I.J. Intelligent Systems and Applications, **2024, 5, 68-78**
Published Online on October 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijisa.2024.05.06

Identification of Customer Through Voice Biometric System in Call Centres

Amjad Hassan Khan M. K.*
Department of Electronics, Kristu Jayanti College, Bengaluru-560077, India
Institute of Engineering & Technology, Srinivas University, Mangalore-575001, India
E-mail: itzamjad@gmail.com
ORCID iD: https://orcid.org/0000-0003-4299-7948
*Corresponding Author

P. S. Aithal
Institute of Engineering & Technology, Srinivas University, Mangalore-575001, India
E-mail: psaithal@gmail.com
ORCID iD: https://orcid.org/0000-0002-4691-8736

Received: 04 March 2024; Revised: 20 April 2024; Accepted: 15 June 2024; Published: 08 October 2024

Abstract: In recent times, there has been a growing emphasis on adjusting communication strategies to foster strong customer relationships. This shift is driven by intensified competition, market maturation, and swift advancements in business technology. Consequently, companies have established call centers to efficiently handle customer support and fulfil customer inquiries. A pivotal aspect of enhancing service quality within these call centers involves accurately identifying customers during their interactions. The primary objective of this study is to introduce a methodology for identifying customers within call centers by analyzing their voice characteristics. Voice authentication (VA) has gained prominence in critical security operations, including banking transactions and conversations within call centers. The susceptibility of automatic speaker verification systems (ASVs) to deceptive spoofing attacks has prompted the development of countermeasures (CMs). These countermeasures are designed to differentiate between authentic and fabricated speech. ASVs and CMs collectively constitute contemporary VA systems, positioned as robust access control mechanisms. To achieve this goal, various customer identification systems within call centers have been examined, along with an analysis of audio signal attributes. Ultimately, the manuscript presents a novel approach to customer identification through voice biometrics. Notably, this method excels in recognizing customers even when provided with limited voice data. Empirical findings demonstrate that the suggested speaker identity confirmation method outperforms alternative techniques utilizing different algorithms, exhibiting a higher recognition rate. The present research work is based on two important perspectives of the call centres: a. call center agents experience and b. customer experience. The data collected separately from customers and agents for understanding the effective usage of voice biometric system in call centres. The data represented and satisfies the effectiveness of voice biometric system from both the perspectives. From the data it is also cleared that, the implementation of voice biometric system in call centres still have long way to go but will be a major technological change for the industries worldwide.

Index Terms: Voice Biometric, Call Centers, Customer Relation Management, Voice Authentication.

1. Introduction

The investigation and assessment of biometric data for business objectives is a growing area of interest for practitioners and researchers [1]. Voice biometrics serves as a multifaceted solution that addresses three distinct objectives. Its application leads to improved security of customer data, a seamless customer experience, and cost-effectiveness. The technology effectively establishes a means to ensure that authorized individuals gain access while preventing unauthorized entities from infiltrating systems. This potent tool has gained widespread adoption within the intricate realm of call centers, offering a pivotal layer of protection. In parallel with technological advancement designed to mitigate human overexertion, the landscape of cyber-related crimes, particularly fraud, has taken on a more sophisticated guise. Among the sectors susceptible to falling victim to such fraudulent activity, the Contact Center industry stands as a noteworthy example. Continuously seeking avenues to enhance customer experiences while maintaining cost-efficiency and heightened security, the contact center sector has gravitated towards embracing Voice

Authentication.

At the heart of voice biometrics lies a reliance on the distinct speech characteristics exhibited by callers to ascertain their legitimacy. When customers reach out to contact centers, voice biometrics pivots towards validating the speaker's claim of identity by cross-referencing their voice against an existing Voiceprint [2]. Unlike traditional authentication methods that hinge on knowledge-based queries (such as favorite color or PIN) or token-based mechanisms, Voice Biometric leverages inherent biological markers unique to each caller for verification and authentication. These markers encompass a blend of behavioral traits such as pronunciation, accent, and emphasis, as well as physical attributes encompassing lung capacity, vocal tract configuration, and nasal passages. This amalgamation of unique vocal markers attributed to each caller is subjected to analysis involving hundreds of speakers. The resulting distinct voice pattern is christened a "Voiceprint" and is encrypted to ensure its exclusivity within the system of its origin. This inherent encryption bolsters the system's resistance to hacking attempts [3]. Through a process of comparing a caller's voice to the stored voiceprint corresponding to their identity, Voice Biometrics authoritatively confirms the caller's identity, thereby aligning with the individual's registered credentials. Leveraging sophisticated voice biometrics software, accuracy, and security, contact centers are also empowered to thwart the entry of unauthorized individuals.

Two distinct enrollment processes are instrumental in fostering a sense of reassurance among agents regarding the

Authenticity of callers: Active Enrollment involves prompting customers to recite specific phrases during calls to establish their unique voiceprint. This authentication process is repeated each time a caller connects with the center, allowing a comparison of their voice pattern with the stored voiceprint.

In contrast, Passive Enrollment introduces a more advanced and secure approach. This background process generates and registers a voiceprint during a normal conversation between a caller and an agent. Subsequent calls are verified through this established voiceprint without requiring additional recitation of phrases or numbers. The passive voice authentication mechanism facilitates a seamless procedure for the caller. Both enrollment methods contribute to agents' peace of mind, as they can confidently identify callers based on their Positive Voiceprint. Additionally, the concept of a Negative Voiceprint proves valuable for blacklisting unauthorized callers and issuing alerts, thereby bolstering the safeguarding of customer data against fraudulent activities.

Machine learning and artificial intelligence have revolutionized voice recognition technology, enabling remarkable advancements in human-computer interaction. Through sophisticated algorithms and neural networks, these systems can analyze and interpret spoken language with unprecedented accuracy and efficiency. By training on vast datasets, machine learning models can learn the intricacies of various accents, dialects, and speech patterns, continuously improving their performance over time. This technology has been seamlessly integrated into numerous applications, from virtual assistants like Siri and Alexa to speech-to-text transcription services. Moreover, AI-driven voice recognition has found extensive utility in diverse fields, including healthcare, finance, and customer service, streamlining processes and enhancing user experiences. As research in this domain continues to evolve, we can anticipate even more innovative applications and refinements, ultimately enhancing the accessibility and effectiveness of voice-based interfaces in our daily lives. However, the present approach of this research work is in line with the same. The techniques irrespective of ML and Ai, it’s not implemented for the banking or call centers. The research approach in this article will be helpful for the AI and ML for the practical implementation of voice biometric system in day to day life.

Despite the evident merits of voice biometrics, its widespread deployment remains limited due to various challenges faced by contact centers. These challenges encompass issues of customer adoption, with privacy concerns leading to reluctance among a substantial portion of callers to generate their voiceprints [4,5]. This results in a significant proportion of callers remaining unregistered. Furthermore, concerns related to call quality contribute to verification failures, leaving only a fraction of caller voices available for generating voice biometric patterns. Instances of false authentication also pose a challenge, with a small probability of the system inaccurately authenticating a fraudulent caller. This situation is exacerbated by the fact that once a fraudster gains authentication, they enjoy prolonged access, exploiting voice biometrics as a single layer of protection. Moreover, voice biometrics is limited in its ability to detect fraud, thus relying on post-incident forensics for identification. Lastly, the potential of false or stolen voiceprints adds an additional layer of concern to the implementation of voice biometrics. Fig.1. represents the block diagram for the voice biometric system implemented in call centre. This figure illustrates how voice-based biometric technology is used in call centres to improve security standards and verify callers. It also shows the interconnected parts and processes that are essential to the system's functioning. This sophisticated system's operation, from the initial receipt of voice samples to the complex matching algorithms used for identity verification, can be fully understood by stakeholders through visual aids, emphasizing the system's importance in enhancing operational efficiency and reducing the risks associated with fraudulent activities.

Amidst these potential challenges, there are compelling reasons that position Voice Biometrics as a potent weapon against fraud. The technology, as established, offers heightened security compared to traditional authentication methods [6]. With its capacity to provide robust security and a guaranteed solution against fraud, Voice Biometrics holds great promise. The manner in which it can benefit a contact center is articulated as follows:

Average Handle Time and Cost Reduction: Traditional manual authentication of callers' identities consumes an average of 30 to 45 seconds per call. The integration of passive voice authentication reduces the average handle time by approximately 40 seconds. Passive authentication eliminates the need for agents to pose questions to customers. In comparison, calls managed by live agents using CATI Surveys are significantly more expensive than those handled

through IVR Survey Software. By containing calls within the IVR, optimal use of verification tools and data security are ensured, resulting in a cost reduction of approximately 6 to 7 times. Consequently, increased operational efficiency enables contact centers to enhance security measures while simultaneously reducing costs.

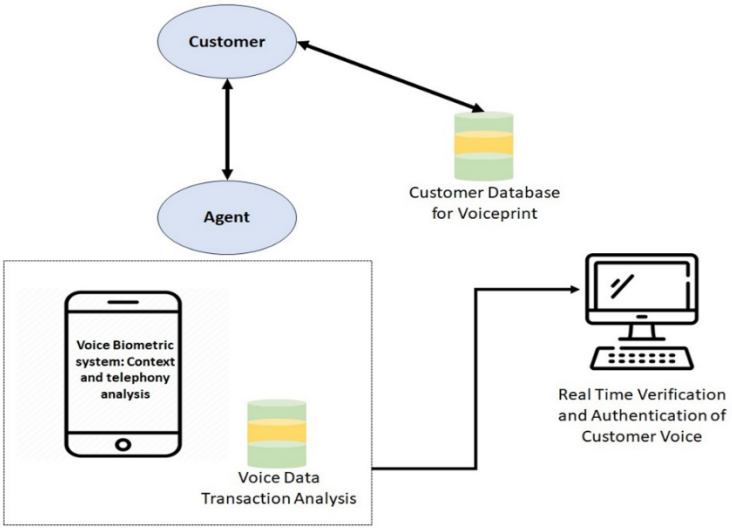

Fig.1. Block diagram represent the voice biometric system in call centres

Preventing Fraud: Voice biometrics authentication effectively identifies fraudsters and serves as a bulwark against account takeovers. The process of enrolling customers' voices and creating encrypted voiceprints bolsters the contact center's security infrastructure. By integrating the system with voice detection software, a high level of accuracy in caller authentication is achieved. The effectiveness of fraud prevention is directly correlated with the enrollment rate, with higher enrollment rates translating to enhanced fraud prevention. For instance, with a yearly enrollment rate of 49%, fraud losses are diminished by approximately 49%.

Enhanced Customer and Agent Experience: Traditional methods of authenticating callers proved arduous and repetitive, leading to customer dissatisfaction. Knowledge-based authentication (KAB) relied on agents posing a series of questions to callers to verify their identity, a process that failed to meet customer expectations for swift issue resolution. The introduction of Voice Biometrics overcomes these challenges, ensuring a consistent and hassle-free customer experience [7]. Agents, in turn, benefit from an improved experience as they are relieved of the burden of determining the authenticity of callers. Real-time notifications provided by voice biometrics further validate the customer's identity. Passive authentication, devoid of the need for questions, empowers agents to focus on addressing customer issues.

Frictionless Experience: Passive, real-time enrollment introduces a seamless authentication process. Voice biometrics verify the caller's identity in real-time during ongoing conversations with agents, comparing the voice to the enrolled voiceprint. This process integrates seamlessly into the flow of conversation, requiring only a few seconds for verification.

Enhanced Security: Traditional authentication methods relied on security questions or PINs; credentials that proved susceptible to compromise. Voice Biometrics introduces a paradigm shift by utilizing a unique voice pattern that is highly resistant to compromise. This level of security transcends attempts by fraudsters to manipulate the system through IVR, mobile apps, or contact centers. The combination of preventive measures positions voice biometric authentication as a robust response to fraud.

Another important aspect is Data security measures for voice biometric systems in call centers which are paramount to safeguarding sensitive customer information and maintaining trust. Firstly, robust encryption protocols must be implemented to protect voiceprints and other biometric data transmitted and stored within the system. This ensures that even if intercepted, the data remains unintelligible to unauthorized parties. Additionally, stringent access controls should be enforced to limit who can view, modify, or access the biometric data, thereby reducing the risk of insider threats or unauthorized access. Regular security audits and penetration testing can help identify vulnerabilities and ensure compliance with industry standards and regulations, such as GDPR or HIPAA, depending on the jurisdiction and industry. Moreover, anonymization techniques can be employed to dissociate voiceprints from personal identifiable information, further enhancing privacy protections. Continuous monitoring and real-time threat detection mechanisms are essential to promptly identify and mitigate any security breaches or suspicious activities. Employee training on security best practices and protocols is also crucial to prevent human error or negligence that could compromise data security. By implementing these comprehensive data security measures, call centers can instill confidence in customers regarding the protection of their biometric information and uphold the integrity of their operations.

In this research article, the process of identity verification of customer through voice biometric system, is illustrated. However, beyond the negative experiences that customers endure, there are broader business implications for companies that entrust user verification to methods such as these. Voice biometrics presents a compelling solution that addresses the complex interplay of security, customer experience, and cost efficiency within the dynamic landscape of call centers. Its ability to provide heightened security, prevent fraud, enhance experiences, and offer a frictionless authentication process underscores its potential as a transformative technology that can reshape customer interactions and bolster the integrity

2. Objective and Implementations

The objective of implementing a voice biometric system in call centers is to enhance security, improve customer experience, and streamline operations. Fig.2. describes a thorough explanation of the actions that must be taken in order to successfully integrate and implement a voice biometric system that is specifically designed for use in contact centres. Each step of the implementation process is carefully outlined in this detailed breakdown, which includes things like system design, purchasing hardware and software, integrating it with the current call centre infrastructure, training staff, and conducting quality assurance testing. Stakeholders can gain a deep understanding of the careful planning and execution required for the smooth integration of voice biometrics into call centre operations by outlining these complex steps in detail. This highlights the system's critical role in bolstering security measures and improving customer service delivery. Voice biometrics technology uses unique vocal characteristics to verify the identity of callers, making it a valuable tool for authentication and identification purposes. Here are the key objectives and steps involved in implementing for present research work:

Improved Security: One of the primary objectives is to enhance the security of call center operations. Voice biometrics can verify that callers are who they claim to be, reducing the risk of unauthorized access and fraudulent activities.

Efficient Authentication: Implementing voice biometrics can streamline the authentication process, making it quicker and more convenient for customers. This can reduce the time spent on security checks and improve the overall customer experience.

Cost Reduction: By automating identity verification using voice biometrics, call centers can reduce the need for manual authentication processes, which can result in cost savings over time.

Fraud Detection: Voice biometrics can also be used for fraud detection. By analyzing voice patterns, the system can identify suspicious behavior or potential fraud attempts in real-time.

Customer Experience: An important objective is to enhance the customer experience by reducing the need for customers to answer numerous security questions. This can lead to quicker and more efficient interactions.

Implementation Steps:

- Assessment and Planning: Begin by conducting a thorough assessment of your call center's needs and objectives. Determine the specific use cases for voice biometrics, such as authentication, fraud prevention, or customer experience enhancement.
- Vendor Selection: Choose a reputable voice biometrics technology vendor. Evaluate different solutions based on factors like accuracy, scalability, integration capabilities, and cost.
- Integration: Integrate the voice biometric system with your call center's existing infrastructure, including customer relationship management (CRM) systems and telephony platforms.
- Enrolment: Customers need to be enrolled in the system by recording their unique voiceprints. This involves collecting voice samples during the normal course of interactions or through dedicated enrollment processes.
- Authentication: Implement voice biometric authentication as part of your call center's verification process. When a customer calls, their voiceprint is compared to the stored voiceprint on file to confirm their identity.
- Monitoring and Continuous Improvement: Regularly monitor the performance of the voice biometric system and fine-tune it to improve accuracy and efficiency. This may involve re-enrollment of customers and updating voiceprint models.
- Compliance: Ensure that your voice biometric system complies with relevant data privacy regulations, such as GDPR or CCPA. Obtain necessary consent from customers for voice data collection and storage.
- Training and Support: Train call center staff to use the voice biometric system effectively and provide support for customers who may have questions or issues with the technology.
- Feedback and Evaluation: Collect feedback from customers and employees to evaluate the impact of the voice biometric system on security, efficiency, and customer satisfaction.
- Scalability: Plan for the scalability of the system as call volumes increase. Ensure that the infrastructure can handle a growing number of voiceprints and authentication requests.

Implementing a voice biometric system in a call center requires careful planning, integration, and ongoing management to achieve the desired objectives of enhanced security, improved customer experience, and operational efficiency.

Fig.2. Steps involved for implementation voice biometric system in call centres

3. Methodology

While companies are required to integrate voice biometric authentication alongside other methods such as liveness detection, this form of biometric security represents a significant enhancement over traditional password and credential-based security measures [8,9]. Voice-recognition biometrics offer greater security compared to passwords and simultaneously enhance data security while eliminating obstacles in the customer experience. Imagine the typical multi-factor login process. Initially, you enter your password, and then the service provider prompts you to respond to a security question or enter a one-time code sent to your mobile device. The reality is that cybercriminals can effortlessly discover personal information online, which can be exploited to guess answers to common security questions like your mother's maiden name or your first street of residence. They can also intercept one-time passcodes or potentially clone your mobile device through SIM card swaps. Additionally, these additional security steps slow down the customer login process and do not address the risk of forgetting, misplacing, or theft of credentials.

Incorporating a voice biometrics solution into the customer authentication process streamlines the customer experience and aligns well with current customer preferences. Consider that 63% of customers contacted service providers last year and favor calling over other customer service channels. Particularly, younger customers are accustomed to issuing voice commands to many of their devices. In the United States, 46% of individuals believe that biometric identifiers have enhanced their lives. Companies are eager to find new ways to create seamless customer experiences that cater to these preferences. Nearly seven out of ten organizations aim to enable digital customer verification and shopping history access without relying on live agents, yet only 38% can currently do so. Therefore, why not make voice recognition the centerpiece of customer-service interactions? Voice biometrics can enhance data security, create a seamless experience, and allow companies to engage with customers in their preferred manner: through conversations.

When companies opt to incorporate speech-based verification methods, they have two primary implementation options: on-device authentication and third-party authentication. Smart devices employ on-device biometric authentication to enable password less sign-ins, often using features like face detection or fingerprint recognition. In the case of voice assistants, devices capture voice patterns and employ them to authenticate user requests. However, on-device authentication may not be suitable for all industries.

In cases where biometric authentication falls short, most mobile devices revert to password or PIN entry, which is easier for criminals to circumvent. Organizations operating in heavily regulated industries such as financial services, which have strict know-your-customer (KYC) requirements, cannot rely solely on on-device authentication. These organizations may instead explore third-party authentication [10]. Third-party biometric authentication offers companies a platform-agnostic speaker-verification solution. In this setup, the third party can be the mobile application or the online customer experience workflow. When a customer logs in using biometric verification, the app or workflow matches the information with a template stored in the cloud. Even if a device is lost or stolen, criminals who gain access to the device won't be able to infiltrate the victim's accounts. Moreover, many third-party solution providers offer companies tailored control over customer enrollment and configuration. With such controls, organizations can also choose to incorporate additional methods alongside voice biometrics to meet their risk tolerance or business needs.

This research presents a methodology for multi-modal password less authentication utilizing face and voice biometrics across various use cases. This study combines sophisticated biometric elements that are extremely difficult

to falsify—namely, face recognition, voice verification, and liveness detection—to reinforce trust in your customers' real-world identities. This approach has the potential to enhance security and customer experience by replacing passwords and one-time passcodes with easily integrated voice biometric authentication in existing platforms and customer workflows. Fig. 3. represents a comprehensive depiction that intricately illustrates the flow, methodology, and execution of integrating voice biometrics within call center environments. This detailed representation offers a thorough examination of the entire process, encompassing the systematic flow of data, the analytical methodologies employed for voice recognition, and the practical implementation strategies utilized within call center settings. By delving into the nuances of each aspect, stakeholders gain valuable insights into the holistic approach required for seamless integration, ensuring effective utilization of voice biometric technology to enhance security, streamline operations, and elevate the overall customer experience within call centers.

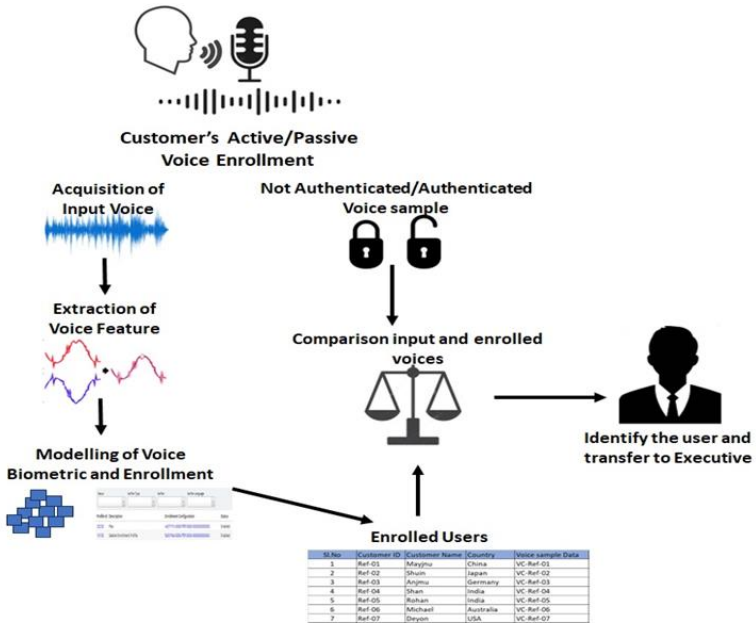

Fig.3. Representation of the flow, methodology and implementation of the voice biometric in call centres

4. Results and Discussion

Applying Biometric System in Call Centers

The integration of voice biometric systems into existing call center technologies poses several significant challenges. One of the foremost hurdles is compatibility with legacy systems, which may lack the necessary infrastructure to support advanced biometric authentication processes. Call centers often rely on outdated software and hardware, necessitating extensive modifications or upgrades to accommodate voice biometrics seamlessly. Additionally, ensuring the security and privacy of sensitive customer data presents another critical concern. Integrating biometric authentication requires robust encryption protocols and stringent access controls to prevent unauthorized access or data breaches. Moreover, the variability in voice quality and environmental factors during phone calls introduces complexities in accurately capturing and verifying voiceprints. This necessitates sophisticated algorithms and continuous training to enhance accuracy and reliability. Furthermore, the cost implications of implementing voice biometric systems, including procurement, installation, and ongoing maintenance, can pose financial constraints for organizations. Addressing these integration challenges demands a strategic approach that prioritizes interoperability, security, accuracy, and cost-effectiveness to realize the full potential of voice biometrics in enhancing call center operations.

What distinguishes the two scenarios depicted in the call centers connectivity? Why did one scenario require nearly 2 minutes to confirm an identity, while the other managed to verify the identity and route the call in just 6 seconds? Is this particular situation a valid use case? The affirmative response to the last query is affirmative. Established companies such as BBVA and Deutsche Telekom are already leveraging the voice biometrics technology to enhance their customer service procedures, rendering them both more secure and expeditious. Veridas' voice biometrics can authenticate an identity with only 3 seconds of spoken language, irrespective of the language or text used. Are these characteristics unparalleled? On their own, no, they are not, but when combined, they are unique. No other entity in the market offers an accuracy rate exceeding 99% along with processing times under 150 milliseconds using just 3 seconds of audio, regardless of language or text—there is no comparable offering.

The application of this technology delivers three advantages that were hitherto thought to be mutually exclusive: prevention of fraud, optimization of costs, and improvement of user experience. We were once compelled to select one of these three drivers for business enhancement, but that is no longer the case.

The suggested and results in this particular study significantly enhance security by transitioning from rigid and easily circumvented security measures to robust ones. Moreover, we achieve substantial cost reductions by reducing processes that, on average, took 60, 90, or even 120 seconds to a mere 3 seconds. The reduction in Time to Market (TMO) is remarkable. Finally, there's the aspect of customer experience. Frankly, our customers choose to partner with us due to the cost savings and the self-evident business case, which they, in turn, can present to their own customers as an enhanced experience, which it truly is.

The present research work describes the usage of voice biometric system in call centres. The call centres generally work with two perspectives, (a) Call centres agents experience and (b) Customer experience. The introduction of the voice biometric system implementation in the call centres effects both agent's and customers behavior and their work. The contemporary call center industry operates in a highly dynamic environment characterized by ever-increasing customer expectations and a relentless pursuit of efficiency. In this landscape, call center agent performance is the linchpin upon which customer satisfaction, operational efficiency, and data security hinge. One technological innovation that has gained significant traction in recent years for optimizing agent performance is the use of voice biometric systems. These systems, leveraging the unique vocal characteristics of individuals, offer a multifaceted approach to improve security, streamline operations, enhance customer experiences, and provide valuable insights for agent training and development.

Voice biometric systems, a subset of biometric authentication technology, harness the distinct vocal attributes of individuals to establish their identities. Unlike traditional methods of identification such as PINs or passwords, voice biometrics offer a non-intrusive, secure, and highly accurate means of verifying an individual's identity. Following parameters such as Voiceprint Creation, voice Enrollment and create database, Voice Verification, and voice Authentication made the work easy for the agents of the call centres. Table 1 followed by Fig. 4, describes how the agents interacted with the system, illuminating their ability to quickly identify and react to authentication prompts, promptly handle alerts from the system, handle call rejections in compliance with established procedures, and effectively handle hold times while awaiting authentication confirmation. In order to improve overall operational efficiency and customer satisfaction levels within the call centre environment, stakeholders can make well-informed decisions and optimize system utilization by clarifying these various aspects, which provide valuable insights into the interaction dynamics between the agents and the voice biometric system.

The database is collected with the survey taken from the people who is working in call centres inbuilt with the biometric system. The questionnaire to the call centres agents was based on their working history and experience facing towards the usage of voice biometric system. According to survey we have found that, the usage of voice biometric authentication, reduced the burden and ease the work of the agent. In average they can attend more customers and solve their problem. In addition to that the time spending on each customer and holding time was drastically reduced. The comfortable towards the hectic call centre job was clearly visible by the collected data. Voice biometric systems have emerged as a game-changer in the call center industry, delivering a myriad of benefits that significantly augment agent performance. From heightened security and streamlined authentication to improved customer experiences and fraud prevention, these systems are a powerful tool in the call center arsenal. Moreover, voice biometrics provide a unique opportunity for continuous agent development through data-driven insights. As organizations increasingly recognize the pivotal role that call center agents play in shaping customer perceptions and driving business outcomes, investments in technologies like voice biometric systems are likely to continue to grow [11, 12]. In an era where data security, efficiency, and exceptional customer experiences are paramount, voice biometric systems have proven themselves to be more than a technological novelty—they are an indispensable tool for elevating call center agent performance to new heights.

Table 1. Voice biometric embedded call centres agent performance analysis

Name	Accept	Alert	Reject	A-Handling Time	Busy %	Hold
Agent-1	12	12	0	00:15:49	0%	20s
Agent-2	10	11	1	00:19:50	30%	15s
Agent-3	5	6	1	00:30:15	55%	55s
Agent-4	8	8	0	00:28:15	40%	50s
Agent-5	11	11	0	00:22:35	0%	20s
Agent-6	12	12	0	00:17:40	0%	25s
Agent-7	13	14	1	00:11:29	0%	22s
Agent-8	11	12	1	00:22:45	0%	25s
Agent-9	10	10	0	00:18:55	0%	10s
Agent-10	9	9	0	00:25:33	25%	35s

Fig.4. Agent Average response towards acceptance, alert, rejection and holding of calls using voice biometric system

Table 2. Customer Experience of connecting to call centers via voice biometric system

	Verification Time	Listening Skill (Rate Out of 10)	Hold Time	Problem Resolution (Rate Out of 10)	Agent Behaviour (Rate Out of 10)
Customer-1	00:00:10	8	20s	7	9
Customer-2	00:00:15	7	15s	9	9
Customer-3	00:00:07	9	55s	10	9
Customer-4	00:00:15	8	50s	10	8
Customer-5	00:00:09	9	20s	9	8
Customer-6	00:00:20	8	25s	8	10
Customer-7	00:00:35	9	22s	10	10
Customer-8	00:00:25	10	25s	10	10
Customer-9	00:00:10	6	10s	9	9
Customer-10	00:00:15	7	35s	9	8

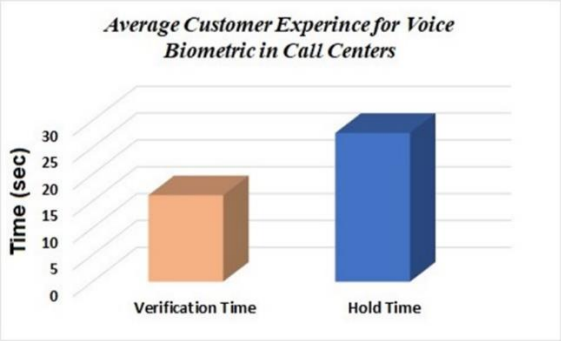

Fig.5. Customer Average response towards acceptance, alert, rejection and holding of calls using voice biometric system

Further study of the work is based on the customer experience of the call centres using voice biometric authentication system. Table 2 and Fig. 5 represents the collective data of the customers gone through the voice biometric system during the Call centres communication. The survey data relies on the customer experience on the basis of faster problem solution. In general customer do not like to wait for the longer for the verification purpose. The voice biometric system has provided them a direct route with minimal hold and wait time for getting the solution for their problem. In the current business climate, customer relationship management (CRM) is becoming into a crucial success component. To increase sales, data mining is being used organizational data warehouses' knowledge. The key to controlling client turnover is identifying the targeting those who are most likely to depart with rewards to stay. As a result, these voices assist marketing decisions help to create marketing campaigns for the appropriate customers. One technology that has gained significant traction in recent years is voice biometrics, a cutting-edge tool employed by call centers to streamline operations and improve security. This write-up explores the impact of voice biometrics on the customer experience within call centers, shedding light on its benefits and potential challenges. In call centers, voice biometrics has been integrated into various processes, such as authentication, fraud prevention, and customer service, to enhance the overall customer experience. Voice biometrics, on the other hand, provides a secure means of verifying a customer's identity by matching their voiceprint with stored data. This not only reduces the risk of unauthorized access but also prevents fraudsters from impersonating legitimate customers [13, 14]. Voice biometrics simplifies the authentication process for customers, eliminating the need to remember passwords or answer security questions. Call center agents can quickly and accurately verify the caller's identity by analyzing their voiceprint, making the customer onboarding process smoother and more efficient. Customers appreciate the convenience of this approach, as it reduces

the time and effort required to access services or resolve issues.

Voice biometrics can also be used to enhance the personalization of customer service. When a customer calls, the system can recognize their voiceprint and access their account information, allowing agents to provide more tailored assistance. This not only saves time but also demonstrates that the company values its customers and their individual preferences. Voice biometrics can be integrated into call routing systems to ensure that customers are directed to the most suitable agent based on their profile and previous interactions [15, 16]. This reduces the need for customers to repeat information and enhances the efficiency of issue resolution. The result is a smoother and more pleasant experience for the caller.

5. Future Perspectives

Every organization handling customer data must prioritize robust data protection and effective data authentication. With continuous technological advancements and the constant influx of innovative solutions in the market, this task may appear deceptively straightforward. However, the ever-evolving landscape of technology, while revolutionizing our world, also presents new opportunities for illicit financial gain through fraudulent activities and cybercrimes [17, 18]. The online and telephonic realms still offer relatively uncomplicated avenues for fraudsters to operate. Furthermore, verifying a customer's identity over the phone can be challenging. How can organizations ensure both customer data protection and a seamless customer experience? This research work focuses towards how voice biometrics, a relatively new yet highly advanced technology, can assist businesses, particularly call centers and contact centers, in authenticating customers and outsmarting fraudsters [19]. Before delving into the details, it's essential to consider one critical aspect: How do call centers currently verify their customers' identities? Typically, the most common method involves using personal information such as name, date of birth, login credentials, and/or phone numbers. But is this the most secure approach? Certainly not. Voice biometric authentication and the utilization of voice biometrics solutions represent the future of contact center authentication The voice management system will function as a virtual customer support agent by identifying the speakers who respond to the questionnaire [20]. This promises enhanced security for customers, an improved customer experience, and advancements in the efficiency of contact center agents. There are certain advantages of the voice biometric system in the call centers such as [21, 22]:

- Enhanced Authentication Security: Voice biometrics solutions provide one of the most secure methods for customers to verify their identities. There is no need for them to disclose personal data over the phone, complete online forms, or answer a series of questions to confirm their identity. Customers utilizing call centers employing voice authentication can rest assured that their data remains secure, impervious to potential fraud or cybercrime attempts.
- Elevated Customer Satisfaction: Each enhancement in the customer interaction process with a call center translates into a noticeable boost in customer satisfaction. Reduced time spent on identity verification, quicker issue resolution, elimination of passwords or login credentials to remember, and decreased fraud risk all contribute to this improvement. It is worth noting that a study reveals that nearly 112 million Americans use voice assistants on a monthly basis, indicating their familiarity with this technology and their rapid adaptability to new voice-powered solutions.
- Robust Omnichannel Customer Experience: Utilizing a unified authentication platform that supports all call center functions can eliminate the need for multiple authentication systems, resulting in cost savings amounting to millions of dollars. Reductions in time and processes translate into substantial economic benefits. Furthermore, employing the same authentication method across various channels enables companies to provide a seamless omnichannel customer experience.
- Contented Agents: Reduced time spent on customer authentication, fewer frustrated customers due to extended wait times, shorter average handling times, and reduced concerns about potential fraud are tangible advantages of voice biometric authentication that simplify and lessen the stress of call center agents' work. Happy agents invariably lead to satisfied customers, don't they?
- Telephone Fraud Detection: Advanced voice biometrics technology not only serves as a means of authenticating customers and confirming their identities but also assists agents in identifying telephone fraud. With a dependable voiceprint and an operational biometrics solution, agents can receive real-time risk assessments for each call they conduct. Armed with this real-time information, they can proactively counteract any illicit activities.
- Decreased Average Handling Times: Thanks to efficient contact center authentication, customers can connect with agents more swiftly compared to traditional identity verification processes. This translates to shorter verification times. Simultaneously, the average handling time—the duration customers spend from initiating a call to resolving their requests—is significantly reduced. Data indicates that businesses can reduce their average handling time by an average of over 30 seconds per call with voice biometric authentication. Additionally, hold times, when customers are temporarily placed on hold, tend to be shorter because agents can accomplish more within less time.

- Enhanced Return on Investment (ROI): As mentioned earlier, voice biometrics enhance call center performance by reducing waiting times, average handling times, and hold times, among other factors. These efficiencies lead to substantial time savings and increased agent productivity. Consequently, improved ROI and revenue growth naturally follow these enhancements. Research has even demonstrated that voice biometrics technology can save companies millions of dollars by reducing verification processes' steps and time by 70-80%.

Future of the voice biometric system is very bright specially in the industrial usage. This technology has a wide range of applications. As previously highlighted and verified from the various survey in this article, one of the most common uses is biometric identity verification. Various companies can leverage voice biometrics to seamlessly confirm the identities of customers, enabling them to provide a multitude of services more efficiently compared to traditional authentication methods. Voice authentication can also serve as a component within a multi-factor identity verification solution. A diverse array of industries can reap substantial benefits from the integration of voice biometric authentication into their daily operations. Those poised to derive the greatest advantages include healthcare, the financial services sector, insurance, utilities, telecommunications, travel and hospitality, and even governmental organizations. Given the increasingly stringent industry regulations and the growing threat of cyber fraud, biometric authentication may indeed represent a highly effective means of combating fraudulent activities.

The adoption of voice biometrics in call centers carries significant implications for the future of privacy and data security. On one hand, it promises enhanced authentication processes, streamlining customer verification and reducing the risk of identity fraud. However, concerns arise regarding the collection and storage of sensitive voice data, raising questions about privacy infringement and the potential for misuse. As call centers increasingly rely on voiceprints for customer identification, robust measures must be implemented to safeguard this data against breaches and unauthorized access. Striking a balance between leveraging the benefits of voice biometrics and ensuring stringent data protection measures will be crucial in maintaining customer trust and upholding privacy standards in the evolving landscape of call center operations.

6. Conclusions

Biometric authentication is the straightforward procedure of confirming an individual's identity by utilizing their distinct characteristics and subsequently granting them access to a service, application, device, or similar. The present research work describes the process of identification and authentication of customer through voice biometric system in call centres. Voice authentication is a technology employing an individual's voice to confirm and authenticate their identity, known for its efficiency and rapid processing of voice patterns. The adoption of such systems is also notably uncomplicated. It's crucial to clarify that voice-based biometric authentication differs from speech recognition technology. Speech recognition technology recognizes spoken words (e.g., in smartphone speech recognition systems) but does not constitute biometric technology. The present research work is based on two important perspectives of the call centres: a. call center agents experience and b. customer experience. The data collected separately from customers and agents for understanding the effective usage of voice biometric system in call centres. The data represented and satisfies the effectiveness of voice biometric system from both the perspectives. From the data it is also cleared that, the implementation of voice biometric system in call centres still have long way to go but will be a major technological change for the industries worldwide.

References

[1] De Keyser, A., Bart, Y., Gu, X., Liu, S. Q., Robinson, S. G., & Kannan, P. K. Opportunities and challenges of using biometrics for business: Developing a research agenda. Journal of Business Research, 136(1): 52-62, 2021.

[2] Rabea Kurdi, Fawzia Hersi, Sara Bahagari, Mohammed Kaosar, S. M. Qaisar, A. Subasi. A Mobile Fingerprint Authentication in Saudi Arabian Call Centers, International Conference on Electrical and Computing Technologies and Applications (ICECTA), 2017

[3] Nuance provides voice biometric technologies for Manulife contact centers, Retrieved November 21, 2015, from http://www.biometricupdate.com/201509/nuance-provides-voicebiometric-technologies-for-manulife-contact-center, 2015.

[4] Ahmad, S. M. S., Ali, B. M., & Adnan, W. A. W. Technical issues and challenges of biometric applications as access control tools of information security. International journal of innovative computing, information and control, 8(11): 7983-7999, 2012.

[5] Kristof Coussement, Dirk Van den Poel. Integrating the voice of customers through call center emails into a decision support system for churn prediction, Information & Management, 45(1):164–174, 2008.

[6] W. Reinartz, V. Kumar. The impact of customer relationship characteristics on profitable lifetime duration, Journal of Marketing, 67(1):77–99, 2003.

[7] S.L. Pan, J.N. Lee. Using e-CRM for a unified view of the customer, Communications of ACM, 46(4):95–99, 2003.

[8] T. Toda, A. Black, and K. Tokuda. Voice conversion based on maximum-likelihood estimation of spectral parameter trajectory, IEEE Transactions on Audio, Speech, and Language Processing, 15(1):2222–2235, 2007.

[9] Andre Kassis, Urs Hengartner. Breaking Security-Critical Voice Authentication, 2023 IEEE Symposium on Security and Privacy (SP), 2023.

[10] H. Abdullah, K. Warren, V. Bindschaedler, N. Papernot, and P. Traynor. The faults in our ASRs: An overview of attacks against automatic speech recognition and speaker identification systems, in IEEE S&P, Oakland, 2020.
[11] Monireh Hosseini, Elnaz Nasirzadeh. Customer identification through voice biometric index at call centers using learning algorithms, International Journal of Economics, Commerce and Management, 3(5):1519-1535, 2015.
[12] Benesty, J., Sondhi, M. M. & Huang, Y. In: Springer Handbook of Speech Processing. s.l.:Springer, 2008.
[13] Jain, A., Hong, L. & Pankanti, S. Biometric Identification. Communications of the ACM, 43(2):90-98, 2000.
[14] Magboub, H. M., Ali, N., Osman, M. A. & Alfandi, S. A. Multimedia speech compression techniques, s.l., IEEE, 9-11, 2011.
[15] Sahoo, S. K., Choubisa, T. & Prasanna, S. M. Multimodal Biometric Person Authentication: A Review. IETE Technical Review, 29(1): 54-75, 2012.
[16] SoonHoo So. An Empirical Analysis on the operational Efficiency of CRM call centers in Korea, International Journal of Computer Science, 7(12):171-178, 2007.
[17] Joaquín González-Rodríguez, Doroteo Torre Toledano & Javier Ortega-García. Handbook of Biometrics, pages 151–170, 2008.
[18] Hicham Atassi; Zdenek Smékal. Automatic identification of successful phone calls in call centers based on dialogue analysis, 5th IEEE Conference on Cognitive Infocommunications (CogInfoCom), Vietri sul Mare, Italy, pages 425-429, 2014.
[19] Andrew Boles; Paul Rad. Voice biometrics: Deep learning-based voiceprint authentication system, 12th System of Systems Engineering Conference (SoSE), Waikoloa, HI, USA, pages 1-6, 2017.
[20] Kao, C. Y., & Chueh, H. E. Voice Response Questionnaire System for Speaker Recognition Using Biometric Authentication Interface. Intelligent Automation & Soft Computing, 35(1), 2023.
[21] Ranjan, Shashi; Mahesh, P. K. Voiceprint Authentication System to Securely Verify and Protect Personal Identity, Grenze International Journal of Engineering & Technology (GIJET), 3(3): 241-243, 2017.
[22] B. Yan, R. Zhang and Z. Yan. VoiceSketch: a Privacy-Preserving Voiceprint Authentication System, IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Wuhan, China, pages 623-630, 2022.

Authors' Profiles

Amjad Hassan Khan M. K. received M.Sc. and M.Phil., from Bangalore University and Vinayaka Mission University respectively. currently pursuing Ph.D. from Srinivas University, Mangalore and working as assistant professor in Department of Electronics, Kristu Jayanti College (Autonomous). He has more than 16 years of teaching experience in Higher Education Institutes. He is member of Board of Examination (BOE) for Higher Education Institutes like Mount Carmel College, Bengaluru, Indian Academy, Bengaluru. His areas of interests are wireless communication systems, High Power devices, Biometrics. His research area is in voice biometrics.

P. S. Aithal obtained M.Sc. in Physics from Mangalore University, India, M.Sc. in E-Business from Manipal University, India, M. Tech. in Information Technology from Karnataka University, India, Ph.D. in Physics from Mangalore University, India, and Ph.D. in Management from Manipal University, India. His major fields of study are the characterization of nonlinear optical materials, optical solutions, e-commerce and mobile business. He has two years postdoctoral research experience at Physical Research Laboratory, Ahmedabad, India and one-year postdoctoral research experience at CREOL, University of Central Florida, USA, in the field of Characterization of nonlinear optical materials. He has about 22 years teaching experience both at UG and PG level in Electronics, Computer Science and Business management. Currently, he is working as PRINCIPAL at Srinivas Institute of Management Studies, Mangalore, India. He has published more than 100 research papers in peer-reviewed journals and two textbooks on physics and Electronics for Engineering students. He has the research interest in Nonlinear optical absorption, Optical Phase Conjugation, Photorefractive materials, business, m-business, ideal business, and nanotechnology business Opportunities. Dr. Aithal is the member of World Productivity Council, U.K., the member of Strategic Management Forum, India, the member of Photonics Society of India, CUSAT, Cochin, senior member of IEDRC.org, Singapore.

How to cite this paper: Amjad Hassan Khan M. K., P. S. Aithal, "Identification of Customer Through Voice Biometric System in Call Centres", International Journal of Intelligent Systems and Applications(IJISA), Vol.16, No.5, pp.68-78, 2024. DOI:10.5815/ijisa.2024.05.06