysis tools to conduct a security assessment and identify any flaws or potential exploits. The proposed framework needs various datasets; therefore, in this work, we performed the implementation with chatbot-related datasets such as the NewQA dataset for questions and answers that contains over 10,000 human-generated questions and answers. This data set uses the Reading Comprehensive Model (RCM) to understand and interpret new articles and investigate new methods for handling complex questions and large documents. We use the Scheme Guided Dialog (SGD) dataset for dialog interactions. It consists of over 20,000 annotated multi-domain, task-oriented conversations between a human and a virtual assistant. We used the Tufts face dataset for face recognition, which is a large-scale and public benchmark for face recognition. It includes 10,000 images for different countries with an age range of 4–74. The SentiWordNet dataset is used to analyze the sentiment analysis of customers because it is a large lexical database that provides numerical scores representing the positivity, negativity, and neutrality of words. In addition, we used the MNIST dataset for federated learning model training. The full homomorphic encryption algorithm performs the computation or analysis on these datasets while ensuring data privacy.

5 Result and discussion

The framework explained in this paper was proposed for the security of the chatbot system by dividing it into three stages, including login access, secure transmission, and data privacy in the backend of the chatbot. Blockchain-enabled federated learning techniques are used to improve data privacy, transparency, performance, and store data in the backend of the chatbot, as well as process it decentralized without transferring real data to the central point. Blockchain technology utilizes a decentralized and distributed ledger in record management to address scalability issues without significantly affecting performance. The proposed framework only sends model updates or gradients to the blockchain for aggregation instead of raw data because the model training occurs on local devices over their private data; therefore, it significantly reduces the amount of data transmission across the network, which makes bandwidth and storage easy, which are critical factors for scalability. Furthermore, simultaneous training on several nodes efficiently utilizes the network's processing resources, allowing the system to grow by adding more users without increasing overall training time. In addition, the proposed framework uses a full homomorphic encryption algorithm that is designed to support the computation of encrypted data directly without decryption

while maintaining the structure of the plaintext domain to improve transmission performance. It is also suitable for privacy-preserving machine learning and other applications. It requires carefully selecting the parameters to balance the efficiency, security, and precision of the computation to improve performance, as well as permitting the safe outsourcing of computations to untrusted third parties, allowing for scalable and cost-effective data processing without exposing unencrypted data to prospective attackers.

The implementation and tested results of FHE are shown in Fig. 16. It calculates the encryption time according to file size, which is performed on plaintext from 256 to 1792 bits of data by adding 256 bits in each round, which indicates that a fully homomorphic algorithm encrypts more data in less time to improve performance, but its encryption time increased along with the size of plaintext.

On the other hand, Fig. 17 shows the encryption and decryption performance times of a fully homomorphic algorithm according to key size. Here the key sizes are selected as 512, 1024, 1536, 2048, and 2560 bits to achieve 80, 112, 128, 192, and 256 bit security levels. The encryption and decryption times have a direct relationship with key size because of the exponentiation operation, which is increasing exponentially.

We used federated learning, which trains and learns the models from a more diverse set of data that mitigates bias and overfitting as well as collects a wider range of patterns and insights that might not be available in a centralized dataset. Figure 18 shows the comparison of accuracy between federated learning (distributed) and centralized systems. Federated learning has improved computational accuracy (90%), but central system accuracy has decreased with more iteration (75%).

The proposed framework used blockchain-enabled federated learning in the backend of chatbots to store and process the model; therefore, federated learning performs model training directly on a local device's dataset without transferring it to a central location, which reduces the amount of data to be transferred over the network, which leads to low communication bandwidth. Blockchain also allows decentralized model management by storing federated learning models over a distributed network of nodes, which improves the overall performance of chatbot systems. Figure 19 shows the comparison of performance

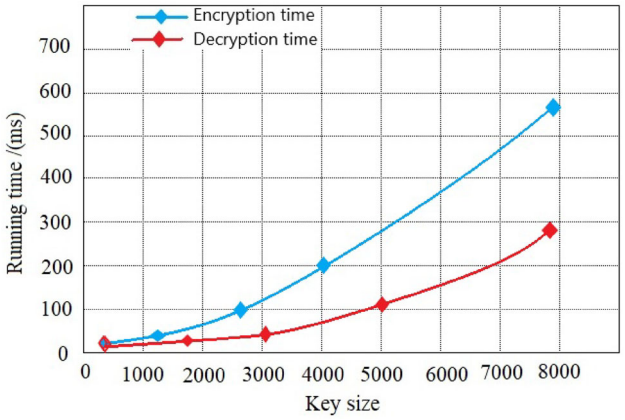


Fig. 17 FHE running encryption/decryption time per key size

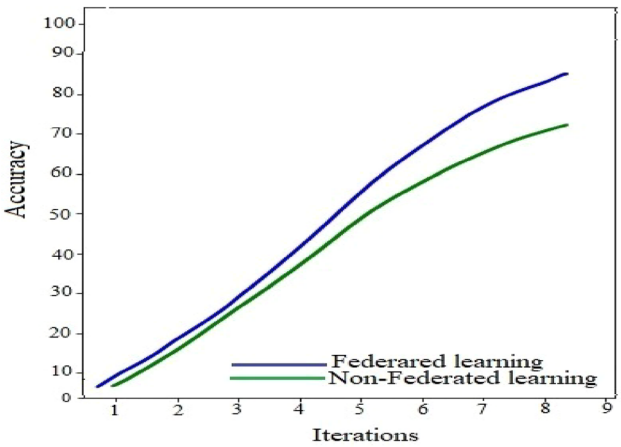


Fig. 18 Accuracy between centralized and distributed (FL)

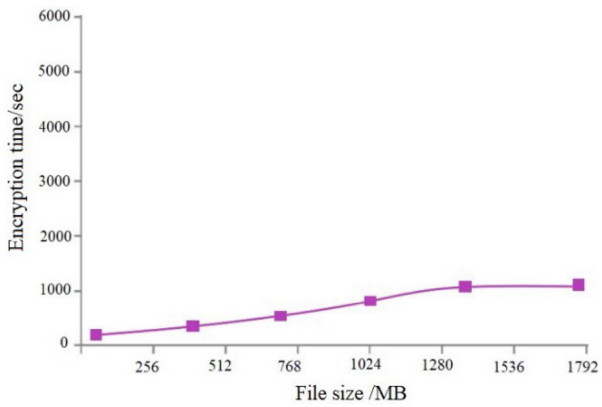


Fig. 16 Fully homomorphic encryption time/file size

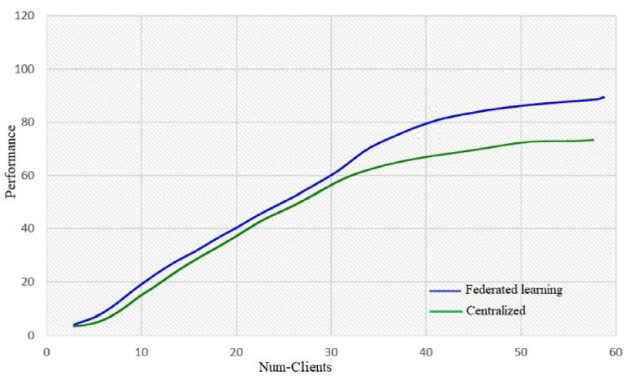


Fig. 19 Performance between centralized and distributed (FL)

between centralized and federated learning (distributed) chatbot systems, where blockchain-enabled federated learning chatbot systems improve performance more than centralized systems.

Blockchain operates decentralized peer-to-peer direct transactions between users, eliminating the need for intermediaries like payment processes or banks; therefore, it reduces transaction costs, prevents single points of failure, and improves the privacy of the users who conduct the transaction via chatbot. On the other hand, blockchain supports smart contracts that perform self-execution on predefined terms and conditions. Smart contracts can automate and enforce financial transactions through chatbots, reducing the need for manual intervention and boosting transaction processing efficiency. Figure 20 shows the improvement of the transaction process with high speed in our scheme from the perspective of the user's creation and transaction.

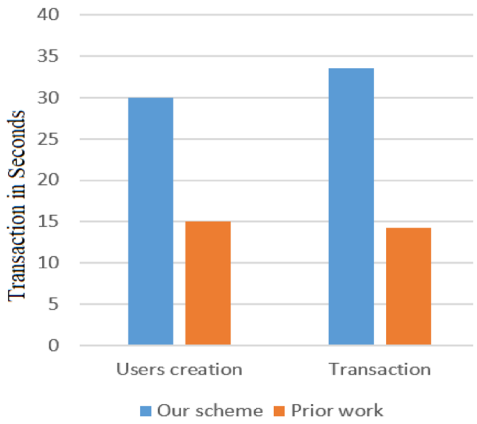


Fig. 20 Comparison of transactions and user creation

We can summarize our research findings in the context of some attributes, impacts, and specific countermeasures, as described in Table 4.

6 Conclusion and future work

This research is concentrated on how to improve the privacy and security of chatbot systems, including three stages: login access, data transmission, and data at the backend. We used a face recognition system over the normal authentication (username, password) method to secure and control unauthorized logins. The user enrolls their facial features like landmarks, contours, and textures, and the extracted data is then processed and securely stored in a blockchain. Whenever the user attempts to login to the chatbot the next time, they will be asked to verify their identity by using common authentication. After that, the chatbot captures an image of the user's face using the device's camera and transfers the image feature to the backend of the chatbots for comparison with enrolled data stored in the blockchain for validation to prevent attacks

Table 4 our research summarization according to attributes and its countermeasures

Attributes	Impacts	Our scheme countermeasures
Access control	Data leakage and lose trust	Strong authentication and identity validation
Data transmission (DoS and MiTM issues)	Services interruption and data leakage during transmission	Data encryption during transmission (FHE) and Blockchain to prevent DoS attacks
Data management	Malicious data injection during model training to send wrong information to users by chatbot	Blockchain has the capability to validate all input data, strong encryption mechanism through consensus and hash mechanism
Accuracy	Inaccurate response form chatbot can lead to frustration and dissatisfaction among users, and chatbot will lose its trust	enabled decentralized and collaborated model training also data aggregation to ensure that sensitive user data remains encrypted and protected throughout the training process that improve the accuracy
Performance	Slow response times, overloaded on server, delay in processing	Enabled decentralized data storage, aggregation and model training cross multiple nodes without relying on central server. It prevents from single point of failure, and FHE also encrypts more data files and perform computation over encrypted data without decryption to save process time and improve performance
Scalability	Resource constraint, database limitation can hinder chatbot ability to handle peak loads and scale dynamically	Improved chatbot scalability due to decentralizing data aggregation and model training, parallelizing computation, distributed task cross multiple nodes
Security and privacy	Data breaches, leading unauthorized access, malicious attacks	Decentralized data storage, FHE encryption, smart contract for governance and immutable record of data

related to login access. A full homomorphic encryption algorithm has been integrated to securely transfer the data between the user and chatbot to prevent malicious attacks like DoS and MiTM attacks. Because it performs the process over encrypted data without decryption, user input remains confidential and unreadable to any party. Blockchain-enabled federated learning has been used in the backend of chatbots. It enables decentralized data processing and management by storing a federated learning model over a distributed network of nodes to improve the overall performance and transaction process of the chatbot system because this system reduces the amount of data transferred through the network, which leads to low communication bandwidth. On the other hand, transactions on a blockchain are transparent and immutable, meaning they can't be altered or deleted after recording. Therefore, this technology improves trust by providing a tamper-proof record of all transactions and reducing the risk of fraud in the chatbot system. Blockchain also enables fast, low-cost, borderless payments for financial chatbots, simplifying cross-border transactions. For future direction, we recommend laying out the chatbot, especially the financial chatbot, based on beyond-generation mobile technology, which is envisioned to revolutionize chatbots for delivering different services in the future.

Acknowledgements This work was supported by the National Key Research and Development Program of China (No.2023YFC3303803 and 2023YFC3303800), State Key Laboratory of Public Big Data of Guizhou University (No.PBD2023-24), CCF NSFocus Kunpeng Foundation (No.CCF-NSFocus2023012) , Fundamental Research Funds for the Central Universities (No. FRF-AT-19-009Z and FRF-AT-20-11) from the Ministry of Education of China.

Author contributions All authors contributed equally to the conceptualization and design of the solution for mentioned challenges. Data collection and analysis performed by Nasir Ahmad Jalali and Professor Chen Hongsong provide supervision as well as reviewed the paper for quality improvement.

Funding National Key Research and Development Program of China, 2023YFC3303803

Data availability All data sets analysed during this study to support the results of the article are publicly available.

Declarations

Competing interests The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Asbjorn Folstad, Cecilie Bertiussen Nordheim, & Cato Alexander Bjorkli, What makes users trust a chatbot for customer services? an exploratory interview study, in *The proceeding fof the Fifth International conference on Internet Science*, Oslo, Norway (2018)
2. Lorenz Cuno Klopfenstein, Saverio Delpriori, Silvia Malatini, Aessandro Bogliolo, The Rise of Bots: A Survey of Conversational Interfaces, patterns, and Paradiams, in *DIS17: Proceedings of the 2017 Conference on Designing Interactiv System* (2017)
3. Gentsch, P.: Conversational AI: How (Chat)Bots Will Reshape the Digital Experience. In: *AI in Marketing Sales and Services: How Marketers without a Data Science Degree can user AI, Big Data and Bots*, Frankfurt, pp. 81–95. SpringerLink, Germany (2019)
4. Daniel Adiwardana, Minh-Thang Luong, David R. So, et al, Towards a human-like open-domain chatbot, arXiv:2001.09977v3 [cs.CL] *27 Feb 2020* (2020)
5. Okuda, T., Shoda, S.: AI-Based chatbot service for financial industry. FUJITSU Scientific and Technical Journal **54**(2), 4–8 (2018)
6. Milind H Shah, mahesh Panchal, Theoretical evaluation of securing modules for educational chatbot, in *Proceedings of the Sixth International Conference on Intelligent Computing and Control System (ICICCS)* (2022)
7. Kuhail, M.A., Alturki, N., Alramlawi, S., Alhejori, K.: Interacting with educational chatbots: a systematic review. Educ. Inf. Technol. **28**, 973–1018 (2023)
8. Asim Mohammed Eltahir, hussam Abdullah, Jan Platos, and Vaclav Snasel, Review of chatbot security systems, in *2022 26th International Conference on Circuits, Systems, Communications and Computers (CSCC)* (2022)
9. Rahime Belen Saglam, Jason R.C., Nurse, and Duncan Hodges Privacy Concerns in Chatbot Interactions: When to Trust and When to Worry, in *23rd HCI International Conference, HCII 2021*, Swithzerland (2021)
10. Nazar Waheed, Muhammad Ikram, Saad Sajid Hashmi, et al, An empirical assessment of security and privacy risks of web-based chatbots, *WISE international Journal,* pp. 1–25 (2022)
11. Erik Derner, and Kristina Batistic, Beyond the safguards: exploring the security risks of chatGPT, arXiv:2305.08005v1 (2023)
12. Hoy, M.B.: Alexa, siri, cartana, and more: an introduction to voice assistants. Med. Ref. Serv. Q. **37**(1), 81–88 (2018)
13. Fabio Clarizia, Francesco Colace, Marco Lombardi, et al, Chatbot: An education support system for students, in *International Symposium on Cyberspace Safety and Security* (2018)
14. Okonkwo, C.W., Ade-Ibijola, A.: Chatbots applications in education: a systematic review. Comptuers and Education: Artificial Intelligence **2**, 100033 (2021)
15. Huang, X.: Chatbot: design, architecture, and applications. Univesity of Pennsylvania, School of Engineering and Applied Science, Pennsylvania (2021)
16. Dasagrandhi, Understanding The conversational chatbot architecture, V-Soft consulting, 2550 Eastpoint Pkwy Suite 300 Luisville, Ky 40223 (2020)
17. Haristiani, Nuria, Artificial Intelligence (AI) Chatbots as Language Learning Medium: An inquiry, in *International Conference on Education, Science and Technology 2019*, Gothenburg, Sweden (2019)
18. Jing Xu, Da Ju, Margaret Li, et al, Bot-Adversarial Dialogue for Safe Conversational Agents, in *Proceedings of the 2021 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies*, New York. (2021)
19. Domna Bilika, Nikoletta Michopoulou, et al, "Hello me, meet the real me: audio deepfake attacks on voice assistants, arXiv:2302.10328v1 [cs.CR] (2023)
20. Chung, H., Lorga, M., Voas, J., Lee, S.: Alexa, can i trust you? IEEE Xplore **9**, 100–105 (2017)

21. Krishna Gondaliya, Sergey Butakov, and Pavol Zavarsky, SLA as Mechanism to Manage Risks Related to Chatbot Services, in *2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity)* (2020)
22. Cheng Qian, Haode Qi, Gengyu Wang, et al, Distinguish Sens from Nonsens:Out-of-Scope Detection for Virtual Assistants, arXiv:2301.06544v1 [cs.CL] *16 Jan 2023* (2023)
23. Zheng, Y., Feng, XiaoYi, Xia, Z., et al.: Why adversarial reprogramming works, when it fails, and how to tell the difference. Inf. Sci. **632**, 130–143 (2023)
24. Stefano Bistarelli, Francesco Santini, and Carlo Taticchi (2020) A Chatbot Extended with Argumentation, in *5th workshop on Advances In Argumentation In Artificial Intelligence*, Milano, Italy
25. Kadayan, N.S., Dave, A., Vinit, K.: Chatbot using deep learning. J. Emerg. Technol. Innov. Res. **6**(2), 137–141 (2019)
26. Wube, H.E., Esubalew, S.Z., et al.: Text-based chatbot in financial sector: a systematic literature review. Data Science in Finance and Economics **2**(3), 209–236 (2022)
27. Nivila, A., Sujitha, S., Prithika, N., Gnana Prakash, V.: Design of chatbots using deep learning. International Research Journal of Engineering and Technology (IRJET) **9**(20), 1105–1110 (2022)
28. Kidwai, B., Nadesh, R.K.: Design and development of diagnostic chatbot for supporting primary health care system. Procedia Computer Science **167**, 75–84 (2020)
29. Aishwarya Surani, and Sanchari Das, Understanding privacy and security postures of healthcare chatbots, *Association for Computing Machinery (ACM)* (2022)
30. Hamza Harkous, Kassem Fawaz, Kang G. Shin, Karl Aberer, PriBots: conversational privacy with chatbots, in *Workshop on the Future of Privacy Indicators, at the Twelfth Symposium on Usable Privacy and Security (SOUPS)*, Denver, Colorado (2016)
31. Md. Saiful Islam Bhuiyan, Abdur Razzak, Md Sadek Ferdous, et al, BONIK: A Blockchain Empowered Chatbot for Financial Transactions, in *Conference on Trust, Security and Privacy in Computing and Communications* (2020)
32. Martin Hasal, Jana Nowakova, et al, Chatbots: Security, Privacy, Data protection, and Social aspects, *Wiley*, pp. 1–13 (2021)
33. Lee, M., Frank, L., IJsseelsteijin, W.: Brokerbot: a cryptocurrency chatbot in the social-technical gap of trust. Computer Supported Cooperative Work (CSCW) **30**, 79–117 (2021)
34. Cai, S., Han, D., Li, D., Zheng, Z., Crespi, N.: An reinforcement learning-based speach censorship chatbot system. J. Supercomput. **78**, 8751–8773 (2022)
35. Cordero, J., Barba-Guaman, L., Guaman, F.: Use of chatbots for customer serivces in MSMEs. Applied Computing and Informatics (2022). https://doi.org/10.1108/ACI-06-2022-0148
36. Zumstein, D., Hundertmark, S.: Chatbots-and interactive technology for personalized communication, transactions and services. IADIS International Journal on WWW/Internet **15**(1), 96–109 (2018)
37. Jide Edu, Cliona Mulligan, and Fabio Pierazzi, Exploring the security and privacy risk of chatbots in messaging services, in *Proceeding of the 22nd ACM Internet Measurement Conference (IMC'22)*, France (2022)
38. Sen-Tarng Lai, Fang-Yie Leu, and Jeng-Wei Lin, A banking chatbot security control procedure for protecting user data security and privacy, in *13th International Conference on Broadband and Wireless Computing Communication and Applications (BWCCA-2018)*, Switzerland (2019)
39. de Cosmo, L.M., Piper, L., de Vittorio, A.: The role of attitude toward chatbots and privacy concern on the relationship between attitude toward mobile advertising and behavioral intent to use chatbots. Ital. J. Mark. **2021**, 83–102 (2021)
40. Josip Bozic, & Franz Wotawa, Security testing for chatbots, in *In IFIP interanation Conference on Testing Software and System (ICTSS)*, Switzerland (2018)
41. Jide Edu, Cliona Mulligan, Fabio Pierazzi, et al, Exploring the Security and Privacy Risks of Chatbots in Messaging Services, in *In Proceedings of the 22nd ACM Internet Measurement Conference (IMC '22)*, New York, USA (2022)
42. Koien, M.A., Geir, M.: Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security **4**, 65–88 (2015)
43. Kar, R., Haldar, R.: Applying chatbots to the internet of things: opportunities and architectureal elements. International Journal of Advanced Comptuer Science and Application (IJACSA) (2018). https://doi.org/10.14569/IJACSA.2016.071119
44. Mallik, A., Ahsan, A., et al.: Man-in-the-middle attack: understanding in simple words. International Jouranl of Data and Network Science **3**, 77–92 (2019)
45. Laura Feinstein, Dan Schnackenberg, et al, Statistical approaches to ddos attack detections and response, in *Proceedings of the DARPA Information Survivability Conference and Exposition* (2013)
46. Yameen Ajani, Krish Mangalorkar, Yohann Nadar, et al, Homomorphic encryption for Secure Conversation with AI bots over cloud to prevent Social Engineering attacks, *International Journal of Engineering Research and Applications,* pp. 21–27 (2021)
47. Pathrabe, Trupti V. Survey on security issues of growing technology: big data, in *National Conference on Latest Trends in Networking and Cyber Security* (2017)
48. Jung, S.: Semantic vector learning for natural language understanding. Science Direct **56**, 130–145 (2019)
49. Eric Wallace, Shi Feng, et al, Universal adversarial triggers for attacking and analyzing NLP, in *Proceedings of the 2019 Conferene on Empirical Methods in natural Language Processing*, Hong Kong, China (2019)
50. Tian, J., Wang, B., Guo, R., et al.: Advarsarial attacks and defenses for deep-learning-based unmanned aerial vehicles. IEEE Internet Things J. **9**(22), 22399–22409 (2022)
51. Tiam, J., Wang, B., Wang, Z., et al.: Joint adversarial example and false data injections attacks for state estimation in power systems. IEEE Transactions on Cybernetics **52**(12), 13699–13713 (2022)
52. Yang, J., Chen, Y.-L., Por, L.Y., Chin Soon, Ku.: A systematic literature review of information security in chatbots. Appl. Sci. **13**, 2–18 (2023)
53. Michael Lahzi Gaid, Mohamed Waleed Fakhr, and Gamal Ibrahim Selim, Secure Translation Using Fully Homomorphic Encryption and Sequence-to-Sequence Neural Network, in *28th International Conference on Computer Theory and Application (ICCTA)*, Alexandria: Egypt (2018)
54. Jalali, N.A., Chen, H.: Federated learning security and privacy-preserving algorithm and experimental research under internet of things critical infrastracture. Tsinghua Science and Technology **29**(2), 400–414 (2023)
55. Acar, A., Aksu, H., Uluagac, A.S.: A survey on homomorphic encryption scheme: theory and implementation. ACM Comput. Surv. **51**(4), 79 (2018)
56. Romanov, D.: Secure multi-party computation for supply chain collaboration. University of Technology, Delft (2021)
57. Jalali, N.A., Chen, H.: Security issues and solutions in federated learning under IoT critical infrastructure. Wireless Personal Communication **129**, 475–500 (2022)
58. Sebastian, Glorin (2022) Privacy and data protection in ChatGPT and other AI Chatbots: strategies for securing user information, Georgia Instituite of Technology

59. Jalali, N.A., Chen, H.: Security issues and solutions in federated learning under IoT critical infrastructure. Wirel. Pers. Commun. **129**, 475–500 (2023)
60. Kairouz, P., Mcmahan, H.B., Avent, B., et al.: Advanced and open problems in federated learning. Found. Trends Mach. Learn. **14**(1–2), 1–210 (2021)
61. Renhao, Lu., Zhang, W., Li, Q., et al.: Adaptive asynchronous federated learning. Futur. Gener. Comput. Syst. **152**, 193–206 (2023)
62. Zibin Zheng, Shaoan Xie, Hongning Dai, et al, An overview of blockchain technology: architecture. Consensus, and Future Trends, in *2017 IEEE 6th International Congress on Big Data* (2017)
63. Lukman Adewale Ajao, Simon Tooswem Apeh, Blockchain integration with machine learning for securing fog computing vulnerability in smart city sustainability, in *1st International Conference on Advanced Innovations in Smart Cities (ICAISC)*, Jeddah: Saudi Arabia (2023)
64. Khalid, U., Asim, M., Baker, T., et al.: A decentralized lightweight blockchain-based authentication mechanism for IoT system. Liverpool John Moores University (Cluster Computing) **23**, 2067–2087 (2020)
65. Mohan, V.S., Sankaran, S., Nanda, P., Achuthan, K.: Enabling secure lightweight mobile Narrowband Internet of Things (NB-IoT) applications using blockchain. Journal of Network and Computer Application **219**, 103723 (2023)
66. Ngabo, D., Wang, D., Iwendi, C., Anajemba, J.H., Ajao, L.A., Biamba, C.: Blockchain-based security mechanism for the medical data at fog computing architecture of internet of things. Electronics **11**(17), 2110 (2021)
67. Guang Chen, Bing Xu, Manli Lu, and Nian-Shing Chen, Exploring Blockchain Technology and Its Potential Applications for Education, *Springer Link,* vol. 5, no. 1 (2018)
68. Kshetri, N.: Blockchain's roles in strngthening cybersecurity and protecting privacy. Elsevier (Telecommunications Policy) **41**(10), 1027–1038 (2017)
69. Lukman Adewale Ajao, Buhari Ugbede Umar, Daniel Oluwaseun Olajide, Sanjay Misra, Blockchain Applications in the Smart Era, in *Application of Crypto-Blockchain Technology for Securing Electronic Voting System*, A. K. T. Sanjay Misra, Ed., EAI/ Springer Innovations in Communication and Computing Springer: Cham (2022)
70. Winson Ye, & Qun Li, Chatbot security and privacy in the age of personal assistants, in *2020 IEEE/ACM Symoposium on Edge Computing (SEC)* (2020)
71. Voege, P., AbuSulayman, I.I.M., Ouda, A.: Smart chatbot for user authentication. Electronics **11**, 4016 (2022)
72. Aneesa, M.P., Sabina, N., Meera, K.: Face recognition using CNN: a systematic review. Int. J. Eng. Res. Technol. **11**(6), 182–185 (2022)
73. Endeley, R.E.: End-to-End encryption in messaging services and national security-case of whatsapp messanger. J. Inf. Secur. **9**, 95–99 (2018)
74. Gentry, G.: A fully homomorphic encryption scheme. Stanford University, California (2009)
75. Blatt, M., Gusev, A., et al.: Secure large-scale genome-wide association studies using homomorphic encryption. Proc. Natl. Acad. Sci. U.S.A. **117**(21), 11608–11613 (2020)
76. Bani Salamah, J.N., Salameh, J.B., Altarawneh, M.: Evaluation of cloud computing platform for image processing algorithm. J. Eng. Sci. Technol. **14**(4), 2345–2358 (2019)
77. Ajani, Y., Mangalorkar, K., et al.: Homomorphic encryption technology for securing data in cloud computing: a survey. Int. J. Comput. Appl. **160**(6), 1–5 (2017)
78. Singh, S.K., Yang, L.T., Park, J.H.: FusionFedBlock: fusion of blockchain and federated learning to preserve privacy in industry 5.0. Inforamtion Fusion **90**, 233–240 (2023)
79. Mazzei, D., Baldi, G., Fantoni, G., et al.: A blockchain tokenizer for industrial IoT trustless application. Futur. Gener. Comput. Syst. **105**, 432–445 (2020)
80. Chenhao, Xu., Youyang, Qu., Xiang, Y., Gao, L.: Asynchronous federated learning on heterogeneous devices: a survey. Comput. Sci. Rev. **50**, 100595 (2023)
81. Ferdous, S., Chowdhury, F., Alssafi, M.O.: In search of self-sovereign identity leveraging blockchain technology. IEEE Access **7**, 103059–103079 (2019)
82. Abylay Satybaldy, & Mariusz Nowostawski, Reveiw of Technical for Privacy-Preserving Blockchain Systems, in *Proceeding of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure*, Taipei, Taiwan (2020)
83. Bharimalla, P.K., Choudhury, H., et al.: A blokchain and NLP based electroni health record system: Indian subcontinent context. Informatica **45**, 605–616 (2021)
84. Kun Shao, Yu., Zhang, J.Y., Li, X., Liu, H.: The triggers that open the NLP model backdoors are hidden in the advaresial samples. Comptuer & Security **118**, 102730 (2022)
85. Kaur, R., Gabrijelcic, D., Klobucar, T.: Artificial intelligence for cybersecurity: literature review and future research direction. Information Fusion **97**, 101804 (2023)
86. Chaka, C.: Geerative AI Chatbots-ChatGPT versus YouChat versus Chatsonic: use case of selected areas of applied English language studies. International Journal of Learning, Teaching and Eduactioanl Research **22**(6), 1–19 (2023)
87. AI-HawawrehAljuhaniJararweh, M.A.Y.: Chatgpt for cybersecurity: practical applications, challenges and future directions. Clust. Comput. **26**, 3421–3436 (2023)
88. Kocon, J., Cichecki, I., Kaszyca, O., et al.: ChatGPT : jack of all trades, master of none. Information Fusion **99**, 101861 (2023)

Nasir Ahmad Jalali received his B.S Degree from Kabul Education University and his Master degree (MS) from Kabul University cooperated by Tallinn University, Estonia in 2016. Currently he is pursuing his PhD degree from the School of Computer and Communication Engineering at University of Science and Technology Beijing (USTB), China from 2020. Mr. Jalali has been an associate professor at Ghazni University, Ghazni, Afghanistan since 2012. His research interest includes network security, information security, federated learning, machine learning, big data, chatbots security and IoT privacy-preserving. Mr. Jalali has published four academic papers and he is the author of two books entitled MPLS-

VPN Impacts on VoIP-QoS and Framework Development for Higher Education Information Security in Afghanistan respectively.

Chen Hongsong received his Ph.d Degree of Computer Science in Harbin Institute of Technology in 2006. He is a professor in University of Science and Technology Beijing (USTB), China from 2008. He was a visiting scholar in Department of Computer Science of Purdue University from 2013–2014. He is a high-level member of China Computer Federation. He is an IEEE member now. His research interests include Artificial Intelligence and information securitywireless network and pervasive computing, trust computing. He got the excellent young academic paper award in USTB in 2009.He has published more than 60 academic papers and 5 books.