IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 1 February 2024, accepted 11 April 2024, date of publication 25 April 2024, date of current version 3 May 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3393487

RESEARCH ARTICLE

Blockchain-Based Caller-ID Authentication (BBCA): A Novel Solution to Prevent Spoofing Attacks in VoIP/SIP Networks

I. MELIH TAS[1] AND SELCUK BAKTIR[2], (Senior Member, IEEE)
[1]Department of Computer Engineering, Faculty of Engineering and Natural Sciences, Bahçeşehir University, 34353 İstanbul, Turkey
[2]College of Engineering and Technology, American University of the Middle East, Egaila 54200, Kuwait

Corresponding author: Selcuk Baktir (selcuk.baktir@aum.edu.kw)

ABSTRACT Voice over Internet Protocol (VoIP) networks are vulnerable to caller-ID (caller-identification) spoofing attacks due to the open nature of Session Initiation Protocol (SIP) signaling. Caller-ID spoofing is a critical security threat in modern telecommunication systems, allowing attackers to impersonate legitimate callers and gain access to sensitive information. While these attacks pose a significant threat to the telecom and financial industries, the existing solutions are limited to only closed-circuit options for subscribers of the same service provider. In this paper, we present a novel blockchain-based solution to effectively prevent caller-ID spoofing attacks in real time. Our approach employs a low-latency consensus algorithm to manage and verify end-to-end the caller-ID information of Internet Service Providers (ISPs) and institutions. We propose a two-step verification process, in which the accuracy and integrity of Automatic Number Identification (ANI) information is verified at different stages of the call. The proposed solution initiates a renewal of the ISP registration on every caller-ID change, making it unaffected by unusual situations such as roaming, the use of an IP-PBX (Internet Protocol Private Branch Exchange), or the use of a VPN (Virtual Private Network). We also discuss the proposed solution's feasibility and potential deployment issues, including its integration into existing RFC (Request for Comments) efforts and the necessary regulations for service providers to demonstrate compliance. Furthermore, we address future research directions, such as handling complex call scenarios such as call forwarding and teleconference calls. Our approach not only improves the security of telecommunication systems but also provides an efficient and scalable solution to prevent caller-ID spoofing attacks.

INDEX TERMS Authentication, blockchain, caller authentication, caller-ID spoofing, identity spoofing, PBFT, practical byzantine fault tolerance, robocall, session initiation protocol, SIP, voice over IP, VoIP.

I. INTRODUCTION

Caller-ID (caller-identification) spoofing is a growing concern in the realm of telecommunications, as it allows attackers to manipulate the caller-ID information displayed on the recipient's device. In this section, we provide an overview of the methods used to perform caller-ID spoofing, the challenges in detecting and preventing these attacks, and the reasons for the increase in caller-ID spoofing incidents. We also discuss the limitations of the current solutions and the need for a more comprehensive approach.

The associate editor coordinating the review of this manuscript and approving it for publication was Giuseppe Destefanis.

A. BACKGROUND: UNDERSTANDING CALLER-ID SPOOFING TECHNIQUES

The most common method of performing caller-ID spoofing attacks is through the use of VoIP telephony. The VoIP technology allows for voice communications to be sent over

the Internet, rather than over a fixed phone line or cellular network. This convenience has led to the proliferation of VoIP providers that offer customers the ability to customize their caller-ID information via their services [1].

Caller-ID spoofing can also be performed using ready-made web or mobile applications. These applications typically allow users to enter the phone number they wish to call, followed by the phone number they want to display as the caller-ID. The call is then sent through a VoIP provider, which changes the outbound caller-ID information before connecting to the desired phone number.

In addition to ready-made applications, specialized services such as SpoofCard [2] can be used to generate low-volume spoofed calls. Automated call generators, such as Mr.SIP [3] or SIPp [4], can be used to generate large volumes of calls, each with individual, random, or carefully selected calling numbers. Customized scenarios can also be produced using a VoIP provider connected to an Asterisk system [5], [6], [7], [8].

It is worth noting that the feasibility of caller-ID spoofing varies between countries and regions. In countries with strict regulations, such as the United States (US) and the United Kingdom (UK), initiating a call with a spoofed caller-ID is extremely difficult [1], [9]. However, in countries with less regulation or oversight, such as developing countries, caller-ID spoofing is relatively simple. The ability to spoof caller-ID information and terminate calls in any country regardless of regulations highlights the need for a comprehensive solution that can effectively address this issue. In addition, the ease with which caller-ID spoofing can be performed using ready-made web or mobile applications, specialized services, and automated call generators, further emphasizes the need for a solution that can address this issue at a global scale.

B. CHALLENGES IN DETECTING AND PREVENTING CALLER-ID SPOOFING

The detection and prevention of caller-ID spoofing is a challenging task, as the telephone network is a complex system of carriers and solution providers, making it difficult for most providers and government agencies to track down and prosecute those who engage in this illegal activity. Additionally, distinguishing between a legitimate and a spoofed caller-ID can be difficult, as many VoIP servers now allow their users to choose their own caller-ID, and operators may not perform authentication checks prior to connecting a call. This issue mirrors problems encountered with IP spoofing and underscores the need for service providers to implement egress filtering, further complicating the detection and prevention of spoofing activities.

To prevent caller-ID spoofing on an individual level, a variety of smartphone applications are available that can validate caller-ID information. However, this approach is not sufficient, as it relies on the real caller having installed the application [10]. In the banking sector, where access to customers' accounts is granted through verification of the bank or credit card number associated with the caller-ID, additional measures such as secret questions are employed to identify potential spoofing. However, not all banks take this risk into account and continue to rely on the service provider's assurance of caller-ID spoofing prohibition [11].

The difficulty in detecting and preventing caller-ID spoofing, coupled with the increasing prevalence of this attack, highlights the need for a comprehensive solution that can effectively address this issue on a global scale. The use of a low-latency blockchain-based consensus algorithm to manage and verify end-to-end caller-ID information, as proposed in this study, presents a novel and promising approach to addressing this problem [12], [13].

C. REASONS FOR THE INCREASE IN CALLER-ID SPOOFING INCIDENTS

The increase in caller-ID spoofing incidents can be attributed to the widespread adoption of VoIP telephony. VoIP technology makes caller-ID spoofing cheaper, more flexible, and more easily accessible to a global audience. Additionally, the nature of VoIP, which transfers only the audio signal and not the associated metadata, makes it significantly easier to carry out caller-ID spoofing than other forms of fraud such as email phishing.

As security measures have improved in other areas, such as email filtering, education on various forms of fraud, declining usage of insecure credit cards, and advancements in authentication technologies such as mobile authentication and two-factor authentication (2FA), other forms of fraud have become more difficult to carry out. However, users continue to rely on the telephone system and tend to trust the caller-ID information displayed to them, making them more susceptible to caller-ID spoofing attacks [14], [15].

D. THE DEADLOCK OF HAVING NO VALID SOLUTION

The lack of a comprehensive solution for caller-ID spoofing can be attributed to several factors. Phone operators and service providers have been reluctant to offer caller-ID spoofing blocking solutions to their customers, due to a combination of opportunity cost, regulations, technical difficulties, and investment cost [16].

1) **Opportunity Cost:** The economics of unwanted spam calls play a role in the reluctance to address the problem. Telemarketers and spammers can make money by making phone calls at a low cost and with minimal risk. Telephone companies also profit from connecting these calls to receivers, and service providers have little motivation to prohibit these calls unless their competitors offer a superior option.
2) **Regulations:** Governments heavily regulate telecommunications to promote competition and justice, but this also slows innovation and reduces the risks that service providers are willing to take, as it imposes more obligations on them.

3) **Technical Difficulties:** The complexity of the telephone network, made up of many different operators and service providers, makes it difficult to eliminate spoofed calls without cooperation.
4) **Investment Cost:** The cost of addressing the caller-ID spoofing problem is high, and phone companies are unwilling to invest in solving it since it is not a profit-generating or cost-effective position for them.

Attempts by governments, such as the US, to control telemarketing and robocall issues through new laws and regulations, and partnerships between telecom firms and third-party providers, can only improve domestic issues. However, this is a global issue, and these remedies will be insufficient for calls coming from unregulated nations or difficult-to-follow VoIP sources. It is unlikely that current methods will effectively address the problem globally. This will require governments worldwide to implement similar laws and penalties, and perform necessary oversight, as part of a coordinated effort [14], [17]. The lack of a comprehensive solution to the caller-ID spoofing problem highlights the need for a global approach that can effectively address this issue, taking into consideration the economic, regulatory, technical, and investment challenges.

E. MAIN CONTRIBUTIONS OF THIS STUDY

The main focus of this work is to address the caller-ID spoofing problem, which has been a major headache for the telecom and banking industries worldwide. Despite the numerous attempts to solve this problem, there is currently no universally accepted approach to prevent it. The VoIP and its underlying Session Initiation Protocol (SIP) make it possible to implement caller-ID spoofing and also make it very difficult to prevent it [18]. Existing solutions are primarily closed-loop solutions that are only available under the same service provider and not suitable for real-world applications.

In this work, we make the following main contributions:

1) Building upon prior attempts in the literature to use blockchain technology for combating caller-ID fraud, such as the system proposed in [19], we make a novel contribution by developing a unique blockchain-based caller-ID registration and call flow control mechanism that is deployed in the cloud. Our method stands out by effectively managing and verifying end-to-end the caller-ID information of ISPs and institutions, which results in real-time mitigation of caller-ID fraud attacks. Moreover, our system expands on previous solutions by verifying the caller-ID and ANI information not only at the initiation of a call, but also upon receipt, tracking which ISP it originates from, and monitoring any hop changes throughout the call.
2) We present a detailed technical analysis of existing defensive methods against caller-ID spoofing, and compare them to our solution, highlighting the benefits of our approach. We believe that our solution could potentially contribute to existing RFC (Request for Comments) efforts, or lead to a new RFC, on caller-ID spoofing mitigation.
3) We propose a modified version of the Practical Byzantine Fault Tolerance (PBFT) algorithm as the consensus algorithm used in our solution [20]. This modification allows for low latency and real-time performance by implementing a two-phase commit protocol, where a small subset of nodes called ''verifiers'' are responsible for quickly reaching a consensus on the validity of a caller-ID. The verifiers are selected based on their reputation and past performance in the network.
4) We provide a detailed discussion of the proposed solution's feasibility and potential deployment issues, including its integration into existing RFC efforts and the necessary regulations for service providers to demonstrate compliance.
5) We address future research directions, such as handling complex call scenarios such as call forwarding and teleconference calls. Our approach not only improves the security of telecommunication systems but also provides an efficient and scalable solution to prevent caller-ID spoofing attacks while being able to handle complex call scenarios. Additionally, we discuss the potential challenges and considerations for large-scale deployment and integration into existing systems and regulations.

Overall, our proposed blockchain-based caller-ID authentication (BBCA) scheme offers a novel and effective approach to solving the caller-ID spoofing problem in the telecommunication industry.

The use of a low-latency blockchain-based consensus algorithm to manage and verify end-to-end caller-ID information, as proposed in this study, presents a novel and promising approach to addressing the issue of caller-ID spoofing. In the following sections, we detail the design and implementation of our proposed solution, as well as its evaluation against existing methods in the literature, standards and in practice.

The paper continues as follows. In Section II, we give an overview of the commonly used techniques to mitigate caller-ID spoofing. Furthermore, we give an overview of the existing caller-ID spoofing prevention techniques from the academic and standards perspectives. In Section III, we introduce our blockchain-based solution against caller-ID spoofing and detail its capabilities. Finally, we discuss some future research directions in Section IV and we give our conclusions in Section V.

II. LITERATURE REVIEW

A. COMMONLY USED COUNTERMEASURES AGAINST CALLER-ID SPOOFING

There are several well-known and commonly used mechanisms that are utilized by existing prevention systems against caller-ID spoofing attacks [1]. We classify these into three categories as follows:

TABLE 1. Comparison of commonly used countermeasures against caller-ID spoofing.

Countermeasure	Effectiveness	Ease of Implementation	User Impact
Managed Blacklist	Moderate	Moderate	High
Do Not Originate	Moderate	Difficult	Low
Knowledge-Based Authentication	High	Difficult	High
Voice Biometrics	High	Difficult	High
Mobile Phone	High	Difficult	Low
Digital Signature	High	Very Difficult	Low
Blockchain-based Caller-ID Authentication	High	Difficult	Low

1) **Managed Blacklist:** The majority of telecom vendors such as Cisco Systems, Alcatel-Lucent, and Siemens use an active blacklist. This list determines whether incoming calls should be blocked or allowed, and gets updated as a result of user feedback. However, this strategy has its limitations as it is not effective for new calls coming from numbers that are not on the list or calls that use random fake dial numbers. Furthermore, managing and distributing a blacklist is difficult, risky, and susceptible to manipulation. Infrastructure entities need to be modified to support a blacklist. Additionally, the number of entries in the blacklist and whitelist would affect latency.
2) **Do Not Originate (DNO):** Service providers block a call to their network that is coming from an invalid source number or from a source number that has never been assigned to a person. When calls are made in an irregular pattern, it is assumed that the number is invalid. These standards can be adopted more aggressively due to the impact of the caller-ID spoofing problem. However, there may be large gaps in the coverage of these techniques due to calls that traverse a legacy network. Managing and distributing a blacklist is difficult. All allocated source numbers should be known by solution providers globally. This solution is prone to false positives and is simple to circumvent by using a caller-ID that has already been allocated.
3) **Proprietary Authentication:** There are several methods for validating a call, such as Knowledge-Based Authentication (KBA), Voice Biometrics, Mobile Phone, and Digital Signature.
Knowledge-Based Authentication: It is a typical practice in financial call centers to identify and verify a caller by asking questions that only the caller should know the answer to, but it is inconvenient for customers and requires businesses to employ costly call centers.
Voice Biometrics: It is a well-known method of authenticating the caller's identity using active and passive voice analysis, but it is costly and susceptible to noise, call quality, and other variables [21], [22].
Mobile: The use of a mobile phone for authentication is only beneficial for specialized use cases, such as mobile or specific service providers, as it can easily be bypassed by impersonating the User-Agent information on the originating side [22].
Digital Signature: It is a solution in which every user has a public/private cryptographic key pair associated with their phone number. This approach enables digital signature-based authentication to be used during phone calls [23]. However, key management and performance are significant issues with this approach. Additionally, it requires a trusted and distributed infrastructure which is costly to implement.

In summary, while these commonly known countermeasures against caller-ID spoofing have their advantages and disadvantages, none of them are fully capable of solving the problem on a global scale. It is important to note that implementing any of these solutions in isolation may not be sufficient to protect against caller-ID spoofing attacks. Additionally, these solutions are also not flexible to adapt to new technologies and changing regulations. In Section III, we present a comprehensive solution that will address these limitations.

Table 1 compares the commonly used countermeasures against caller-ID spoofing in terms of their effectiveness in preventing spoofing attacks, ease of implementation, and impact on user experience.

TABLE 2. Comparison of academic solutions for caller-ID spoofing prevention.

Study	Approach	Authentication	Validation	Anti-Spoofing	Shortcoming / Drawback
[24]	*Phone authentication using verified protocols*	High	High	Medium	Inadequate for spoofed calls via VoIP
[25]	*Telephony PKI, cryptographic*	High	High	Medium	Inefficient in terms of timing performance
[26]	*Elliptic curve cryptography*	High	High	Medium	Inadequate for spoofed calls via VoIP, inefficient in terms of performance
[29]	*Machine learning*	Medium	Medium	Low	Inadequate for spoofed calls via VoIP, false positive alarms
[30]	*Password-based authentication*	High	High	Low	Inadequate for spoofed calls via VoIP
[10]	*End-to-end validation*	High	High	Medium	Inadequate for spoofed calls via VoIP
[31]	*Network-assisted*	High	High	Medium	Limited to 4G networks
[23] and [32]	*Self-controlled security, one-time key*	Medium	Medium	Medium	Depends on network infrastructure, inadequate for spoofed calls via VoIP
[33] and [34]	*Standardized caller-ID authentication*	High	High	Medium	Limited to SS7 telecommunication
[19]	*Blockchain-based identity authentication*	High	High	High	Long authentication process, not suitable for real-time communication
This study	*Blockchain-based caller-ID authentication*	High	High	High	Implementation difficulty due to regulatory compliance and integration

B. EVALUATION OF ACADEMIC SOLUTIONS FOR CALLER-ID SPOOFING

Several academic studies have proposed various approaches to address caller-ID spoofing in telephony networks.

In [24], the authors proposed a mechanism called AuthentiCall, which used a robust authentication method to verify caller-ID information before a call is answered. This allowed users to dismiss calls that claimed a specific caller-ID but were unable or unwilling to provide verification.

In [25], the authors proposed an authentication protocol called AuthLoop, which allowed end-to-end validation of caller-ID information for all telephony networks. The proposed protocol was based on the use of a telephony Public Key Infrastructure (PKI) and some cryptographic approaches. It was later enhanced with the RFC 8224.

In [26], the authors integrated elliptic curve cryptography [27], [28] into SIP and showed that the resulting performance was significantly better than the one where the Rivest-Shamir-Adleman (RSA) cryptosystem was used. They suggested that their work could be considered as a first step in standardizing the use of elliptic curves in identity management for SIP. However, the proposed method is inadequate for a spoofed call that originates via VoIP as it is not possible to check the accuracy of the data at the time the VoIP call originated and whether the caller-ID information has been changed in the call flow. In addition, due to the computationally expensive cryptographic workload, the proposed solution is not efficient in terms of performance.

In [29], the authors proposed a machine learning-based approach to predict malicious calls. However, this approach would not work for every type of phone call and may create false positive alarms when spoofed calls originate via VoIP.

In [30], a self-enforcing method was proposed to perform password-based authentication in SIP without involving a trusted third party. However, this solution can only be applied by end-users at their initiative and would not be effective in preventing caller-ID spoofing attacks.

In [10], an end-to-end caller-ID verification scheme was proposed that leverages the features of the existing phone network infrastructure. However, this solution can easily be bypassed via VoIP.

In [31], a network-assisted caller-ID authentication solution was proposed to validate the caller-ID information used during call setup, but is only applicable to 4G (Fourth-Generation) networks and not able to prevent caller-ID spoofing initiated via VoIP.

In [32] and [23], the authors proposed a self-controlled security and one-time key issue mechanism as a solution to prevent data leakage. However, this approach relies on a statistical model for the first verification unit, called the advisory system, to assist in identifying unknown calls. While this method may have some efficacy, it is not a comprehensive solution as it is dependent on the specific network infrastructure and may be easily circumvented by exploiting the flexibility of VoIP networks.

In [33] and [34], the authors proposed a standardized caller-ID authentication scheme for SS7 (Signaling System 7) telecommunication, but it is not useful for preventing caller-ID spoofing attacks that originate via VoIP.

In [21], the authors proposed an end-to-end, dual identity authentication mechanism using data transmission technology and voice-print recognition to verify the identity of the caller. However, the proposed mechanism did not explicitly address the issue of caller-ID spoofing, indicating the need for further research to develop more robust mechanisms to prevent this type of fraud.

In [22], the authors presented a mobile fingerprint-based authentication system for call centers. The proposed system involved integrating a fingerprint scanner feature on smartphones and using it to verify the identities of callers before providing any services. However, the proposed approach is limited in that it does not provide network-based protection, making it susceptible to spoofing attacks and manipulation.

In [19], the authors proposed a blockchain-based system that authenticates the caller and receiver before establishing a call. However, the proposed system requires users to register decentralized identities and phone number credentials, making it less convenient for users. Additionally, the worst-case call establishment overhead of 2.1 seconds for the proposed system would not make it desirable for real-time communication scenarios. Furthermore, the system proposed in [19] is limited to closed-circuit networks and may not be globally scalable. In contrast, our proposed solution in this paper, Blockchain-based Caller-ID Authentication (BBCA), is designed to prevent spoofing attacks in VoIP/SIP networks and applies to a wide range of communication networks.

All in all, the existing solutions in the literature either fail to address caller-ID spoofing attacks or have limitations that would make them ineffective in preventing these attacks. There is a lack of effective and efficient solutions for preventing caller-ID spoofing attacks, particularly for those that originate via VoIP. This highlights the need for further research in this area to address this important security issue.

Table 2 compares different caller-ID spoofing prevention techniques from an academic literature review perspective. It includes the academic literature and highlights the used technical approach, its levels of authentication, validation, and anti-spoofing, and its shortcomings/drawbacks. In Table 2, the *approach* column refers to the used technique to prevent caller-ID spoofing. The *authentication* column refers to the process of verifying the identity of the caller. The *validation* column refers to the process of verifying the authenticity of the calling party's number. The *anti-spoofing* column refers to the measures taken to prevent caller-ID spoofing attacks. Finally, the *shortcoming/drawback* column identifies the limitations and challenges of the given technique. Table 2 also includes our new approach, named *Blockchain-based Caller-ID Authentication*, which is designed to combat caller-ID spoofing attacks in real time by managing and verifying end-to-end caller-ID information. Our approach is efficient in that it reduces the risk of hacking and data tampering while not relying on costly encryption and decryption operations for security.

C. EVALUATION OF STANDARDS AND TECHNICAL CHALLENGES FOR CALLER-ID SPOOFING PREVENTION

Several standards have been proposed for the implementation of solutions against caller-ID spoofing. However, the assumptions made by these standards do not always align with the different types of infrastructures and caller-ID spoofing methods, leading to technical difficulties in their implementation [35], [36], [37]. In this section, we review six solutions against caller-ID spoofing attacks that are found in the existing RFCs and standards.

1) **RFC 3325 - Private Extensions to the SIP for Asserted Identity within Trusted Networks [38]:** The P-Asserted-Identity (PAI) header is a SIP header that is used to indicate the identity of the caller in a VoIP network. It is often used to pass caller-ID information from one network element to another. In the context of caller-ID spoofing, attackers can manipulate PAI headers to impersonate legitimate callers or conceal their identities, making it difficult to trace and prevent fraudulent activities. RFC 3325 assumes that end systems that originate calls cannot change SIP headers, or that intermediary devices can be trusted to remove PAI headers. However, this approach is inadequate as both situations can easily be circumvented with the flexibility provided by VoIP, allowing attackers to manipulate the PAI header and conduct caller-ID spoofing attacks. The PAI header format is shown in Figure 1.

```
...
P-Asserted-Identity: "Melih Tas <sip:melih@domain.com>
P-Asserted-Identity: tel:+14085264000
...
```

FIGURE 1. P-Asserted-Identity (PAI) header format in SIP.

2) **RFC 4474 - Enhancements for Authenticated Identity Management in the SIP [39]:** RFC 4474 suggests signing all SIP INVITE messages with the Session Description Protocol (SDP). However, if there is a Session Border Controller (SBC) in the call flow, the

TABLE 3. Comparison of standards and technical challenges for caller-ID spoofing prevention.

Study	Approach	Authentication	Valdiation	Anti-Spoofing	Shortcoming / Drawback
RFC 3325	*Uses the P-Asserted-Identity header in the SIP to assert the identity of the caller*	Medium	Low	Low	Inadequate for VoIP calls, easily circumvented and vulnerable to spoofing attacks
RFC 4474	*Uses digital signatures to ensure the authenticity of the SIP INVITE message*	High	Medium	Low	Complexity of the legacy infrastructure, not applicable in scenarios w/ SBCs, requires a public key infrastructure
STIR/SHAKEN	*Uses a signature-based token to verify the caller's number, aiming to reduce the impact of robocalling*	High	High	Medium	Complexity of legacy infrastructure, centralized database required
RFC 8226	*Uses X.509 certificates to authenticate the identity of the caller*	High	High	Medium	Requires a trusted certificate authority
RFC 8224	*Uses a header field in the SIP to carry a signature of the caller's identity*	Medium	Medium	Low	Complexity of extracting caller-ID information, a requirement for a centralized database
RFC 8225	*A framework for verifying caller-ID using digital certificates; only applicable to VoIP calls that traverse the IP network and not to calls that are made via SS7*	Medium	Medium	Medium	Lack of detailed implementation solution; inadequate for VoIP calls
This study	*Uses blockchain technology to create a decentralized ledger that stores caller-ID information and allows for real-time validation of caller-ID information to prevent caller-ID spoofing attacks*	High	High	High	Implementation difficulty due to regulatory compliance and integration

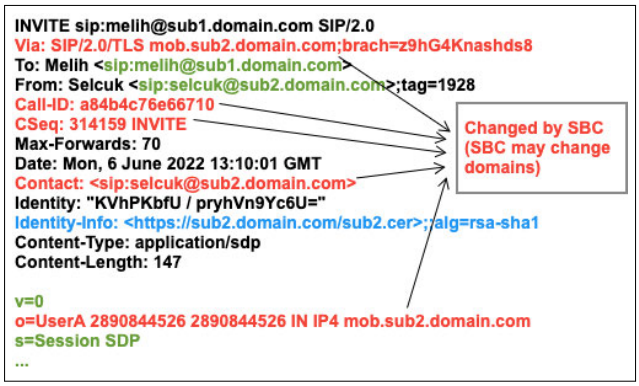

FIGURE 2. Example of SIP INVITE message with Session Description Protocol (SDP) included.

SBC has to change the headers, as shown in Figure 2. This makes the proposed solution inapplicable in such scenarios. Additionally, the proposed solution relies on the RSA algorithm, which may become increasingly challenging to implement as small and simple devices proliferate and VoIP traffic increases [26], [39], [40]. Moreover, the proposed caller-ID authentication mechanism cannot identify the person to whom the phone number is assigned. Intermediary devices must re-sign the request which introduces a performance overhead.

Back-to-Back User Agents (B2BUA) are intermediary entities that can modify SDP messages used to establish communication sessions. In the context of caller-ID spoofing prevention, when a B2BUA modifies an SDP message, it may change the caller number information, which can affect the accuracy of the used caller-ID authentication mechanism. Therefore, for the B2BUA scenario, the SDP must be rewritten to ensure that the caller number information remains accurate and consistent throughout the communication session.

Regulatory authorities often encourage the interconnection of VoIP networks. However, non-SIP interconnections can create challenges in implementing caller-ID authentication mechanisms that require comprehensive solutions. Changing communication infrastructures on a global scale is a challenging task, and existing infrastructures, such as SS7, which is widely used for the setup and tear-down of most telephone calls in the public switched telephone network, are expected to remain unchanged for a long time. This can create obstacles in the implementation of effective caller-ID authentication mechanisms since these mechanisms must consider the unique characteristics of the various communication infrastructures involved.

Therefore, in order to address the issue of caller-ID spoofing, more comprehensive solutions are needed, which can take into account the complexities of the existing various infrastructures and the interconnection points between them [41], [42].

3) **STIR/SHAKEN [43]:** STIR/SHAKEN is a framework that aims to verify a caller number using a signature-based token, with the goal of minimizing the impact of robocalling [44]. STIR (Secure Telephony Identity Revisited) RFC [45] and SHAKEN (Signature-based Handling of Asserted Information Using Tokens) [46] are the result of a collaboration between the Internet Engineering Task Force (IETF), Automatic Terminal Information Service (ATIS), the SIP Forum, and service providers [46]. SHAKEN is a more recent definition of how to implement STIR in practice. These efforts are based on an attempt to verify the caller number presented to the target user [45], [47].
   The STIR/SHAKEN framework allows service providers to add a digital signature to each call using public key encryption, thereby facilitating the authentication of the caller-ID information. This digital signature is included in the newly introduced SIP Identity header. When all originating service providers enable STIR/SHAKEN in their network, terminating providers will have much more control over both which calls to pass and which provider a call goes to [48] and [49].
   However, STIR/SHAKEN has some challenges in terms of interoperability. This is because it consists of works from different organizations such as IETF and ATIS, each with its own unique style of writing SIP specifications. Additionally, there are some known uncertainties in the certification model, such as determining who will sign first and who will be the first to approve. These scenarios are not clearly defined, which causes confusion regarding the applicability of this method.
4) **RFC 8226 - Secure Telephone Identity Credentials: Certificates [47]:** RFC 8226 describes the use of certificates in establishing authority over telephone numbers as part of a larger architecture for handling telephone numbers as identities in protocols like the SIP. The certification model is integrated with number assignments, such as ''Public key X has the authority to use number Y''. Number assignments are issued by the number assignment authority, such as the Number Portability Administration Center (NPAC), possibly through a delegation chain of authorization [10], [50]. The certification model also offers voice verification similar to web domain verification, such as ''enter the number you hear on the web form'' [51], [52].
   From the perspective of need, major carriers want to eliminate auto-call complaints, legitimate outgoing call centers want their messages to be delivered, and high-value users want to avoid identity theft. Carriers are concerned about inter-carrier compensation fraud and are tired of receiving complaints from customers. Newcomers look for a differentiator to make the transition and stop receiving automated calls. The certification model is proposed as a method that can meet all of these requirements. However, there are some known uncertainties in the certification model, such as who will sign first, and whether this should be done by choice or by mandate. Additionally, the applicability of this method causes confusion as the scenarios are not clearly defined.
5) **RFC 8224 - Authenticated Identity Management in the SIP [53]:** The proposed mechanism in RFC 8224 aims to securely identify the source of SIP requests through the use of a SIP header field for transmitting a signature used for authentication, and a reference to the signer's credentials. However, as noted in previous research, the baseline security mechanisms in the SIP are inadequate for cryptographically assuring the identity of end-users in an inter-domain context [54], [55]. Furthermore, RFCs do not explicitly define the method or algorithm for extracting caller-ID and callee-ID information from SIP messages, leading to uncertainty in the prioritization of various SIP headers. The SIP headers used for caller-ID, such as ''display name,'' ''PAI,'' or ''incoming,'' and those for callee-ID, such as ''display name,'' ''username'' in the ''to'' header, or the ''username'' in the Request-URI (Universal Resource Identifier), may have different priorities depending on the implementation. This lack of clear specification poses challenges to the practical implementation of this approach. A well-defined and consistent algorithm for the extraction and prioritization of caller and callee identification information from SIP messages is needed for the proper implementation of caller-ID authentication mechanisms.
6) **RFC 8225 - A Framework for Session Initiation Protocol (SIP) Caller Authentication and Identification [55]:** RFC 8225 presents a framework for authenticating and identifying callers in SIP-based telephony systems. The standard recommends the use of the STIR/SHAKEN framework for caller-ID validation, which utilizes digital signature-based tokens for authentication. However, the standard does not provide a comprehensive implementation guide for the proposed framework and fails to address the issue of caller-ID spoofing that originates via VoIP, highlighting the need for further research in this area.

Similar to Table 2, which compares the solutions against caller-ID spoofing in the academic literature, Table 3 compares the existing standards proposed for caller-ID spoofing prevention. Each standard has its own set of strengths and weaknesses, as described in the table. For instance, RFC 3325 assumes that end systems that originate a call will not change SIP headers, or that intermediary devices can be

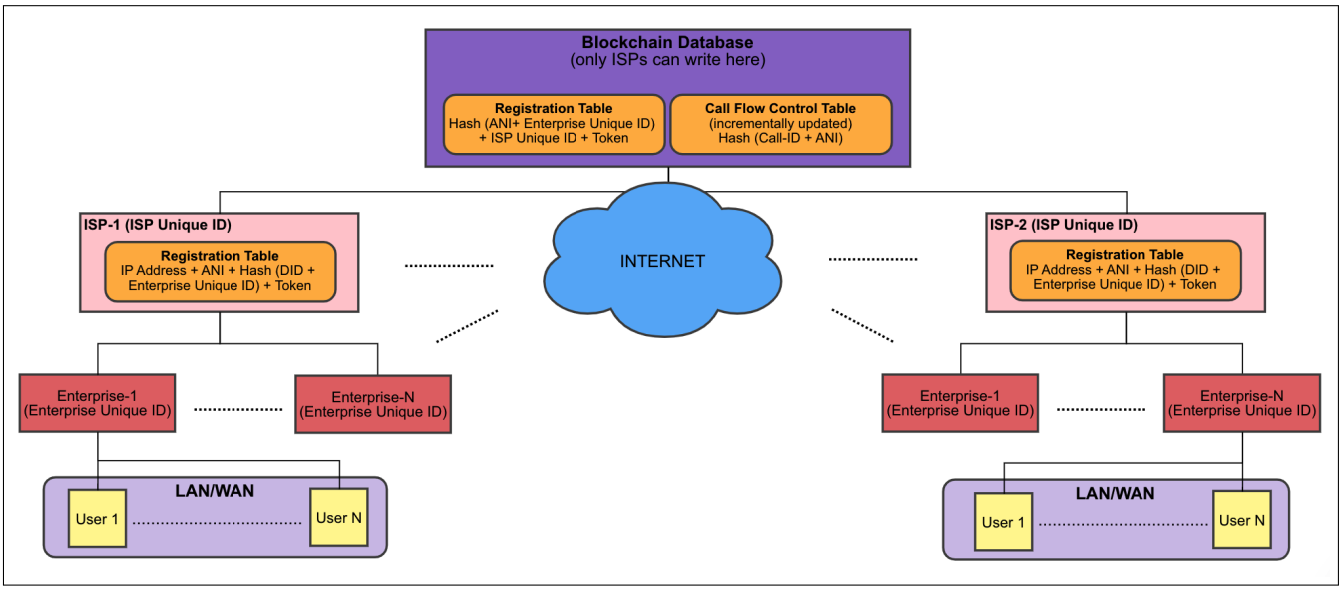

FIGURE 3. Visual representation of the proposed Blockchain Based Caller-ID Authentication (BBCA) mechanism.

trusted to remove PAI headers. This approach is inadequate as both situations can easily be circumvented with the flexibility provided by VoIP. On the other hand, STIR/SHAKEN is a framework to verify a caller number using a signature-based token aiming to minimize the impact of robocalling, but it is only applicable to VoIP calls that traverse the IP network and not to calls that are made via SS7. Additionally, it still suffers from challenges such as the need for a centralized database and the need to handle the complexity of the legacy infrastructure. Overall, it can be concluded that while existing standards have the potential to address the caller-ID spoofing problem, they also have limitations and challenges that need to be overcome.

In Table 3, we also include our novel blockchain-based caller-ID authentication solution which will be explained in detail in Section III. Our solution has the advantage of allowing for real-time validation of caller-ID information by using a decentralized ledger that stores caller-ID information.

III. OUR NOVEL BLOCKCHAIN-BASED SOLUTION APPROACH FOR CALLER-ID AUTHENTICATION

A. METHODOLOGY AND DESIGN

We have designed a novel defense mechanism that employs a low-latency blockchain consensus algorithm to effectively prevent caller-ID spoofing attacks in real time. Our blockchain-based novel registration and call flow control processes that are positioned in the cloud are able to manage and verify ISPs' and institutions' caller-ID information end-to-end. Our solution verifies when a call is initiated, from which ISP the call originated, whether there is a change in the caller-ID and ANI information and whether there is a change in the ANI information where the call originates at each hop change.

We chose to design a blockchain-based solution for caller-ID spoofing prevention because it offers a transparent, decentralized, and distributed solution that also helps reduce the risk of hacking and data tampering. Additionally, it allows for a more efficient approach to security by eliminating the need for costly encryption and decryption operations, resulting in less computational load and lower delay [19].

Our proposed solution for caller-ID spoofing prevention uses a modified version of the Practical Byzantine Fault Tolerance (PBFT) algorithm as the consensus algorithm. PBFT is a consensus algorithm that ensures all nodes in a distributed system agree on a common state, even in the presence of some faulty or malicious nodes. PBFT is known for its high performance, low latency, and tolerance to a large number of faulty nodes [56]. In our modification, we implement a two-phase commit protocol where a small subset of nodes called ''verifiers'' are responsible for quickly reaching a consensus on the validity of a caller-ID. The selection of verifiers is based on their reputation and past performance in the network, similar to the blockchain consensus mechanisms used in [20], [57], [58], [59], [60], [61], and [62]. This modification allows for low latency and real-time performance, which is critical for voice communication. The use of PBFT allows for a transparent, decentralized, and distributed solution that reduces the risk of hacking and data tampering. It eliminates the need for costly encryption and decryption operations, resulting in less computational load and lower delay, and thus helps meet the constraints on the real-time nature of voice communication and its sensitivity to Quality of Service (QoS) parameters.

In our blockchain-based caller-ID authentication mechanism, described in Figure 3, the Registration and Call Flow Control tables are kept in the blockchain database located in

the cloud. Only the ISPs that are registered to this database are allowed to write to it, but everyone can read from it. Each ISP has a unique ID value, named *ISP Unique ID*, that is assigned to it. Each organization that receives voice service from an ISP has a unique ID value, named *Enterprise Unique ID*, that is assigned to it.

Each ISP registers to the Registration Table using a Token value and its *ISP Unique ID*. ISPs renew their registrations periodically. The registration table logic is implemented similarly for sub-parties served by ISPs. Each ISP provides its enterprise clients with an ANI number or a group of ANI numbers based on the client's needs. A SIP client is registered in the Registration Table in the ISP with its registered IP address, ANI information, the hash of its Direct Inward Dialling (DID) number, and its *Enterprise Unique ID*. This information is updated whenever there is any change. When a VoIP call is initiated, the call-ID information along with this recorded information is stored in the Call Flow Control table in the blockchain database, as shown in Figure 3. This information is kept in this table until the call is terminated. The ISP, enterprise, or user information from which the call originated can be checked from the blockchain database at any time during the call flow. Hence, one can verify if the caller-ID is forged, hidden, or altered. Exemplary contents for the Call Flow Control and Registration tables are given with Figures 4 and 5, respectively. By using a blockchain-based consensus algorithm, our proposed solution can handle call flows under many different conditions. Additionally, the use of a reputation-based selection of verifiers allows for increased security and resilience against potential malicious actors in the network.

Call Flow Control Table Structure

1	Reg ID-1 (hash)	Call Flow ID-1 (hash)	Call initiated
2	Reg-ID-1 (hash)	Call Flow ID-2 (hash)	SBC involved
3	Reg-ID-2 (hash)	Call Flow ID-1 (hash)	Call initiated
4	Reg-ID-2 (hash)	Call Flow ID-1 (hash)	Call forwarded
5	Reg-ID-2 (hash)	Call Flow ID-1 (hash)	Roaming
6	Reg ID-1 (hash)	Call Flow ID-1 (hash)	Call terminated
7	Reg-ID-2 (hash)	Call Flow ID-1 (hash)	Call terminated

FIGURE 4. Call flow control table structure for the proposed Blockchain-Based Caller-ID Authentication (BBCA) mechanism.

An example of the use of this verification method is to send a certain verification token to the receiving end of the call to show whether the call is trustworthy or not. This verification mark can be a predefined sound recording or a certain signal tone, or it can be verification information that will be displayed on the phone screen if this is used on a mobile phone.

Registration Table Structure

1	ISP-1	Reg ID-1 (hash)	First registration
2	ISP-1	Reg ID-2 (hash)	Update-1
3	ISP-2	Reg ID-1 (hash)	First registration
4	ISP-2	Reg ID-1 (hash)	Update-1
5	ISP-1	Reg ID-3 (hash)	Update-2

FIGURE 5. Registration table structure for the proposed Blockchain-Based Caller-ID Authentication (BBCA) mechanism.

In our proposed system, we employ a two-step verification process to ensure the accuracy and integrity of ANI information throughout the entire call flow, as described in Figure 6.

The first step, Verification-1, is divided into two sub-stages:

1) V1.1 - Verifying the accuracy of the ANI information from the point of origin until it reaches the Internet via the first ISP.
2) V1.2 - Verifying the accuracy of the ANI information from the first ISP until it reaches the blockchain-based database/trusted authority.

In V1.1, as depicted in Figure 3, each VoIP service provider, referred to as an ISP, is assigned an *ISP Unique ID*. Each ISP customer, referred to as an Enterprise, is assigned an *Enterprise Unique ID*. Each ISP provides its enterprise clients with one or more ANI numbers based on their needs. The registration table, maintained by each ISP, stores the ANI information for each ANI provided to Enterprises, along with the IP address, a token value and the hash value of the combination of the DID number and *Enterprise Unique ID*. Each Enterprise is aware of its own hash value and includes it in the call information when initiating a call. Upon receiving a call request to be sent over the Internet, the ISP verifies the information against its registration table to confirm that the call is not spoofed.

In V1.2, our solution employs a low-latency consensus algorithm and a blockchain-based database that all ISPs can access in near real-time. Only registered ISPs are permitted to write to this database. Each ISP is assigned an *ISP Unique ID*, and for each Enterprise, the *ISP Unique ID*, a token value, and the hash value calculated from the combination of ANI and *Enterprise Unique ID* are stored in the registration table in the blockchain-based database. Each row in the registration table has a unique reference ID. Each ISP is aware of its own hash values in the registration table and includes the corresponding hash value in the call information when a call originates from its network. For each call request sent over the Internet, the call information is verified against the registration table to confirm that the call is not spoofed, and the reference

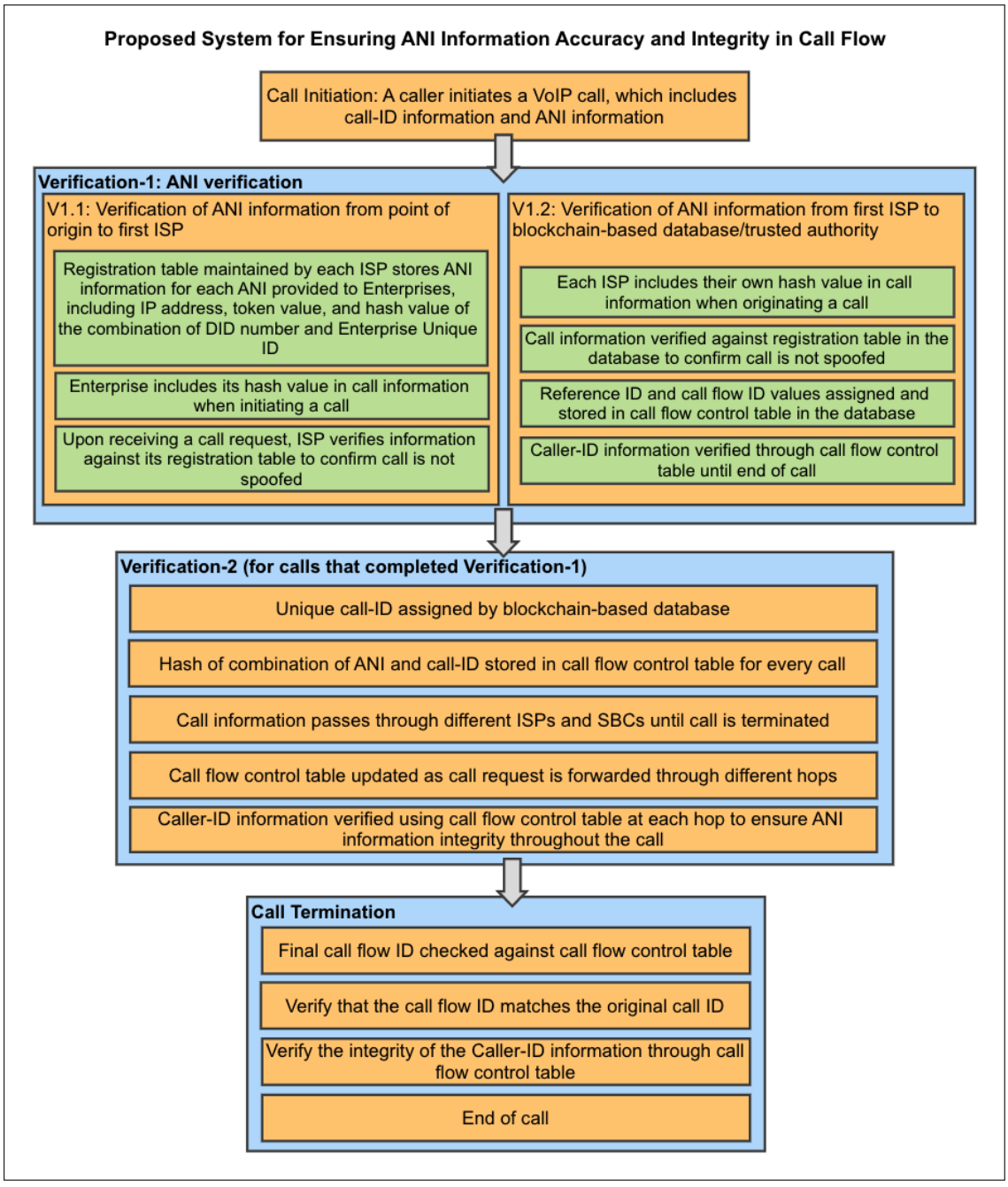

FIGURE 6. Flow diagram of ANI verification process for VoIP calls using a blockchain-based database and trusted authorities.

ID and call flow ID values are assigned and stored in the call flow control table in the blockchain-based database. The verification of the caller-ID information is carried out through this table until the end of the call.

The second step, Verification-2, is used for calls that have completed Verification-1. A unique call-ID is assigned by the blockchain-based database and the hash of the combination of ANI and call-ID is stored in the call flow control table for every call, as shown in Figure 3. This information passes through different ISPs and SBCs until the call is terminated. The originating information of the call may change as it passes through different ISPs and SBCs. The information in the call flow control table is updated as the call request is forwarded through different hops. The caller-ID is verified using the call flow control table in the blockchain-based database at each hop, ensuring the integrity of the ANI information throughout the call.

To ensure the scalability and robustness of our proposed solution, we have employed a low-latency consensus algorithm for maintaining the blockchain-based database. The

consensus algorithm ensures that all registered ISPs have a copy of the same database and that any changes made to the database are validated and agreed upon by all registered ISPs. This ensures that the database remains tamper-proof and that any malicious attempts to alter the caller-ID information are immediately detected and rejected.

In order to address scenarios in which caller-ID information may need to change frequently, our proposed system includes a mechanism for initiating a renewal of ISP registration every time the caller-ID information is updated. This approach ensures that our solution is not affected by situations such as the use of an IP-PBX at the end-user level, the use of a VPN at the end-user level, or instances in which roaming causes the caller-ID information to fluctuate between ISPs. By implementing this feature, we aim to ensure that our proposed solution remains effective and robust in dealing with these unusual scenarios.

Figure 6 shows the steps involved in verifying the authenticity of the ANI information for VoIP calls using a combination of a blockchain-based database and trusted authorities, which are third-party organizations or entities that are trusted to verify and validate the ANI information. The verification process consists of three main phases: Verification-1.1 (V1.1), Verification-1.2 (V1.2), and Verification-2, which together ensure that the ANI information remains intact and untampered throughout the call. In the V1.1 phase, the ANI information is verified from the point of origin to the first ISP by checking the hash values stored in a registration table. In the V1.2 phase, the ANI information is verified from the first ISP to the blockchain-based database by checking the hash values stored in the registration table in the database. Finally, in the Verification-2 phase, the ANI information is verified throughout the call by assigning unique call IDs and storing hash values in a call flow control table in the database. At the end of the call, the final call flow ID is checked against the call flow control table to ensure it matches the original call ID, and the caller-ID information is verified to ensure it has not been tampered with during the call.

B. SECURITY FEATURES

In addition to its primary function of protecting against caller-ID spoofing attacks, the proposed system is equipped with multiple security features to guard against various cyber threats, including denial of service and man-in-the-middle attacks. The system is designed to be highly resilient to these types of attacks by incorporating several different security measures.

One key security feature of the proposed system is its use of a low-latency consensus algorithm. This algorithm ensures that all ISPs have access to the blockchain database in almost real-time, making it difficult for an attacker to disrupt the system by overwhelming it with a large number of requests. Additionally, the system only allows registered ISPs to write to the blockchain database, further reducing the risk of a denial-of-service attack.

In order to fortify against man-in-the-middle attacks, the system employs a unique call ID, assigned by the blockchain database, to ensure the integrity of ANI information throughout the call process. This is complemented by the combined verification of ANI and the unique call ID at each communication hop, substantially diminishing the possibility of such attacks.

Addressing privacy concerns is paramount in our system design. To ensure the confidentiality of caller-ID information, we have implemented robust encryption protocols and strict access controls within our blockchain framework. Each transaction on the blockchain is encrypted, ensuring that only authorized entities can access sensitive caller-ID data. Moreover, we adhere to rigorous data protection standards, including compliance with international privacy regulations such as the General Data Protection Regulation (GDPR) [63]. This comprehensive approach to data privacy not only safeguards user information from unauthorized access but also builds trust in our system's integrity and reliability.

In order to ensure the integrity of the system, the proposed system also includes several other security features such as the use of a token value and the hash value of the combination of the ANI and Enterprise Unique ID. These features, along with the other security measures, ensure that the proposed system is highly resilient to a variety of different types of attacks.

In order to mitigate the risk of a single point of failure, our system employs a decentralized architecture, distributing data storage and processing across multiple nodes. This design ensures that the failure of any single node or component does not compromise the entire system's functionality. Additionally, we implement regular system health checks and automatic failover mechanisms to maintain continuous operation. By leveraging the distributed nature of blockchain technology and incorporating these redundancy features, our system maintains high availability and resilience, significantly reducing the vulnerability to both internal and external disruptions.

While the proposed system significantly enhances security against a broad spectrum of attacks, ongoing research and development are essential to further strengthen its defenses and address any emerging vulnerabilities.

IV. LIMITATIONS AND FUTURE WORK

Our proposed solution demonstrates potential in effectively mitigating caller-ID spoofing attacks in real time. However, further research is required to explore and address several aspects for its successful large-scale deployment.

Specifically, future studies will focus on detailed implementation aspects and experimental evaluations to validate the scalability and performance of our proposed consensus algorithm in diverse real-world scenarios [64], [65], [66], [67]. These investigations will include but are not limited to handling complex scenarios such as call forwarding

and teleconferencing, where the dynamics of caller-ID verification are significantly different. We aim to conduct extensive testing to not only assess the robustness of our system in varied conditions but also to identify and rectify any limitations that may arise.

Additionally, the relevance and integration of blockchain technology in mitigating caller-ID spoofing are of paramount importance. We intend to further elucidate the role of blockchain in enhancing the security and trustworthiness of caller-ID information. This involves exploring the integration of our solution within existing SIP systems, assessing compatibility, and ensuring smooth transition and backward compatibility. Protocol enhancements, if required for full functionality, will be a key focus of our research, ensuring that the proposed solution augments existing calls and connections positively without introducing disruptions.

Moreover, we recognize the necessity of aligning our solution with existing standards and regulatory frameworks. Future work will encompass conducting an RFC study to update protocol specifications, thereby aiding telecom vendors in complying with the new requirements at various levels, including server, client, and network. This aligns with our goal to facilitate a seamless and compliant integration of our solution into the existing telecommunications infrastructure.

Finally, we will concentrate on the regulatory aspects of our solution, defining and implementing necessary compliance standards for service providers. This will include working collaboratively with service providers to establish an alliance agreement that effectively governs the administration of our system. Research into the feasibility and timeline for service providers to demonstrate compliance will also be a critical part of our future efforts.

V. CONCLUSION

In this paper, we have critically reviewed existing solutions against caller-ID spoofing, pinpointing their limitations from both academic and standard perspectives. Building on this analysis, we proposed an innovative blockchain-based defense mechanism, tailored for real-time mitigation of caller-ID spoofing attacks. Our solution, leveraging blockchain technology, creates an immutable record of each call, its origin, and offers a secure, decentralized approach for managing and verifying caller-ID information.

Our blockchain-based solution not only presents a practical mechanism to combat caller-ID spoofing but also considers its integration within existing SIP systems and its backward compatibility. As we move forward, our future work will be dedicated to refining this solution, focusing on its scalability, performance in real-world settings, and ensuring that it aligns with the evolving technological landscape and regulatory requirements. This future work will be instrumental in advancing the practical implementation of our solution, making it a robust, scalable, and integral part of the telecommunications security infrastructure.

REFERENCES

[1] H. Tu, A. Doupé, Z. Zhao, and G.-J. Ahn, "SoK: Everyone hates robocalls: A survey of techniques against telephone spam," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2016, pp. 320–338, doi: 10.1109/SP.2016.27.

[2] *SpoofCard*. Accessed: Apr. 20, 2023. [Online]. Available: https://www.spoofcard.com/

[3] I. M. Tas. *SIP-Based Audit and Attack Tool*. Accessed: Mar. 1, 2023. [Online]. Available: https://github.com/meliht/mr.sip

[4] J. Stanek and L. Kencl, "SIPp-DD: SIP DDoS flood-attack simulation tool," in *Proc. 20th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2011, pp. 1–7, doi: 10.1109/ICCCN.2011.6005946.

[5] I. M. Tas, B. G. Unsalver, and S. Baktir, "Our proposed SIP-based distributed reflection denial of service (DRDoS) attacks & effective defense mechanism," in *Proc. Interdiscipl. Cyber Res. Workshop (ICR)*, 2015, 2015, pp. 15–16.

[6] I. M. Tas, B. G. Unsalver, and S. Baktir, "A novel SIP based distributed reflection denial-of-service attack and an effective defense mechanism," *IEEE Access*, vol. 8, pp. 112574–112584, 2020, doi: 10.1109/ACCESS.2020.3001688.

[7] I. M. Tas, B. Ugurdogan, and S. Baktir, "Novel session initiation protocol-based distributed denial-of-service attacks and effective defense strategies," *Comput. Secur.*, vol. 63, pp. 29–44, Nov. 2016, doi: 10.1016/j.cose.2016.08.007.

[8] I. M. Tas and S. Baktir, "A novel approach for efficient mitigation against the SIP-based DRDoS attack," *Appl. Sci.*, vol. 13, no. 3, p. 1864, Jan. 2023, doi: 10.3390/app13031864.

[9] S. Pandit, J. Liu, R. Perdisci, and M. Ahamad, "Applying deep learning to combat mass robocalls," in *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2021, pp. 63–70, doi: 10.1109/SPW53761.2021.00018.

[10] H. Mustafa, W. Xu, A.-R. Sadeghi, and S. Schulz, "End-to-end detection of caller ID spoofing attacks," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 3, pp. 423–436, May 2018, doi: 10.1109/TDSC.2016.2580509.

[11] D. S. K. Putra, M. A. Sadikin, and S. Windarta, "S-mbank: Secure mobile banking authentication scheme using signcryption, pair based text authentication, and contactless smart card," in *Proc. 15th Int. Conf. Quality Res. (QiR): Int. Symp. Electr. Comput. Eng.*, Jul. 2017, pp. 230–234, doi: 10.1109/QIR.2017.8168487.

[12] T. Stefanovic and S. Ghilezan, "Preserving privacy in caller ID applications," in *Privacy and Identity Management* (IFIP Advances in Information and Communication Technology), vol. 619, M. Friedewald, S. Schiffner, and S. Krenn, Eds. Cham, Switzerland: Springer, 2021, pp. 151–168, doi: 10.1007/978-3-030-72465-8_9.

[13] J. Li, F. Faria, J. Chen, and D. Liang, "A mechanism to authenticate caller ID," in *Recent Advances in Information Systems and Technologies (WorldCIST)* (Advances in Intelligent Systems and Computing), vol. 570, Á. Rocha, A. Correia, H. Adeli, L. Reis, and S. Costanzo, Eds. Cham, Switzerland: Springer, 2017, pp. 745–753, doi: 10.1007/978-3-319-56538-5_75.

[14] M. Sahin, A. Francillon, P. Gupta, and M. Ahamad, "SoK: Fraud in telephony networks," in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroS&P)*, Apr. 2017, pp. 235–250, doi: 10.1109/EUROSP.2017.40.

[15] D. V. S. R. K. Koilada, "Strategic spam call control and fraud management: Transforming global communications," *IEEE Eng. Manag. Rev.*, vol. 47, no. 3, pp. 65–71, 3rd Quart., 2019, doi: 10.1109/EMR.2019.2924635.

[16] P. Gupta, B. Srinivasan, V. Balasubramaniyan, and M. Ahamad, "Phoneybot: Data-driven understanding of telephony threats," in *Proc. Netw. Distrib. Syst. Secur. (NDSS) Symp.*, San Diego, CA, USA, Feb. 2015, pp. 8–11, doi: 10.14722/ndss.2015.23176.

[17] H. Tu, A. Doupé, Z. Zhao, and G. J. Ahn, "Users really do answer telephone scams," in *Proc. 28th USENIX Secur. Symp.*, Santa Clara, CA, USA, Aug. 2019, pp. 1–15.

[18] I. M. Tas and K. A. Kucuk. (2020). *Practical VoIP-UC Hacking Using Mr.SIP- SIP-Based Audit & Attack Tool*. [Online]. Available: https://https://infocondb.org/con/def-con/def-con-28/

[19] Y. Chen, Y. Wang, Y. Wang, M. Li, G. Dong, and C. Liu, "CallChain: Identity authentication based on blockchain for telephony networks," in *Proc. IEEE 24th Int. Conf. Comput. Supported Cooperat. Work Design (CSCWD)*, May 2021, pp. 416–421, doi: 10.1109/CSCWD49262.2021.9437650.

[20] J. Yang, Z. Jia, R. Su, X. Wu, and J. Qin, "Improved fault-tolerant consensus based on the PBFT algorithm," *IEEE Access*, vol. 10, pp. 30274–30283, 2022, doi: 10.1109/ACCESS.2022.3153701.

[21] D. Hou, H. Han, and E. Novak, "TAES: Two-factor authentication with end-to-end security against VoIP phishing," in *Proc. IEEE/ACM Symp. Edge Comput. (SEC)*, Nov. 2020, pp. 340–345, doi: 10.1109/SEC50012.2020.00049.

[22] R. Kurdi, F. Hersi, S. Bahagari, M. Kaosar, S. M. Qaisar, and A. Subasi, "A mobile fingerprint authentication in Saudi Arabian call centers," in *Proc. Int. Conf. Electr. Comput. Technol. Appl. (ICECTA)*, Nov. 2017, pp. 1–4, doi: 10.1109/ICECTA.2017.8252000.

[23] N. Sukma and R. Chokngamwong, "Increasing the efficiency of one-time key issuing for the first verification caller ID spoofing attacks," in *Proc. 15th Int. Joint Conf. Comput. Sci. Softw. Eng. (JCSSE)*, Jul. 2018, pp. 1–6, doi: 10.1109/JCSSE.2018.8457341.

[24] B. Reaves, L. Blue, H. Abdullah, L. Vargas, P. Traynor, and T. Shrimpton, "AuthentiCall: Efficient identity and content authentication for phone calls," in *Proc. 26th USENIX Secur. Symp.*, Vancouver, BC, Canada, Aug. 2017, pp. 1–19.

[25] B. Reaves, L. Blue, and P. Traynor, "AuthLoop: End-to-end cryptographic authentication for telephony over voice channels," in *25th USENIX Secur. Symp.*, Austin, TX, USA, Aug. 2016, pp. 1–17.

[26] Y. Rebahi, J. J. Pallares, N. T. Minh, S. Ehlert, G. Kovacs, and D. Sisalem, "Performance analysis of identity management in the session initiation protocol (SIP)," in *Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl.*, Mar./Apr. 2008, pp. 711–717, doi: 10.1109/AICCSA.2008.4493606.

[27] V. Miller and S. Victor, "Use of elliptic curves in cryptography," in *Advances in Cryptology–(CRYPTO)*. Berlin, Germany: Springer, 1986, pp. 417–426.

[28] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, Jan. 1987.

[29] H. Li, X. Xu, C. Liu, T. Ren, K. Wu, X. Cao, W. Zhang, Y. Yu, and D. Song, "A machine learning approach to prevent malicious calls over telephony networks," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2018, pp. 53–69, doi: 10.1109/SP.2018.00034.

[30] M. A. Azad, S. Bag, C. Perera, M. Barhamgi, and F. Hao, "Authentic caller: Self-enforcing authentication in a next-generation network," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3606–3615, May 2020, doi: 10.1109/TII.2019.2941724.

[31] A. Sheoran, S. Fahmy, C. Peng, and N. Modi, "Nascent: Tackling caller-ID spoofing in 4G networks via efficient network-assisted validation," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2019, pp. 676–684, doi: 10.1109/INFOCOM.2019.8737567.

[32] N. Sukma and R. Chokngamwong, "One time key issuing for verification and detecting caller ID spoofing attacks," in *Proc. 14th Int. Joint Conf. Comput. Sci. Softw. Eng. (JCSSE)*, Jul. 2017, pp. 1–4, doi: 10.1109/JCSSE.2017.8025898.

[33] H. Tu, A. Doupe, Z. Zhao, and G.-J. Ahn, "Toward standardization of authenticated caller ID transmission," *IEEE Commun. Standards Mag.*, vol. 1, no. 3, pp. 30–36, Sep. 2017, doi: 10.1109/MCOMSTD.2017.1700019.

[34] H. Tu, A. Doupé, Z. Zhao, and G.-J. Ahn, "Toward authenticated caller ID transmission: The need for a standardized authentication scheme in Q.731.3 calling line identification presentation," in *Proc. ITU Kaleidoscope: ICTs Sustain. World (ITU WT)*, Nov. 2016, pp. 1–8, doi: 10.1109/ITU-WT.2016.7805728.

[35] H. H. Kilinc and T. Yanik, "A survey of SIP authentication and key agreement schemes," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 1005–1023, 2nd Quart., 2014, doi: 10.1109/SURV.2013.091513.00050.

[36] A. Durlanik and I. Sogukpinar, "SIP authentication scheme using ECDH," *Enformatika*, vol. 8, pp. 350–353, Sep. 2005.

[37] D. Suthar and P. H. Rughani, "A comprehensive study of VoIP security," in *Proc. 2nd Int. Conf. Adv. Comput., Commun. Control Netw. (ICACCCN)*, Dec. 2020, pp. 812–817, doi: 10.1109/ICACCCN51052.2020.9362943.

[38] C. Jennings, J. Peterson, and M. Watson, *Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks*, document RFC 3325, RFC Editor, Nov. 2002, doi: 10.17487/RFC3325.

[39] J. Peterson and C. Jennings, *Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)*, document RFC 4474, RFC Editor, Aug. 2006, doi: 10.17487/RFC4474.

[40] T. Chen, H. Yeh, P. Liu, H. Hsiang, and W. Shih, "A secured authentication protocol for SIP using elliptic curves cryptography," in *FGCN 2010: Communication and Networking*, vol. 119. Berlin, Germany: Springer, 2010, pp. 46–55, doi: 10.1007/978-3-642-17587-9_6.

[41] *E.164: The International Public Telecommunication Numbering Plan*. Accessed: May 25, 2023. [Online]. Available: https://en.wikipedia.org/wiki/E.164

[42] P. Faltstrom, *E.164 number and DNS*, document RFC 2916, RFC Editor, Sep. 2000, doi: 10.17487/RFC2916.

[43] C. Wendt and M. Barnes, *Personal Assertion Token (PaSSporT) Extension for Signature-Based Handling of Asserted Information Using toKENs (SHAKEN)*, document RFC 8588, RFC Editor, May 2019, doi: 10.17487/RFC8588.

[44] *ATIS Tech. Rep. a Framework for Display Verified Caller-ID*, The Alliance for Telecommunication Industry Solutions (ATIS), May 2018. [Online]. Available: https://access.atis.org/apps/group_public/

[45] J. Peterson, H. Schulzrinne, and H. Tschofenig, *Secure Telephone Identity Problem Statement and Requirements*, document RFC 7340, RFC Editor, Sep. 2014, doi: 10.17487/RFC7340.

[46] (Jul. 2017). *Signature-Based Handling of Asserted Information Using toKENs (SHAKEN): Governance Model and Certificate Management*. The Alliance for Telecommunications Industry Solutions (ATIS). [Online]. Available: https://atis.connectedcommunity.org/higherlogic/ws/public/download/67436

[47] J. Peterson and S. Turner, *Secure Telephone Identity Credentials: Certificates*, document RFC 8226, RFC Editor, Feb. 2018, doi: 10.17487/RFC8226.

[48] J. McEachern and E. Burger, "How to shut down robocallers: The STIR/SHAKEN protocol will stop scammers from exploiting a caller ID loophole," *IEEE Spectr.*, vol. 56, no. 12, pp. 46–52, Dec. 2019, doi: 10.1109/MSPEC.2019.8913833.

[49] M. Chiang and E. Burger, "An affordable solution for authenticated communications for enterprise and personal use," in *Proc. IEEE 8th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2018, pp. 810–815, doi: 10.1109/CCWC.2018.8301725.

[50] J. Peterson, *Secure Telephone Identity Threat Model*, document RFC 7375, RFC Editor, Oct. 2014, doi: 10.17487/RFC7375.

[51] J. Penttinen, "Unwanted robocalls challenges and solutions," in *Proc. GSMA Conf.*, Feb. 2020. Accessed: May 27, 2023. [Online]. Available: https://www.gsma.com/northamerica/wp-content/uploads/2020/02/GSMA_Robocall-White-Paper.pdf

[52] D. Bhasker, "STIR SHAKE'N SIP to stop robocalling," in *Proc. RSA Conf.*, Mar. 2019. Accessed: May 10, 2023. [Online]. Available: https://static.rainfocus.com/rsa/presentations/USA19/2019_USA19_str-f01_01_stir-shake-n-sip-to-stop-robocalling.pdf

[53] J. Peterson and C. Jennings and E. Rescorla and C. Wendt, *Authenticated Identity Management in the Session Initiation Protocol (SIP)*, document RFC 8224, RFC Editor, Feb. 2018, doi: 10.17487/RFC8224.

[54] L. Chircu. (Apr. 2021). *Testing the Trending SIP Security Enhancements*, Open SIP Interoperability Testing Event (OpenSIPIt '01). [Online]. Available: https://blog.opensips.org/2021/04/20/

[55] C. Wendt and J. Peterson, *PASSporT: Personal Assertion Token*, document RFC 8225, RFC Editor, Feb. 2018, doi: 10.17487/RFC8225.

[56] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. 3rd Symp. Operating Syst. Design Implement. (OSDI)*, New Orleans, LA, USA, Feb. 1999, pp. 173–186. Accessed: May 12, 2023. [Online]. Available: https://dl.acm.org/doi/10.5555/296806.296824

[57] M. A. Ferrag and L. Maglaras, "DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1285–1297, Nov. 2020, doi: 10.1109/TEM.2019.2922936.

[58] Y. Wang, S. Cai, C. Lin, Z. Chen, T. Wang, Z. Gao, and C. Zhou, "Study of blockchains's consensus mechanism based on credit," *IEEE Access*, vol. 7, pp. 10224–10231, 2019, doi: 10.1109/ACCESS.2019.2891065.

[59] Z. Cai, "Usage of deep learning and blockchain in compilation and copyright protection of digital music," *IEEE Access*, vol. 8, pp. 164144–164154, 2020, doi: 10.1109/ACCESS.2020.3021523.

[60] L. Vishwakarma, A. Nahar, and D. Das, "LBSV: Lightweight blockchain security protocol for secure storage and communication in SDN-enabled IoV," *IEEE Trans. Veh. Technol.*, vol. 71, no. 6, pp. 5983–5994, Jun. 2022, doi: 10.1109/TVT.2022.3163960.

[61] Y. Meshcheryakov, A. Melman, O. Evsutin, V. Morozov, and Y. Koucheryavy, "On performance of PBFT blockchain consensus algorithm for IoT-applications with constrained devices," *IEEE Access*, vol. 9, pp. 80559–80570, 2021, doi: 10.1109/ACCESS.2021.3085405.

[62] R. Saha, G. Kumar, G. Geetha, M. Alazab, R. Thomas, M. K. Rai, and J. J. P. C. Rodrigues, "The blockchain solution for the security of internet of energy and electric vehicle interface," *IEEE Trans. Veh. Technol.*, vol. 70, no. 8, pp. 7495–7508, Aug. 2021, doi: 10.1109/TVT.2021.3094907.

[63] *General Data Protection Regulation*. Accessed: Apr. 20, 2023. [Online]. Available: https://gdpr.eu/
[64] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, and M. A. Imran, "A scalable multi-layer PBFT consensus for blockchain," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 5, pp. 1146–1160, May 2021, doi: 10.1109/TPDS.2020.3042392.
[65] H. N. Abishu, A. M. Seid, Y. H. Yacob, T. Ayall, G. Sun, and G. Liu, "Consensus mechanism for blockchain-enabled vehicle-to-vehicle energy trading in the Internet of Electric Vehicles," *IEEE Trans. Veh. Technol.*, vol. 71, no. 1, pp. 946–960, Jan. 2022, doi: 10.1109/TVT.2021.3129828.
[66] L. Wang, Y. Bai, Q. Jiang, V. C. M. Leung, W. Cai, and X. Li, "Beh-Raft-chain: A behavior-based fast blockchain protocol for complex networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1154–1166, Apr. 2021, doi: 10.1109/TNSE.2020.2984490.
[67] W. Zhang, G. Sun, L. Xu, Q. Lu, H. Ning, P. Zhang, and S. Yang, "A trustworthy safety inspection framework using performance-security balanced blockchain," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8178–8190, Jun. 2022, doi: 10.1109/JIOT.2021.3121512.

I. MELIH TAS received the B.Sc. and M.Sc. degrees in computer and electronics science from Marmara University, İstanbul, Turkey, in 2007 and 2013, respectively, and the Ph.D. degree in computer engineering, specializing in cybersecurity from Bahçeşehir University, İstanbul, in 2023. Currently, he is the VP of Application Security with Instinet, London, U.K. Prior to this, he was a Senior Security Consultant with Synopsys, London, the Tech Lead of Garanti BBVA Bank, İstanbul, and a Cybersecurity Research and Development Engineer at NETAŞ, İstanbul.

Between 2019 and 2023, he was awarded three research grants from The Scientific and Technological Research Council of Turkey (TUBITAK). In 2020, he won first place in the Cybersecurity Project Competition conducted by Turk Telekom and also secured the top position in the Cybersecurity Thesis Competition organized by Turkish Cybersecurity Cluster. Recognized as a Global Talent by Tech Nation, U.K., he delivered speeches at prominent hacker conferences like DEFCON and BlackHat. His research on VoIP security was published in leading academic journals. He is the Creator of the Innovative VoIP Security Testing Framework Mr. SIP. His research interests include VoIP security and application security.

SELCUK BAKTIR (Senior Member, IEEE) received the B.Sc. degree in electrical engineering from Bilkent University, Ankara, Turkey, in 2001, and the M.Sc. and Ph.D. degrees in electrical and computer engineering from Worcester Polytechnic Institute, MA, USA, in 2003 and 2008, respectively.

He worked for companies, including IBM T. J. Watson Research Center and Intel Corporation. He was a Visiting Researcher with the Chair for Embedded Security, Ruhr University Bochum, Germany. In 2013, he founded the M.Sc. Program in Cybersecurity, Bahçeşehir University, İstanbul, Turkey. He is currently with the Computer Engineering Department, American University of the Middle East, Kuwait. His research interests include applied cryptography and computer security. He received the IBM Research Pat Goldberg Memorial Best Paper Award, in 2007, European Union FP7 Marie Curie IRG Award, in 2010, and the TUBITAK Career Award, in 2016.