International Journal of Safety and Security Engineering
Vol. 15, No. 12, December, 2025, pp. 2449-2457
Journal homepage: http://iieta.org/journals/ijsse

Security Enhancements in Cloud-Based Personal Voice Assistants: A Survey and Evaluation of Cryptographic Techniques

K. Winshiny Madonna[1*], Marshiana Devaerakkam[2], L. Nisha Evangelin[3]

[1] Department of Computer Studies, Symbiosis International (Deemed University), Pune 412115, India
[2] Symbiosis Institute of Technology, Pune Campus, Symbiosis International (Deemed University), Pune 412115, India
[3] Department of Computer Science and Engineering, Noorul Islam Centre for Higher Education, Kumaracoil 629180, India

Corresponding Author Email: madonna.win@gmail.com

https://doi.org/10.18280/ijsse.151203

Received: 10 October 2025
Revised: 25 November 2025
Accepted: 22 December 2025
Available online: 31 December 2025

Keywords:
personal voice assistant, cloud-based voice assistants, secure data management, privacy-preserving computation, differential privacy, homomorphic encryption, data privacy

ABSTRACT

The rapid expansion of AI-powered personal voice assistants (PVAs), including Alexa, Siri, and Google Assistant, has significantly transformed human–technology interaction. Despite their convenience, these systems rely heavily on cloud-based processing, which raises serious concerns regarding user privacy and data security. This review investigates vulnerabilities in PVA-cloud architecture, focusing on three critical areas: weak encryption protocols, insecure transmission channels, and insufficient anonymization techniques. To mitigate these risks, this study explores a dual cryptographic strategy that combines differential privacy (DP) with homomorphic encryption (HE). DP protects user identities by adding controlled statistical noise to datasets, while HE enables secure computation on encrypted information without exposing sensitive content. Through a comparative analysis of existing research and cryptographic methodologies, this review identifies significant gaps in the current literature, notably the lack of integrated privacy-preserving frameworks and challenges in achieving real-time system performance. The findings suggest that integrating DP and HE provides a comprehensive, scalable approach to safeguarding user data in cloud-dependent voice assistant platforms.

1. INTRODUCTION

The use of personal voice assistants (PVAs) has increased significantly over the past few years. Voice commands are increasingly popular for controlling smartphones, smart home systems, and vehicles. In the United States, the number of smart speakers, including Amazon Echo and Google Home, has grown by approximately 78%, reaching 118.5 million units, with around 21% of the population owning at least one such device [1]. This trend indicates a growing dependence on PVAs for task execution, information management, and service delivery. However, the rapid adoption of PVAs has also raised serious concerns regarding security and user privacy among consumers, manufacturers, and policymakers, particularly in relation to how user data is collected, processed, and protected [1].

Previous studies analyzing widely used PVAs such as Alexa, Google Assistant, and Cortana have identified several vulnerabilities that may lead to the misuse of sensitive personal information. These vulnerabilities include poor handling of user data, insufficient or absent encryption mechanisms, improper validation of digital certificates, insecure execution of SQL queries, and failure to enforce secure communication protocols such as Secure Sockets Layer (SSL) for data transmission [2]. The presence of issues such as invalid SSL certificates, raw SQL query execution, and weak encryption algorithms is particularly concerning, as these weaknesses may facilitate unauthorized access to user data and increase the risk of privacy breaches [2].

PVAs depend on artificial intelligence techniques to constantly listen for user commands and engage in conversational interactions to complete various tasks. As their popularity continues to grow, understanding the factors prompting PVA adoption has become increasingly important. Addressing operational efficiency, social impact, and perceived risks can help service providers better communicate the benefits of voice assistant technologies and improve user trust in emerging AI-based systems [3].

PVAs regularly transmit large volumes of user data to cloud platforms for processing and storage to fulfil user voice commands [4]. This dependence on cloud infrastructure increases concerns related to data security and privacy, particularly as the collected data often contains sensitive or personally identifiable information. As data volumes increase, the risk of unauthorized access and data breaches also increases, highlighting the need for robust security mechanisms. Cloud services, therefore, play an important role in managing large-scale data efficiently while requiring advanced methods to ensure secure and privacy-preserving data management during processing and storage [5].

This study contributes to existing knowledge by analyzing adoption patterns of PVAs, exposing significant privacy and security weaknesses in mainstream PVA platforms, evaluating the relationship between voice assistants and cloud computing

infrastructure, including inherent risks, and proposing methods to enhance data protection and user trust in AI-based technologies.

2. LITERATURE REVIEW

This literature review categorizes existing research on PVA privacy and security in cloud environments into four main areas: security threats and vulnerabilities, mitigation techniques, AI-based smart assistant privacy challenges, and legal and ethical considerations. Each section concludes with key insights and research gaps relevant to PVAs.

2.1 Security threats and vulnerabilities

Cloud computing offers flexible storage solutions and processing capabilities that allow users to store, retrieve, and manage data efficiently. However, storing data in centralized cloud systems increases the risk of unauthorized access and data breaches [6, 7]. IoT devices and PVAs, which depend heavily on cloud storage, inherit these vulnerabilities. Additionally, attacks such as the GVS-attack allow malicious actors to manipulate voice assistants to send messages, access private information, or control devices remotely [8]. The rapid growth of third-party applications for platforms such as Amazon Alexa and Google Home also introduces new attack surfaces, allowing remote attackers to publish malicious skills [9, 10]. These studies highlight that cloud-dependent PVAs are vulnerable to multiple security threats, including unauthorized access, remote attacks, and vulnerabilities arising from third-party integrations. Mitigating these security concerns is essential for protecting user information.

2.2 Mitigation techniques

Various approaches have been suggested for protecting cloud-based data and IoT networks. Machine learning-based intrusion detection systems (IDS) can identify unusual behavior and potential threats [11]. Multi-layered encryption strategies, combined with one-time passcode authentication, provide additional protection against unauthorized access [12]. Cryptographic solutions, such as Trusted Third-Party Auditor (TPA) models and blockchain-based frameworks such as AuthPrivacyChain ensures data authenticity, distributed access control, and tamper-evidence [13, 14]. Advanced encryption methods, including obfuscation-enhanced elliptic curve cryptography (OB-ECC) and order-preserving symmetric encryption (OPES), can secure sensitive data while minimizing processing delays [15, 16]. Although numerous mitigation strategies exist, integrating these approaches into PVAs remains a challenge, particularly when balancing security, efficiency, and user convenience.

2.3 AI-based smartphone assistance

Voice-activated personal assistants such as Google Assistant, Siri, Alexa, and Cortana depend on natural language processing and machine learning techniques to interpret and respond to user commands [17]. Earlier studies show that consumer adoption of voice-activated digital assistants (VADAs) is strongly influenced by perceived privacy risks, user trust, and concerns about the misuse of personal data [18]. Ongoing security and privacy issues, including information theft, unauthorized voice command execution, and inadequate authentication mechanisms, continue to place user data at risk. Moreover, reinforcement learning and deep learning techniques can enhance the robustness of PVAs by enabling flexible responses to emerging security threats [19, 20]. Although artificial intelligence improves system adaptability and performance, the integration of effective privacy-preserving mechanisms remains essential to maintain user trust and confidence.

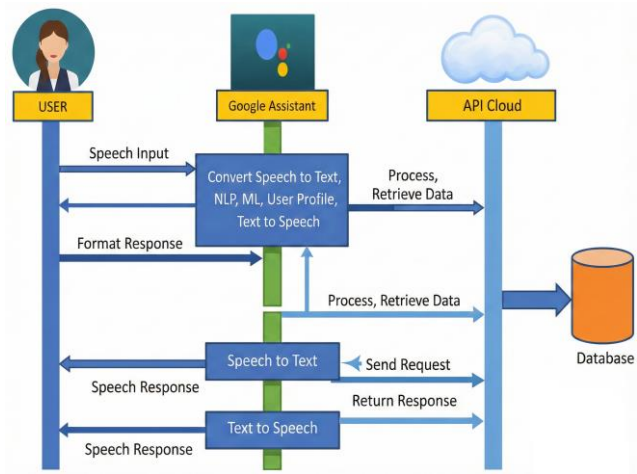

Figure 1. Architecture of a cloud-based personal voice assistant (PVA) workflow

As shown in Figure 1, user voice input is collected and converted into text using speech-to-text modules, followed by natural language processing and machine learning analysis. The processed requests are forwarded to cloud-based APIs for computational tasks, data retrieval, and storage operations. The system then produces a reply, which is converted back into speech using text-to-speech functionality and returned to the user. This architecture highlights how continuous data exchange between the user, AI models, and cloud infrastructure introduces security and privacy challenges, reinforcing the need for privacy-preserving techniques in cloud-based PVA systems.

2.4 Vulnerabilities in smartphone assistance

Malicious actors can exploit unauthorized Android applications, such as Voice Employer, to take control of Google Voice Search for executing commands, spoofing messages, accessing private information, and transferring sensitive data. Vulnerabilities in Google Search enable GVS-attacks to dial contacts even when the device is locked [21].

Current research highlights the lack of adequate authentication mechanisms in VAs such as Amazon Alexa and Google Assistant [22]. The rapid expansion of VA skills has created opportunities for malicious skills, posing critical risks to users interacting with IoT devices [23]. Ethical and privacy challenges in chatbot development, including biases, consent, and transparency, must also be addressed to ensure reliable AI deployment [24]. Privacy and ethical aspects require special attention in educational environments [25], whereas developing legal provisions and regulations may improve personal information security in voice assistant infrastructures [26, 27]. These observations suggest that insufficient user verification and unmonitored third-party skill frameworks represent serious security flaws in smartphone-based voice

assistants, warranting improved security controls.

2.5 Legal, ethical, and regulatory considerations

The collection and transmission of personal data by PVAs introduce significant legal and ethical concerns. Privacy-enhancing technologies (PETs), anonymization mechanisms, and governance frameworks have been proposed to safeguard users' personal information. Ethical challenges, including systematic biases in AI systems, user consent, and transparency in chatbot algorithms, require careful consideration to prevent discriminatory practices and exploitation [28, 29]. Furthermore, emerging laws related to digital services and artificial intelligence are anticipated to enhance data protection standards for PVAs by improving accountability and privacy safeguards [30, 31]. Despite these initiatives, gaps in enforcement practices and technical implementation continue to limit the effectiveness of legal and ethical frameworks in real-world PVA systems.

3. RESEARCH GAPS

3.1 Research gap 1: Integration of privacy-preserving techniques in personal voice assistants

Notwithstanding comprehensive research on privacy risks in PVAs, there is limited clarity on how anonymization and advanced cryptographic techniques can be systematically incorporated into cloud-based PVA architectures. Existing studies primarily discuss privacy threats at a conceptual level, with limited focus on integrated privacy-preserving frameworks that combine anonymization with secure computation mechanisms. Additionally, user-level control over privacy-preserving operations remains underexplored, limiting the practical adoption of such techniques in real-world PVA systems [1].

3.2 Research gap 2: Comprehensive assessment and improved security measures for virtual assistants

Existing literature lacks complete and comparative security and privacy evaluation of virtual assistants across multiple platforms, especially in cloud-dependent environments. Many studies focus on isolated vulnerabilities, while encryption strength, secure data transmission, and authentication mechanisms are not jointly evaluated. Furthermore, limited attention is given to privacy awareness among users and developers, despite its importance in mitigating data exposure and misuse risks [2].

3.3 Research gap 3: Addressing security and privacy challenges of virtual assistants holistically

There is a lack of a comprehensive understanding of how various issues, such as user concerns, malicious attacks, and authentication mechanisms, interact in the context of voice assistant (VA) security and privacy. Existing studies show a limited focus on effectively addressing privacy and security concerns, requiring more comprehensive approaches to mitigate these concerns. Moreover, the dominance of certain VA systems in current research leads to potential bias and overlooks other VA systems that merit investigation [4].

4. RESEARCH QUESTIONS

Question 1: How can anonymization techniques be effectively integrated into current PVA systems?

Question 2: What mechanisms can empower users to exercise control over privacy-preserving techniques in PVAs?

Question 3: To what extent can advances in cryptographic methods improve privacy protection in PVA contexts?

5. PROBLEM STATEMENT

In recent times, the number of people using cloud storage to ensure the security of their data on smartphones has been growing rapidly. This need is felt more strongly in the context of AI-based PVAs intervening as mediators in facilitating the interaction and exploration of users in digital environments. Cloud storage provides numerous benefits to users regarding the scalability and accessibility of cloud storage solutions. At the same time, it also generates significant security and privacy risks. These aspects of security and privacy become major challenges in the context of integrating AI-based PVAs and the cloud storage environment, as it involves the movement of high volumes of data to be processed by these PVA mediators. The major challenge here is how to incorporate these privacy-preserving strategies, like differential privacy (DP) and HE, effectively. DP involves adding randomness to data to obscure the specific data being processed, while HE helps to perform the desired operations without actually decrypting the data. Although these approaches show immense potential to enhance the privacy of data in cloud storage using smartphones, it is a significant challenge to incorporate these PVA systems effectively.

The integration of DP and HE into the PVA systems is not easy it provides several challenges. First, there is a lack of clarity on how to strongly integrate anonymisation techniques into current PVA systems. Although it was discussed that anonymization plays a crucial role in protecting user privacy by making personally identifiable information non-identifiable.

Furthermore, cryptographic methods need to be further developed to improve privacy protection in the PVA system. While HE confirms enabling secure computation with encrypted data, its applicability and effectiveness in PVA systems have yet to be evaluated. Advances in cryptographic methods such as zero-knowledge proofs and secure multi-party computation may have the potential to address privacy concerns in PVA environments.

These difficulties highlight the urgent necessity to close the knowledge gap between privacy-preserving strategies' theoretical advancements and their actual application in PVA systems. To overcome these obstacles, a deep comprehension of the different PVA systems, user conduct, and privacy requirements is necessary. For the further improvement of security in smartphone cloud storage, researchers, developers, and policymakers must work together to create practical solutions. The need to address privacy issues in this field has been underlined by the growing reliance on cloud storage and the widespread usage of AI-based PVAs. Protecting user privacy and enhancing data security in cloud storage settings requires the successful integration of privacy-friendly approaches like DP and HE into PVA systems.

6. STUDY OBJECTIVE AND SCOPE

6.1 Objective

To study how cloud-based PVAs function, including how they collect, transmit, and process voice data. Identify common security and privacy issues, such as weak encryption, unsafe data transmission, and a lack of adequate user data protection. To explore and evaluate voice data protection techniques, including Traditional Encryption, DP, and HE, and propose enhanced, real-time, privacy-focused solutions.

6.2 Scope

Integration of DP and HE in PVA Systems: The research focuses on exploring new approaches to integrate the DP and HE techniques into an existing system. This includes the investigation of architectural implications, algorithmic adaptations, and interface design required for effective integration.

Security Assessment and Examination: This study will examine the successful implementation of DP and HE techniques in enhancing the privacy of the user dataset in a cloud storage system. Both quantitative and qualitative analyses will be conducted to examine the impact of these techniques on privacy preservation, and they will consider factors such as the utility of data, privacy guarantees, and user satisfaction.

Analysis of Computational Burden: An in-depth study of the computational burden created by the integration of DP and HE techniques will be conducted. This includes measuring processing times, resource consumption, and performance degradation to understand the trade-offs between improving data privacy and processing efficiency.

Experimental Approval: The proposed solution will be validated by the experimental studies conducted in real-world scenarios. The experiments will be designed to progress the performance, scalability, and robustness of the integrated DP and HE techniques across diverse use cases and data types commonly encountered in cloud storage environments on smartphones.

Broader Implications: The research will explore the broader implications of integrating DP and HE techniques for solving privacy issues in cloud storage on smartphones. This will include exploring how the proposed solution can contribute its effort and time for the development of more secure and privacy- friendly data management systems, by providing insights into the design and implementation of privacy-friendly systems in the evolving landscape of mobile computing.

7. METHODOLOGY

This research aims to propose and investigate a new approach to enhance privacy in cloud storage on mobile devices, particularly in the context of AI-based PVA. This study is conducted as a systematic review of privacy-preserving techniques in PVAs. The methodology includes the following steps to ensure transparency and reproducibility:

Study selection was based on specific inclusion and exclusion criteria. The review covered peer-reviewed publications in English spanning the timeframe from 2015 to 2025. Studies were considered if they focused on personal or virtual voice assistants and examined mechanisms related to privacy or security. Records that were duplicated, unpublished materials, and articles that were purely descriptive without any technical analysis were excluded.

The review process comprised an initial evaluation of titles and abstracts to assess relevance, followed by a thorough text analysis of chosen studies. For each selected paper, essential information regarding PVA systems, privacy-preserving techniques, cryptographic methods, and assessment strategies was methodically collected. A comparative evaluation was then performed to pinpoint key trends, methodological constraints, and existing research gaps in the literature.

The approach investigates a comprehensive framework that combines DP and HE techniques to strengthen the safeguarding of individuals' sensitive data maintained in server environments on mobile devices. The study evaluates how effectively these techniques minimize confidentiality threats and preserve individual anonymity, accounting for factors like information utility, confidentiality measures, and individual satisfaction. Additionally, the computational costs associated with merging DP and HE techniques, including execution time, resource consumption, and efficiency reduction, are analyzed to understand the practical implications of implementing these techniques. The wider impacts of integrating DP and HE techniques to address confidentiality challenges in server storage on handheld devices are examined, providing valuable insights for designing and deploying privacy-focused platforms in the evolving landscape of mobile technology.

8. ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS

8.1 Secure and efficient data storage and retrieval algorithm

In the untrusted cloud environment, a secure and efficient data storage and retrieval (SEDSR) algorithm offers scalable key management for cloud service providers, content owners, and cloud consumers. For cloud service providers, this approach preserves the trustworthy credential verification procedure. It offers a thorough framework for spotting and stopping harmful activity in an untrusted cloud setting. This approach is committed to avoiding basic difficulties. It provides sufficient and compact security with the best retrieval systems in the cloud by combining the Rivest Shamir Adleman (RSA) algorithm with a symmetric key (SSK) mechanism. To offer increased security and privacy, this method enhances encryption using RSA and a currently disclosed symmetric algorithm. Nevertheless, to provide appropriate solutions for a greater number of sensitive data of different kinds, it requires further improvement [32].

8.2 Triple data encryption standard

By making the keys in the data encryption standard (DES) larger, the triple data encryption standard (TDES) methodology provides a comparatively easier way to secure data privacy and prevent attacks. In comparison to the intelligent framework for healthcare data security (IFHDS) approach, TDES demonstrates shorter encryption and decryption times. It works effectively for large healthcare data in a cloud environment. The input data is divided into three groups according to their significance, and the appropriate

encryption method is applied. For extremely sensitive data, triple encryption is used; for medium-sensitive data, double encryption; and for low-sensitive data, single encryption. Nevertheless, this approach necessitates increased CPU and network consumption [33].

8.3 Attribute-based encryption

Most people agree that the best access control technique for protecting the cloud environment is attribute-based encryption (ABE). To lessen the computing load on the DU, cloud service providers offer decryption outsourcing in addition to data storage. Furthermore, it offers CP-ABE-based fine-grained access control for the DU. It is successful in thwarting selective-attribute plaintext attacks, according to the security study. According to the experimental findings, ABE-DSC had lower computational overhead than the other techniques. For big databases, ABE has a larger overhead and performs worse in integrity checks [34].

8.4 Blowfish algorithm

Blowfish is a symmetric encryption approach that encrypts and decrypts messages using a single key. In addition to giving high-end information privacy during information broadcasting in a dangerous medium, it gives messages greater privacy. This method first verifies the user's identity in order to improve system security. Following authentication, the uploaded data is first divided utilizing a pattern-matching algorithm. The divided data is then encrypted utilizing the Blowfish algorithm (BA). The information is then encrypted and stowed in the cloud at the best possible place. Because the data is cloud-optimised and column-separated, this method is safer and more difficult to hack. This approach is very safe since the user cannot retrieve the document without authentication. The 64-bit result is added to the Blowfish cipher to create a new 64-bit chunk. After that, it copies every value in the p-array and every s-box sequentially [35, 36]. Table 1 represents the review of existing approaches.

Table 1. Review of approaches

Approaches	Benefits	Drawbacks
Genetic algorithm [37]	With just two primary processes, like crossover and mutation, it is straightforward to execute. The GA's unpredictability, which is inspired by nature, optimizes security when data is being uploaded and downloaded to and from the cloud or between the transmitting and receiving ends.	To overcome the problem of memory requirements, the model's space complexity minimization needs to be enhanced.
Enhanced Merkle hash tree [38]	For cloud data security, a multi-owner authentication method combined with an improved Merkle hash tree is employed. User data is encrypted and stored in the cloud using the enhanced Merkle hash tree method algorithm. In response to a user inquiry, a decryption function retrieves the stored data. This encryption structure aids in detecting modifications to the data pertaining to the leaf node, hence enhancing its integrity.	To improve the resilience against different threats, the cloud data storage application incorporates a secure relevant data retrieval method relevant on elliptic curve cryptography that needs to be considered.
Modular encryption standard [39]	Comparing the encryption and decryption processes to various other encryption techniques, the modular arithmetic operations are often faster to compute, especially with current processors. Because MES is easily adjustable for different key sizes, the encryption system grows to meet changing security needs.	Although modular arithmetic offers benefits, properly applying it is challenging; vulnerabilities like the leakage of cryptographic keys or other private data result from poor implementation.

9. PROPOSED FRAMEWORK

This section analyzes the methods of DP and homomorphic encryption (HE) to enhance data protection in cloud-based PVAs.

9.1 Differential privacy

DP aims to protect data by noise injection. Sensitive information is stored in the cloud by users without being discovered by cloud service providers. Noise is added to DP to protect data privacy. Figure 2 represents the DP mechanism.

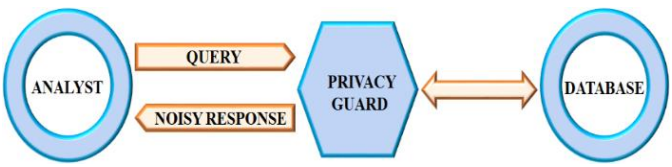

Figure 2. Differential privacy (DP) mechanism

9.1.1 Laplace mechanism

By including a Laplace-distributed noise, the Laplace mechanism in DP protects the privacy of the data. Computation is carried out while maintaining data privacy by utilizing DP. This is attained by adding noise to the data before processing. In this way, the noise is added while maintaining computational accuracy and protecting the privacy of personal data. Calculations using private data are made secure by integrating the Laplace mechanism. Through a Laplace-distributed random contribution, the Laplace mechanism adds unpredictability to the dataset. The Laplace distribution treats adding positive or negative noise with equal chance because of its symmetry [40]. However, the Laplace mechanism is most efficient for low-sensitivity queries.

9.1.2 Gaussian mechanism

One DP technique that is frequently employed to safeguard numerical data is the Gaussian mechanism. To lessen the noise and increase the usefulness of sanitized query results, several variations of the traditional Gaussian technique have been created. The projected accuracy losses of these mechanisms, however, equal the trace of the noise's covariance matrix since all currently available Gaussian processes suffer from the curse of full-rank covariance matrices [41].

9.1.3 Exponential mechanism

Another security-controlled method for ensuring DP in cases when the outputs are not numerical is the exponential technique. The exponential approach, nevertheless, intuitively

ensures that the score function's result is unaffected by the changing of a single DB tuple. When the range of u in the problem's natural parameters is super-polynomially huge, it is not possible to apply the exponential mechanism effectively, even though it describes a complicated distribution over a wide range of domains [42].

9.2 Homomorphic encryption

One kind of encryption that makes it possible to do calculations on ciphertexts without disclosing their plaintext is called HE. Only the owner of the secret key can decrypt the results that have been obtained. HE fixes a lot of privacy and security problems with different apps and technologies. Cloud data protection is one of the many popular real-world uses for HE. Users benefit from the massive processing and storage capacity of an unreliable cloud provider to the power of HE. Both fully homomorphic and partially homomorphic cryptosystems are widely available. Compared to partially HE, the fully homomorphic encryption (FHE) is more secure. Figure 3 reveals the working of the HE technique. The analysis of various HE techniques is depicted in Table 2.

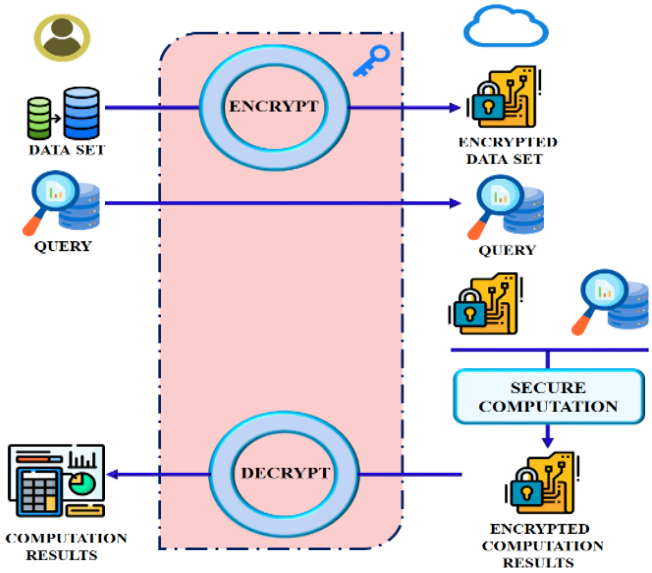

Figure 3. Working of the homomorphic encryption (HE) technique

Table 2. Survey of homomorphic encryption (HE) techniques

Types	Benefits	Drawbacks
Partially HE [43]	By guaranteeing data protection, transaction security, and confidentiality, the developed approach will have a very favourable economic impact by encouraging companies and financial institutions to store their data in the cloud.	Future research is needed to be considered on combining blockchain technology with the developed encryption technique; this would provide a distributed, safe system that improves the general privacy and security of IoT systems.
Somewhat HE [44]	This method has the benefit of sending data in packets, which are then reassembled in the cloud storage device for additional processing. The SHE technique consistently improves the edge device's performance while cutting down on the encryption time dependent on the sensor's input number.	The developed method needs to be improved in the future to satisfy the demands of applications that require quick responses. In order to improve security, the SHE will also be taken into account for Federated Learning applications.
Fully HE [45]	Data is encrypted by the client before being sent to the server, utilising fully HE. The client receives the encrypted processing result after it has been processed by the cloud server.	More than two gigabytes of encryption keys are needed for this procedure, and the encrypted data takes up a lot more storage space than the plain data.

10. RESULTS AND COMPARATIVE ANALYSIS

This section analyses the outcomes reported in existing literature on DP and HE approaches to enhance data protection throughout the data.

Figure 4 represents an analysis of encryption time for TDES and DP–HE-based cryptographic approaches reported in prior studies. As the number of blocks increases, DP–HE-based approaches are observed to outperform TDES with better encryption time. It demonstrates the efficacy and scalability of reported for DP–HE-based approaches when handling large data sets.

The analysis of decryption time for TDES and DP–HE-based approaches reported in prior studies is shown in Figure 5. TDES has a more fluctuating decryption time, while the DP–HE-based approaches have more constant and lower decryption times over all block sizes. It denotes the enhanced stability and efficacy in managing large-scale encrypted data.

Figure 6 illustrates an analysis of running time for TDES and DP–HE-based approaches reported in prior studies. The TDES has a more variable execution time, whereas the developed approach denotes a smoother performance, maintaining a lower running time, indicating reduced computational load, making it more appropriate for PVA applications.

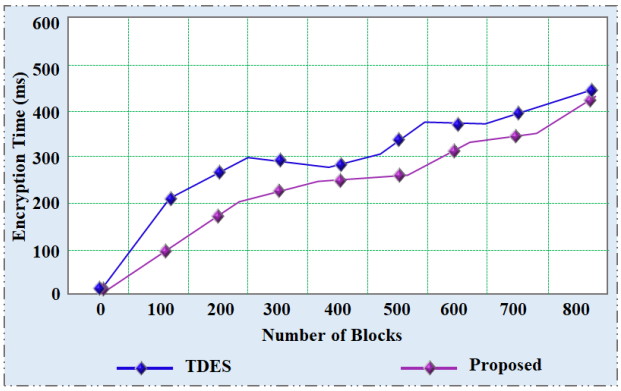

Figure 4. Analysis of encryption time

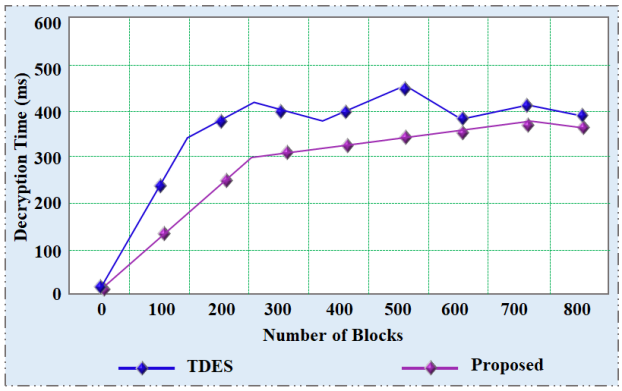

Figure 5. Analysis of decryption time

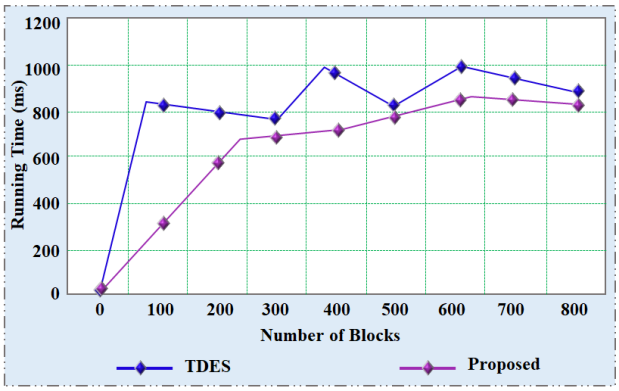

Figure 6. Analysis of running time

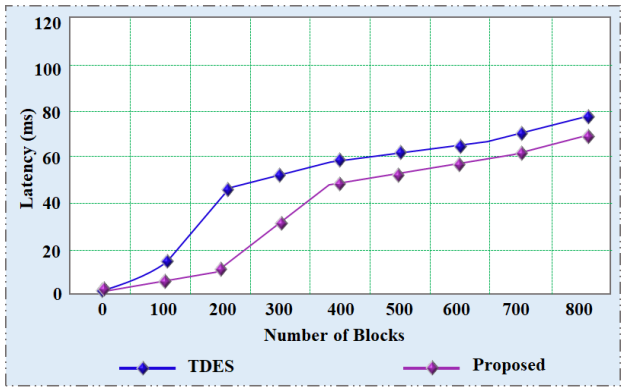

Figure 7. Analysis of throughput

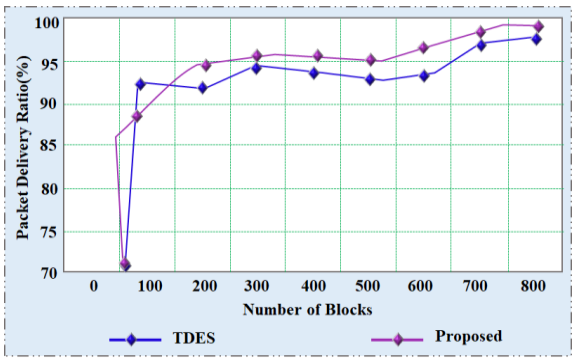

Figure 8. Analysis of packet delivery ratio (PDR)

Table 3. Comparison of network usage

Data Size	TDES (GB)	Proposed Approach
100	0.21	0.20
200	0.29	0.27
300	0.36	0.35
400	0.40	0.39
500	0.55	0.52

Note: TDES = Triple Data Encryption Standard.

Figure 7 displays an analysis of throughput for TDES and DP–HE-based approaches reported in prior studies. The DP–HE-based approaches reliably attain higher throughput values, peaking above 110MBPS, whereas TDES stabilizes around 10 MBPS. The proposed approach handles more data in less time, increasing processing speed and system efficiency.

An analysis of packet delivery ratio (PDR) for TDES and DP–HE-based approaches is revealed in Figure 8. While both approaches have high PDRs, the DP–HE-based approaches steadily provide slightly higher and more stable ratios, particularly beyond 100 blocks. TDES has a dip near 70% at 50 blocks, while the proposed approach maintains better PDR values throughout. This highlights the enhanced reliability and data integrity of the proposed cryptographic approach.

The comparison of network usage for TDES and the proposed approach is presented in Table 3. The proposed approach has better usage of the network than the TDES approach over all data sizes, representing optimal performance in processing sensitive voice data in the cloud environment.

11. LIMITATION

Despite the clear benefits of the DP+HE approaches, several limitations still exist. The combination of DP and HE adds extra processing demands, which can potentially affect the real-time processing in environments with limited resources. There is also a privacy accuracy compromise: increasing DP noise boosts privacy but can slightly lower data accuracy.

Moreover, deploying these techniques in cloud-based PVA applications may need enhanced high-power hardware and careful tuning of parameters to ensure good performance. Tackling these challenges offers opportunities for future work focused on balancing privacy, efficiency, and usability in large-scale deployments.

12. CONCLUSIONS

This study presents a combined privacy-protecting framework for cloud-based PVAs by integrating DP with HE. The evaluation shows that this approach improves data confidentiality and reduces the risk of exposing user identities while keeping performance suitable for real-time processing. Even though challenges like computational overhead and the trade-offs between privacy and utility still exist, the proposed DP+HE model represents a significant step toward better security in PVA-cloud systems. It also highlights important areas for future research focused on increasing efficiency and scalability.

REFERENCES

[1] Cheng, P., Roedig, U. (2022). Personal voice assistant security and privacy—A survey. Proceedings of the IEEE, 110(4): 476-507. https://doi.org/10.1109/JPROC.2022.3153167

[2] Kalhor, B., Das, S. (2023). Evaluating the security and privacy risk postures of virtual assistants. arXiv preprint arXiv:2312.14633. https://doi.org/10.48550/arXiv.2312.14633

[3] Buteau, E., Lee, J. (2021). Hey Alexa, why do we use voice assistants? The driving factors of voice assistant technology use. Communication Research Reports, 38(5): 336-345. https://doi.org/10.1080/08824096.2021.1980380

[4] Bolton, T., Dargahi, T., Belguith, S., Al-Rakhami, M.S., Sodhro, A.H. (2021). On the security and privacy challenges of virtual assistants. Sensors, 21(7): 2312. https://doi.org/10.3390/s21072312

[5] Shapoval, V., Zubyk, L., Zubyk, Y., Kurchenko, O., Kozachok, V. (2024). Automation of data management processes in cloud storage. Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654: 410-418. https://elibrary.kubg.edu.ua/id/eprint/48603.

[6] Akhtar, N., Kerim, B., Perwej, Y., Tiwari, A., Praveen, S. (2021). A comprehensive overview of privacy and data security for cloud storage. International Journal of Scientific Research in Science, Engineering and Technology, 8(5): 113-152. https://doi.org/10.32628/IJSRSET21852

[7] Yang, P., Xiong, N., Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. IEEE Access, 8: 131723-131740. https://doi.org/10.1109/ACCESS.2020.3009876

[8] Diao, W., Liu, X., Zhou, Z., Zhang, K. (2014). Your voice assistant is mine: How to abuse speakers to steal information and control your phone. arXiv preprint arXiv:1407.4923. https://doi.org/10.48550/arXiv.1407.4923

[9] Zhang, N., Mi, X., Feng, X., Wang, X., Tian, Y., Qian, F. (2019). Dangerous skills: Understanding and mitigating security risks of voice-controlled third-party functions on virtual personal assistant systems. In 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, pp. 1381-1396. https://doi.org/10.1109/SP.2019.00016

[10] Zhang, N., Mi, X., Feng, X., Wang, X., Tian, Y., Qian, F. (2018). Understanding and mitigating the security risks of voice-controlled third-party skills on Amazon Alexa and google home. arXiv preprint arXiv: 1805.01525. https://doi.org/10.48550/arXiv.1805.01525

[11] Castro, O.E.L., Deng, X.J., Park, J.H. (2023). Comprehensive survey on AI-based technologies for enhancing IoT privacy and security: Trends, challenges, and solutions. Human-Centric Computing and Information Sciences, 13(39): 1-20. https://hcisj.com/data/file/article/2023080005/13-39.pdf.

[12] Mishra, A., Jabar, T.S., Alzoubi, Y.I., Mishra, K.N. (2023). Enhancing privacy-preserving mechanisms in Cloud storage: A novel conceptual framework. Concurrency and Computation: Practice and Experience, 35(26): e7831. https://doi.org/10.1002/cpe.7831

[13] Kumar, S., Kumar, D., Lamkuche, H.S. (2021). TPA auditing to enhance the privacy and security in cloud systems. Journal of Cyber Security and Mobility, 10(3): 537-568. https://doi.org/10.13052/jcsm2245-1439.1033

[14] Mahalakshmi, J., Reddy, A.M., T., S., Chowdary, B.V., Raju, P.R. (2023). Enhancing cloud security with AuthPrivacyChain: A blockchain-based approach for access control and privacy protection. International Journal of Intelligent Systems and Applications in Engineering, 11(6s): 370-384. https://ijisae.org/index.php/IJISAE/article/view/2863.

[15] NagaRaju, P., Rao, N.N. (2020). OB-MECC: An efficient confidentiality and security enhancement for cloud storage system. Journal of Cyber Security and Mobility, 9(4): 577-600. https://doi.org/10.13052/jcsm2245-1439.944

[16] Mayyahi, M.A.A., Seno, S.A.H. (2022). A Security and privacy aware computing approach to data sharing in cloud environment. Baghdad Science Journal, 19(6(Suppl.)): 1572-1580. https://doi.org/10.21123/bsj.2022.7077

[17] Hoy, M.B. (2018). Alexa, Siri, Cortana, and more: An introduction to voice assistants. Medical Reference Services Quarterly, 37(1): 81-88. https://doi.org/10.1080/02763869.2018.1404391

[18] Vimalkumar, M., Sharma, S.K., Singh, J.B., Dwivedi, Y.K. (2021). 'Okay google, what about my privacy?': User's privacy perceptions and acceptance of voice based digital assistants. Computers in Human Behavior, 120: 106763. https://doi.org/10.1016/j.chb.2021.106763

[19] Li, J., Pan, L., Azghadi, M.R., Ghodosi, H., Zhang, J. (2023). Security and privacy problems in voice assistant applications: A survey. arXiv preprint arXiv: 2304.09486. https://doi.org/10.48550/arXiv.2304.09486

[20] Dhinakaran, D., Sankar, S.M., Selvaraj, D., Raja, S.E. (2024). Privacy-preserving data in IoT-based cloud systems: A comprehensive survey with AI integration. arXiv preprint arXiv:2401.00794. https://doi.org/10.48550/arXiv.2401.00794

[21] Alenizi, B.A., Humayun, M., Jhanjhi, N.Z. (2021). Security and privacy issues in cloud computing. Journal

of Physics: Conference Series, 1979(1): 012038. https://doi.org/10.1088/1742-6596/1979/1/012038
[22] Silva, P., Monteiro, E., Simoes, P. (2021). Privacy in the cloud: A survey of existing solutions and research challenges. IEEE Access, 9: 10473-10497. https://doi.org/10.1109/ACCESS.2021.3049599
[23] Ponomareva, N., Hazimeh, H., Kurakin, A., Xu, Z., et al. (2023). How to DP-fy ML: A practical guide to machine learning with differential privacy. Journal of Artificial Intelligence Research, 77: 1113-1201. https://doi.org/10.1613/jair.1.14649
[24] Hasal, M., Nowaková, J., Ahmed Saghair, K., Abdulla, H., Snášel, V., Ogiela, L. (2021). Chatbots: Security, privacy, data protection, and social aspects. Concurrency and Computation: Practice and Experience, 33(19): e6426. https://doi.org/10.1002/cpe.6426
[25] Terzopoulos, G., Satratzemi, M. (2020). Voice assistants and smart speakers in everyday life and in education. Informatics in Education, 19(3): 473-490. https://doi.org/10.15388/infedu.2020.21
[26] Sartor, G., Lagioia, F. (2020). The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. Publications Office of the European Union. https://doi.org/10.2861/293
[27] Oktavia, T., Agung, C.A., Thalib, D.I., Rahmanda, Y.D. (2023). An empirical study on the factors influencing the attitude and behaviors towards smartphone voice assistant usage. Journal of System and Management Sciences, 13(3): 481-504. https://doi.org/10.33168/JSMS.2023.0333
[28] Zhao, Y., Zhao, J., Yang, M.M., Wang, T., et al. (2020). Local differential privacy-based federated learning for Internet of Things. IEEE Internet of Things Journal, 8(11): 8836-8853. https://doi.org/10.1109/JIOT.2020.3037194
[29] Jarin, I., Eshete, B. (2021). DP-UTIL: Comprehensive utility analysis of differential privacy in machine learning. arXiv preprint arXiv: 2112.12998. https://doi.org/10.48550/arXiv.2112.12998
[30] Olaleye, S.B. (2021). Security of sensitive data on android smartphones using cloud storage with reference to gravitational search algorithm. International Journal of Computer Science and Mobile Computing, 10(3): 72-82. https://doi.org/10.47760/ijcsmc.2021.v10i03.009
[31] Berdasco, A., López, G., Diaz, I., Quesada, L., Guerrero, L.A. (2019). User experience comparison of intelligent personal assistants: Alexa, Google Assistant, Siri and Cortana. Proceedings, 31(1): 51. https://doi.org/10.3390/proceedings2019031051
[32] Elumalai, E., Muruganandam, D. (2024). Secure and efficient data storage with Rivest Shamir Adleman algorithm in cloud environment. Bulletin of Electrical Engineering and Informatics, 13(4): 2659-2667. https://doi.org/10.11591/eei.v13i4.6421
[33] Ramachandra, M.N., Srinivasa Rao, M., Lai, W.C., Parameshachari, B.D., Ananda Babu, J., Hemalatha, K.L. (2022). An efficient and secure big data storage in cloud environment by using triple data encryption standard. Big Data and Cognitive Computing, 6(4): 101. https://doi.org/10.3390/bdcc6040101
[34] Yang, G., Li, P., Xiao, K., He, Y., Xu, G., Wang, C., Chen, X. (2023). An efficient attribute-based encryption scheme with data security classification in the multi-cloud environment. Electronics, 12(20): 4237. https://doi.org/10.3390/electronics12204237
[35] Rao, C., Hiwarkar, T., Kumar, B.S. (2021). Enhanced effective and privacy preserving multi keyword search over encrypted data in cloud storage using blowfish algorithm. Turkish Journal of Computer and Mathematics Education, 12(2): 2845-2853. https://pdfs.semanticscholar.org/b795/9b140835a79d3a983606424e0b2a914a2172.pdf.
[36] Dinesh, E., Ramesh, S.M. (2021). Security aware data transaction using optimized blowfish algorithm in a cloud environment. Journal of Circuits, Systems and Computers, 30(01): 2150004. https://doi.org/10.1142/S0218126621500043
[37] Tahir, M., Sardaraz, M., Mehmood, Z., Muhammad, S. (2021). CryptoGA: A cryptosystem based on genetic algorithm for cloud data security. Cluster Computing, 24(2): 739-752. https://doi.org/10.1007/s10586-020-03157-4
[38] Jayaprakash, J.S., Balasubramanian, K., Sulaiman, R., Parameshachari, B.D., Iwendi, C. (2022). Cloud data encryption and authentication based on enhanced Merkle hash tree method. Computers, Materials & Continua, 72(1): 519. https://doi.org/10.32604/cmc.2022.021269
[39] Shabbir, M., Shabbir, A., Iwendi, C., Javed, A.R., Rizwan, M., Herencsar, N., Lin, J.C.W. (2021). Enhancing security of health information using modular encryption standard in mobile cloud computing. IEEE Access, 9: 8820-8834. https://doi.org/10.1109/ACCESS.2021.3049564
[40] Singh, J., Reddy, A.M., Bande, V., Lakshmanarao, A., Rao, G.S., Samunnisa, K. (2023). Enhancing cloud data privacy with a scalable hybrid approach: HE-DPSMC. Journal of Electrical Systems, 19(4): 350-375. https://doi.org/10.52783/jes.643
[41] Ji, T., Li, P. (2024). Less is more: Revisiting the Gaussian mechanism for differential privacy. In 33rd USENIX Security Symposium (USENIX Security 24), pp. 937-954. https://www.usenix.org/system/files/usenixsecurity24-ji.pdf.
[42] Ju, Q., Xia, R., Li, S., Zhang, X. (2024). Privacy-preserving classification on deep learning with exponential mechanism. International Journal of Computational Intelligence Systems, 17(1): 39. https://doi.org/10.1007/s44196-024-00422-x
[43] Medileh, S., Laouid, A., Hammoudeh, M., Kara, M., Bejaoui, T., Eleyan, A., Al-Khalidi, M. (2023). A multi-key with partially homomorphic encryption scheme for low-end devices ensuring data integrity. Information, 14(5): 263. https://doi.org/10.3390/info14050263
[44] Subramaniyaswamy, V., Jagadeeswari, V., Indragandhi, V., Jhaveri, R.H., Vijayakumar, V., Kotecha, K., Ravi, L. (2022). Somewhat homomorphic encryption: Ring learning with error algorithm for faster encryption of IoT sensor signal-based edge devices. Security and Communication Networks, 2022(1): 2793998. https://doi.org/10.1155/2022/2793998
[45] Ahmed, A.A., Madboly, M.M., Guirguis, S.K. (2023). Securing data transmission and privacy preserving using fully homomorphic encryption. International Journal of Intelligent Engineering & Systems, 16(1). https://doi.org/10.22266/ijies2023.0228.25