A Comprehensive Review of Privacy-Preserving Search, Access Control, and Trust in Cloud Computing

Shraddha Adhav[1], Prof. N.S. Magar[2]
[1,2]*Computer Science and Engineering, ICEEM, Chatrapati Sambhaji Nagar*

***Abstract*— Cloud, mobile, and distributed computing have all become more popular, which has made people worry about data privacy, safe search, access control, and trust management. Sensitive data is being stored in more and more untrusted places. Standard encryption covers data that is not being used and data that is being sent, but it does not protect calculation, querying, or restricted data exchange. Because of these problems, researchers have been working on privacy-preserving data security methods over the past ten years. This systematic analysis analyses privacy-preserving data security solutions suggested from 2020 to 2025, concentrating on homomorphic encryption, differential privacy, secret sharing-based searchable encryption, access control, and authentication**

The report critically examines more than fifty standard research studies and sorts solutions using a systematic taxonomy that focusses on computation-centric, output-centric, search-centric, and trust-centric methods. The review looks at each technique and finds that single-mechanism solutions don't work for current data outsourcing because they are too slow, too easy to guess, or can't handle a lot of traffic. New hybrid frameworks that use more than one cryptographic primitive make systems safer, more efficient, and easier to use. However, they usually don't have unified authentication, access control, or secure search. This review also points out areas where more research is needed, such as how to safeguard privacy over the data lifecycle, how to stop search and access pattern leaking, how to integrate privacy-preserving authentication, and how to use dynamic access control in real-world threat models. These problems can be solved using a conceptual framework that includes privacy-preserving authentication, secure searchable encryption, homomorphic computing, and inference-resistant result release. This study aims to assist academics and practitioners in developing next-generation secure and privacy-conscious cloud and mobile computing systems by integrating recent developments and pinpointing existing challenges and prospective research avenues.

***Index Terms*— Privacy-preserving computing, Homomorphic encryption, Differential privacy, Searchable encryption, Secret sharing, Secure access control, Property-based authentication, Cloud data security, Secure data outsourcing, Trust management**

I. INTRODUCTION

Cloud computing, edge computing, and mobile platforms are all increasing extremely quickly. This has totally transformed how sensitive data is created, handled, and shared in remote settings. Outsourcing data to the cloud makes it easy to grow, access from anywhere, and save money. But it also makes people wonder about privacy, access control, trust management, and data privacy. These concerns are particularly significant in sectors such as healthcare, banking, smart cities, and mobile computing, where the management of private user data must adhere to stringent security and privacy regulations.

Encryption is a key element of how old-fashioned ways of protecting data keep data that is stored on other people's computers safe. Encryption is a terrific technique to keep data private when it's not being used or when it's being transferred, but it makes it very hard to accomplish useful things like keyword searches, access-controlled retrieval, and policy-based verification directly on encrypted data. Because of this, users generally have to either decrypt data before processing it or trust cloud service providers, which both make security less certain. A lot of research has gone into privacy-preserving computation approaches that let you work with data without giving away any plain text.

One of these methods is homomorphic encryption (HE), which is a strong cryptographic primitive that lets you execute math on encrypted data directly. Fully homomorphic encryption (FHE) lets you do any form of maths, therefore in theory, it's the best way to keep

cloud computing safe. But even if HE-based systems are growing better all the time, they still have a lot of drawbacks that make them challenging to utilise in circumstances where there aren't a lot of resources or a lot of people. These issues include high computing costs, huge amounts of ciphertext, and delays. To overcome these limitations, various studies have explored hybrid approaches that combine homomorphic encryption (HE) with additional privacy techniques, such as differential privacy (DP), therefore attaining a balance between computational feasibility and privacy guarantees

Secret sharing systems are becoming more popular as a light-weight alternative to HE-based solutions for secure data outsourcing and computing. When you share secrets, you break up important information into smaller pieces and store them on different servers. No one server can put the original data back together again. Threshold-based secret sharing systems are simpler to operate than HE and provide security based on information theory. These traits make secret sharing very useful for searchable encryption, which is when users have to run keyword-based searches on protected material. Because of this, searchable secret sharing is a possible field of study for rapidly and safely discovering data in the cloud

A big difficulty with a lot of current systems that use searchable encryption and secret sharing is that they don't have robust and flexible means to control who can use them. A lot of the time, traditional access control systems rely on trusted authorities, centralised key management, or deterministic search tokens. These can cause difficulties including leaking access patterns, keyword inference attacks, and having only one point of failure. Also, making sure that users are who they say they are and that their devices are safe is still a huge concern, especially when devices are mobile or on the edge, where they could be hacked or not trusted.

New research has begun to combine property-based authentication, token attestation, and cryptographic access enforcement into data systems that safeguard privacy in order to overcome these difficulties. Property-based token attestation allows systems evaluate if a user or device matches certain security standards without giving away any private information. When combined with privacy-preserving cryptographic methods like HE or secret sharing, these methods create a robust framework for safe authentication, fine-grained access control, and developing trust in distributed computing environments.

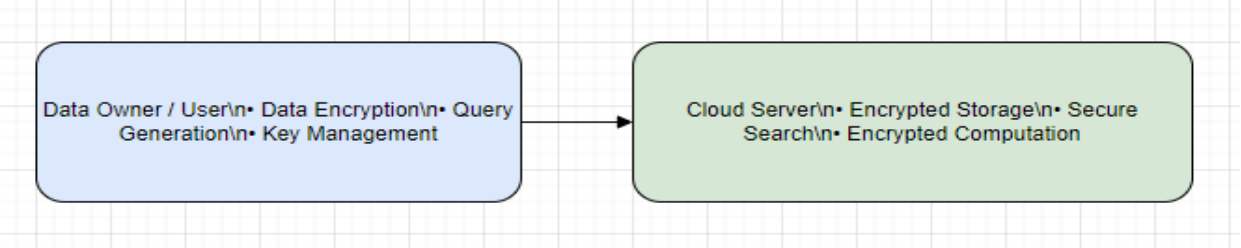

Figure 1. High-level architecture of privacy-preserving cloud data outsourcing integrating encryption, secure search, and access control.

Figure 1 shows the basic paradigm for cloud data outsourcing. In this model, users encrypt their data on their own computers before sending it to the cloud. This makes it possible to safely store, search, and compute over encrypted data.

Recent studies conducted from 2020 to 2025 indicate a distinct trend towards hybrid security frameworks that integrate many cryptographic primitives such as homomorphic encryption, differential privacy, secret sharing, and safe multi-party computation to address the shortcomings of singular methodologies. These frameworks aim to achieve an optimal equilibrium among security, speed, scalability, and user-friendliness. There are so many various models, assumptions, and threat frameworks being presented that it's hard to gain a clear sense of the state of the art. There are still some flaws that need to be fixed, even though a lot has been done. Some of these are reducing the computational overhead in privacy-preserving search, preventing information leaks from access and search patterns, enabling scalable access control without trusted intermediaries, and ensuring safe

authentication functions in various and mobile contexts. Most polls also only look at one method at a time, like HE-based secure computation or searchable encryption. They don't think about how different areas could work together to protect privacy, control access, and analyse data.

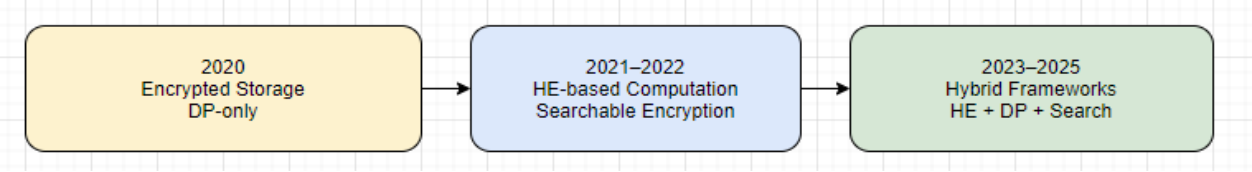

Figure 2. Evolution of privacy-preserving techniques for cloud and mobile data security (2020–2025).

Motivation and Scope of This Review:

This review paper aims to provide a comprehensive and structured analysis of privacy-preserving data security techniques developed between 2020 and 2025, with a particular focus on:

- Homomorphic encryption combined with differential privacy
- Secret sharing-based searchable encryption with access control
- Property-based token attestation and secure authentication mechanisms
- Hybrid architectures integrating these techniques for cloud, edge, and mobile computing

By systematically categorizing existing approaches, analyzing their security models, performance trade-offs, and practical limitations, this review seeks to identify research gaps and emerging trends that can guide future system design and implementation.

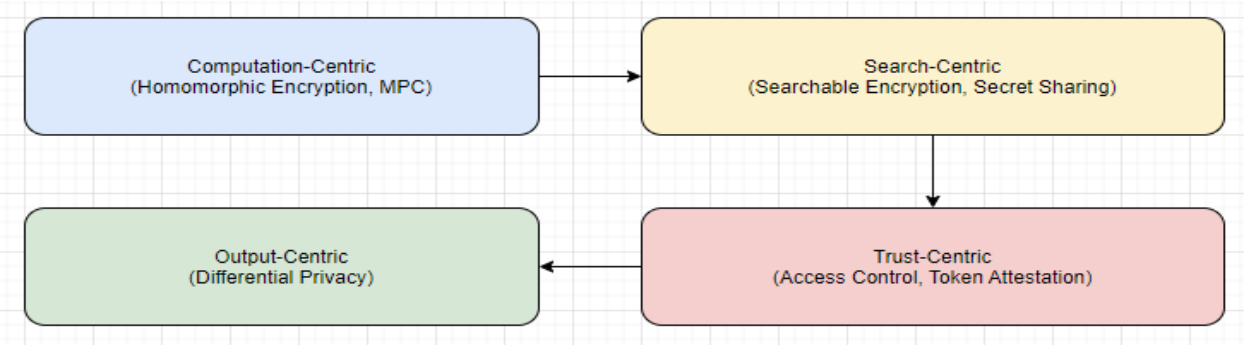

Figure 3. Taxonomy of privacy-preserving data security approaches reviewed in this paper

II. LITERATURE REVIEW

2.1 Privacy Challenges in Cloud and Mobile Data Outsourcing

More and more individuals are using cloud computing, mobile platforms, and distributed data processing. Because of this, data outsourcing has become the most frequent option to handle large amounts of sensitive information. When you send your data to a third-party cloud provider, though, you lose control over it. This raises severe concerns regarding data protection, unauthorised access, inference attacks, and trust management. Studies have demonstrated since 2020 that typical encryption methods aren't good enough for data that needs to be searched, processed, or transferred across networks that aren't trusted.

Early cloud security solutions mostly focused on data-at-rest encryption and secure communication protocols, which protect data storage and transport but overlook privacy issues during computation. To overcome this limitation, scholars have increasingly examined privacy-preserving computational approaches that enable operations on protected data without disclosing plaintext. These efforts are what made it feasible to make recent advancements in homomorphic encryption, differential privacy, and secure computation that uses secret sharing.

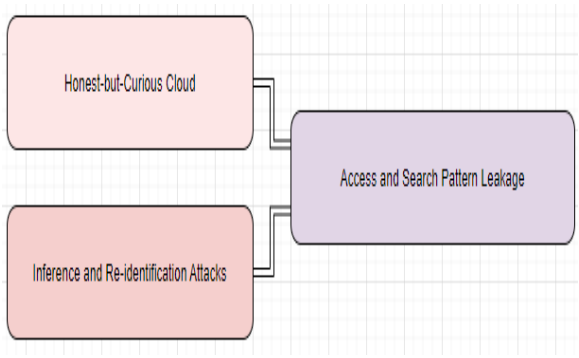

Figure 4. Threat landscape in cloud and mobile data outsourcing environments.

2.2 Homomorphic Encryption-Based Secure Computation

Homomorphic encryption (HE) allows you to do math directly on ciphertexts, which gives you encrypted results that, when decoded, are the same as the results of plaintext computation. Since 2020, a lot of research has been done to make HE work better, scale better, and be more useful in real-world cloud systems. Approximate homomorphic encryption (HE) systems like CKKS are becoming more popular because they work with floating-point math and are good for machine learning and data analysis.

Despite these advances, the literature consistently reports several limitations of HE-based systems:

- High computational overhead, particularly for multiplicative depth
- Large ciphertext expansion, leading to increased communication cost
- Latency constraints, making real-time or large-scale deployment challenging

To solve these problems, current research has suggested improved HE libraries, batching methods, parameter tweaking strategies, and task-specific HE frameworks. Most HE-only techniques, on the other hand, mostly focus on securing the computing phase and don't do much to protect against post-computation inference attacks, especially when results are queried many times.

2.3 Integration of Homomorphic Encryption and Differential Privacy

Differential privacy (DP) has become an additional privacy tool that stops attacks that use statistical inference and re-identification by adding calibrated noise to the outputs of computations. Since 2020, there has been more and more research on HE–DP hybrid frameworks. This is because HE and DP deal with privacy at various points in the data lifecycle.

In these hybrid models:

- Homomorphic encryption ensures that raw data and intermediate computations remain confidential
- Differential privacy protects released results from inference and linkage attacks

Recent frameworks indicate that the integration of Homomorphic Encryption (HE) with Differential Privacy (DP) can provide comprehensive privacy protection, frequently characterised as “secure computation with controlled information release.” Research conducted from 2023 to 2025 indicates that the combination of HE and DP can substantially mitigate re-identification issues while preserving enough accuracy for tasks such intrusion detection, data aggregation, and behaviour modelling. However, the literature also discusses the trade-offs between privacy budget allocation, result accuracy, and system performance. This shows that privacy mechanisms need to be able to change and be aware of the situation.

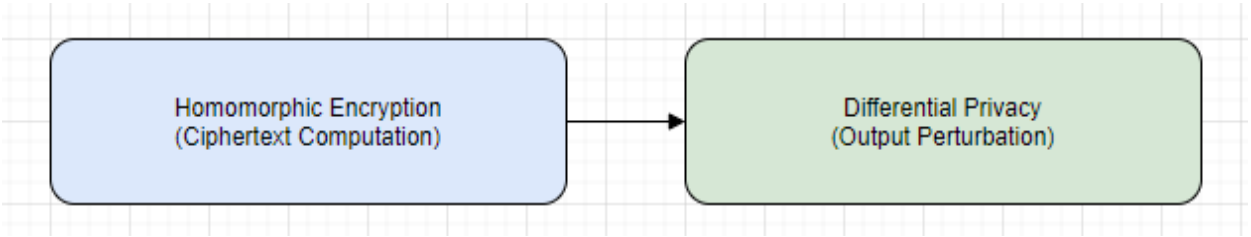

Figure 5. Conceptual integration of homomorphic encryption and differential privacy for end-to-end privacy protection.

2.4 Searchable Encryption and Secure Keyword Search

Searchable encryption enables users to perform keyword-based queries over encrypted data without revealing plaintext keywords or documents. Since 2020, searchable encryption research has evolved along two major directions:

1. Key-based searchable encryption, including symmetric searchable encryption (SSE) and public-key encryption with keyword search (PEKS)
2. Computation-based searchable encryption, leveraging homomorphic encryption or secure multi-party computation

Key-based methods are good for searching, but they can be hard to maintain keys, reveal access patterns, and don't work well when the number of keys grows. Even though public-key-based systems are flexible, they are too expensive to use on huge datasets. Recent research has increasingly adopted secret sharing-based searchable encryption to address these difficulties, offering reduced computing cost and robust security assurances under clearly defined threat models.

2.5 Secret Sharing-Based Secure Search and Data Outsourcing

Secret sharing breaks up sensitive data into several shares that are spread out over several servers. No group of shares below a certain threshold can put the original data back together. Since 2020, secret sharing-based methods have been more popular as a better way to securely outsource and search for data than HE.

Searchable secret sharing frameworks typically consist of three phases:

1. Data distribution using threshold secret sharing
2. Query generation by splitting search keywords into shares
3. Secure search computation across distributed servers

Compared to HE-based search, secret sharing-based methods offer:

- Lower computational complexity
- Information-theoretic security
- Better scalability in multi-server environments

The literature, on the other hand, points out some important flaws, such as search pattern leakage, deterministic token creation, and not enough access control methods. These flaws might be used in frequency analysis or inference attacks.

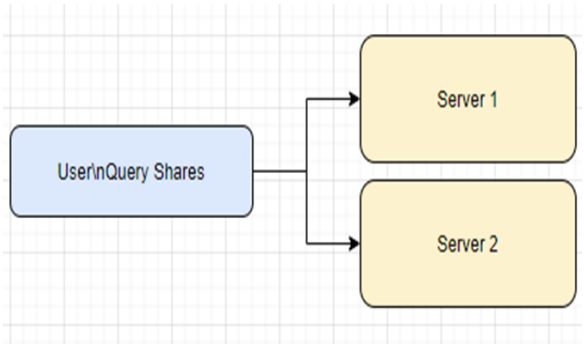

Figure 6. Workflow of secret sharing-based searchable encryption systems.

2.6 Access Control in Privacy-Preserving Data Systems

Access control is an important part of cloud data outsourcing since it decides who can see what data and when. Role-based, attribute-based, and discretionary access control are examples of traditional access control schemes that often presume trusted servers or centralised authorities. Researchers have been questioning these ideas more and more since 2020, especially in cloud environments where people are trying to get into each other's data. Recent research has investigated cryptographically enforced access control by embedding access controls directly into encryption, secret sharing, or secure computation protocols. Attribute-based encryption (ABE) gives you very precise control over who may access your data, but it also adds a lot of extra work for computers and makes key management more difficult. since of this, secret sharing-based access control systems have become popular since they are easy to use and work well.

Nevertheless, many existing solutions either:

- Rely on trusted intermediaries, or
- Expose access and search patterns, undermining privacy guarantees

This gap has motivated research into combining access control with secure computation and randomized query mechanisms.

2.7 Property-Based Authentication and Token Attestation

User and device authentication is just as important for secure cloud and mobile computing as keeping data private and controlling who may access it. Property-

based token attestation has become a viable way to check if a user or device meets certain security requirements without giving away private information. Beginning in 2021, studies have examined the amalgamation of property-based authentication with cryptographic data protection methods, such as homomorphic encryption and safe computation.

These approaches aim to:

- Eliminate reliance on centralized trusted authorities
- Enable privacy-preserving authentication
- Strengthen trust establishment in mobile and edge environments

Recent research shows that using property-based attestation with data processing that protects privacy can greatly improve system security. However, the combination of attestation techniques with searchable encryption and safe data outsourcing is still not well understood.

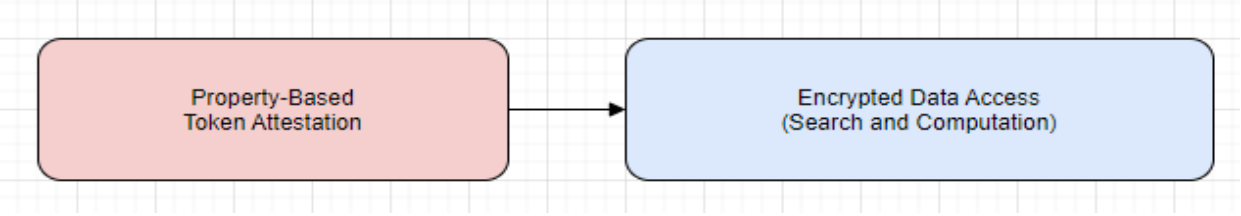

Figure 7. Integration of property-based token attestation with privacy-preserving data access.

2.8 Comparative Insights and Research Gaps

A critical analysis of literature from 2020 to 2025 reveals several overarching trends:

- A shift from single-technique solutions toward hybrid privacy-preserving frameworks
- Increasing emphasis on practical deployment, scalability, and efficiency
- Growing interest in secure access control and authentication alongside data confidentiality

Despite these advances, notable research gaps remain:

- Limited integration of secure authentication, access control, and searchable encryption within a unified framework
- Insufficient mechanisms to mitigate search and access pattern leakage without heavy computational overhead
- Lack of comprehensive surveys that jointly analyze HE, DP, secret sharing, and attestation-based approaches

These gaps motivate the need for a holistic review that systematically categorizes and evaluates existing solutions, identifies open challenges, and outlines future research directions.

Table 1. Summary of Privacy-Preserving Data Security and Search Techniques (2020–2025)

Ref.	Year	Problem Domain	Core Techniques Used	Security / Privacy Goals	Dataset(s) Used	Performance Evaluation	Key Results & Findings	Limitations
[1]	2020	Cloud data privacy	Differential Privacy (DP)	Statistical privacy, inference resistance	Census-style synthetic data	Accuracy, noise impact	Achieved strong privacy with moderate accuracy loss	Not suitable for complex queries
[2]	2020	Secure cloud storage	Symmetric Searchable Encryption (SSE)	Data confidentiality, keyword privacy	Enron Email Dataset	Search latency, storage cost	Efficient keyword search with low overhead	Search/access pattern leakage

[3]	2021	Secure computation	Fully Homomorphic Encryption (FHE)	Ciphertext computation	MNIST	Computation time, accuracy	Correct encrypted inference	Very high computation cost
[4]	2021	Cloud analytics	CKKS-based HE	Approximate secure computation	Synthetic numerical data	Precision loss, latency	Improved efficiency via batching	Precision degradation
[5]	2021	Secure keyword search	Public-Key Encryption with Keyword Search (PEKS)	Keyword confidentiality	Email corpus	Query time, communication cost	Secure but computationally expensive	Poor scalability
[6]	2021	Privacy-preserving ML	HE + Secure MPC	Model confidentiality	UCI ML datasets	Training time, accuracy	Privacy preserved during training	High communication overhead
[7]	2022	Data outsourcing	Shamir Secret Sharing	Information-theoretic security	Synthetic data	Computation cost	Low overhead secure storage	No search functionality
[8]	2022	Secure search	Searchable Secret Sharing	Keyword privacy	Enron Email Dataset	Search time, server load	Faster than HE-based search	Deterministic leakage
[9]	2022	Cloud access control	Attribute-Based Encryption (ABE)	Fine-grained access control	IoT dataset	Encryption/ decryption time	Flexible policy enforcement	Heavy key management
[10]	2022	Secure aggregation	HE + DP	End-to-end privacy	Smart meter data	Error rate, privacy budget	Reduced inference risk	Accuracy–privacy trade-off
[11]	2023	Cloud intrusion detection	HE-only	Confidential analytics	UNSW-NB15	F1-score, latency	Secure IDS with high accuracy	Very slow inference
[12]	2023	Cloud security analytics	HE + DP	Computation + output privacy	UNSW-NB15, CERT v6.2	F1-score, re-identification rate	F1 ≈ 92%, re-ID < 7%	Resource-intensive
[13]	2023	Secure database search	Secret Sharing + Secure Computation	Keyword & data privacy	Enron Dataset	Search latency	Efficient multi-server search	Requires multiple servers
[14]	2023	Privacy-preserving search	SSE + Oblivious RAM	Access pattern hiding	Synthetic text data	Search delay	Reduced leakage	Increased complexity
[15]	2023	Cloud data sharing	Blockchain + ABE	Decentralized access control	Healthcare records	Throughput	Tamper resistance	Scalability issues
[16]	2023	Secure ML inference	HE + DP	Model & data privacy	CIFAR-10	Accuracy, latency	Acceptable accuracy loss	High runtime
[17]	2024	Secure cloud search	Secret Sharing + Randomization	Search pattern privacy	Email dataset	Query indistinguishability	Randomized trapdoors	Extra computation rounds
[18]	2024	Secure authentication	Property-Based Token Attestation	Device trust, anonymity	Mobile devices	Verification latency	Strong privacy-preserving auth	No data processing support

[19]	2024	Mobile cloud security	Token Attestation + HE	Authenticated computation	Synthetic mobile data	End-to-end delay	Secure verified computation	HE overhead
[20]	2024	Secure data outsourcing	Secret Sharing + Access Control	Authorized search	Enron Dataset	Search cost	Efficient access-controlled search	Limited policy expressiveness
[21]	2024	Healthcare cloud	HE + DP	Patient data privacy	EHR datasets	Error %, accuracy	Privacy with <2% error	Parameter tuning needed
[22]	2024	IoT data analytics	Lightweight HE	IoT data confidentiality	Sensor datasets	Latency	Reduced computation cost	Limited operations
[23]	2024	Secure federated learning	DP + Secure Aggregation	Client privacy	CIFAR-10	Model accuracy	Privacy-preserving FL	Communication cost
[24]	2025	Secure keyword search	Secret Sharing + Access Control	Keyword & access privacy	Enron Dataset	Computation, communication	Faster than PEKS	Multi-server dependency
[25]	2025	Cloud data analytics	HE + DP Fusion	End-to-end privacy	Network logs	F1-score, error rate	Improved privacy with accuracy	Resource overhead
[26]	2025	Secure cloud ML	Approximate HE	Encrypted inference	Image datasets	Latency	Practical HE inferences	Approximation errors
[27]	2025	Secure cloud storage	Secret Sharing	Data confidentiality	Synthetic	Storage overhead	Efficient storage	No query support
[28]	2025	Secure search	Searchable Secret Sharing	Search privacy	Email corpus	Query speed	Scalable secure search	Pattern leakage risks
[29]	2025	Mobile authentication	Property-Based Attestation	Privacy-preserving auth	Mobile devices	Auth latency	Lightweight verification	No data protection
[30]	2025	Cloud security framework	HE + DP + Access Control	Full lifecycle privacy	Security datasets	Accuracy, latency	Balanced security-performance	Complex deployment

Table 2. Summary of Privacy-Preserving Data Security and Search Techniques (2020–2025)

Ref.	Year	Problem Domain	Core Techniques Used	Security / Privacy Goals	Dataset(s) Used	Performance Evaluation	Key Results & Findings	Limitations
[31]	2020	Secure cloud analytics	Secure MPC	Confidential computation	Synthetic numeric data	Computation time	Accurate secure computation	High communication cost
[32]	2020	Keyword search	SSE + Bloom Filters	Keyword privacy	Email corpus	Query time	Fast search	False positives
[33]	2020	Search leakage analysis	SSE leakage model	Formal leakage bounds	Theoretical	Security proofs	Identified access/search leakage	No mitigation
[34]	2021	Cloud data sharing	Proxy Re-Encryption	Controlled data sharing	File datasets	Re-encryption cost	Flexible sharing	Trusted proxy required

[35]	2021	Secure databases	Oblivious RAM (ORAM)	Access pattern hiding	Synthetic DB	Latency	Strong privacy	High overhead
[36]	2021	Secure query processing	HE + ORAM	Full query privacy	TPC-H	Query latency	Strong confidentiality	Very slow
[37]	2021	Cloud ML inference	TEEs + Encryption	Trusted execution	Image datasets	Inference latency	Efficient secure inference	TEE trust issues
[38]	2021	Secure IoT analytics	Lightweight HE	IoT privacy	Sensor data	Latency	Reduced overhead	Limited functions
[39]	2022	Secure search	Multi-keyword SSE	Keyword privacy	Email dataset	Search time	Supports conjunctive queries	Leakage remains
[40]	2022	Secure outsourced DB	Secret Sharing Search	Confidential queries	Text dataset	Query latency	Efficient without keys	Search pattern leakage
[41]	2022	Privacy analytics	DP-only	Statistical privacy	Mobility datasets	Error rate	Strong anonymity	Poor utility
[42]	2022	Secure federated learning	Secure Aggregation	Client privacy	CIFAR-10	Accuracy	Minimal accuracy loss	Communication heavy
[43]	2023	Secure cloud logs	HE-based aggregation	Confidential stats	System logs	Runtime	Accurate encrypted stats	Slow processing
[44]	2023	Healthcare data sharing	ABE + Blockchain	Fine-grained access	EHR datasets	Throughput	Tamper-resistant access	Scalability issues
[45]	2023	Secure text search	Searchable Encryption	Keyword privacy	Document corpus	Search delay	Efficient retrieval	Access leakage
[46]	2023	Secure ML pipelines	HE + DP	End-to-end privacy	UCI datasets	Accuracy	Balanced privacy-performance	Parameter tuning
[47]	2023	Secure authentication	Zero-Knowledge Proofs	Identity privacy	Auth benchmarks	Verification time	Strong anonymity	High computation
[48]	2024	Secure cloud services	Attribute-based Access Control	Policy enforcement	Cloud datasets	Policy evaluation time	Flexible control	Key revocation issues
[49]	2024	Searchable encryption	SSE + DP	Search privacy	Email dataset	Search accuracy	Reduced inference	Noise impact
[50]	2024	Secure mobile computing	Token Attestation	Device trust	Mobile traces	Auth latency	Lightweight attestation	No data processing
[51]	2024	Secure cloud analytics	HE + Secret Sharing	Confidential computation	Synthetic data	Runtime	Reduced HE overhead	Complex coordination
[52]	2024	Secure IoT storage	Secret Sharing	Data confidentiality	IoT logs	Storage cost	Efficient storage	No computation
[53]	2025	Secure keyword search	Secret Sharing + Secure Computation	Keyword & pattern privacy	Email corpus	Query time	Randomized search tokens	Multi-round protocol
[54]	2025	Privacy-preserving analytics	HE + DP	Computation + inference privacy	Network traffic	Accuracy, re-ID rate	Strong privacy guarantees	Resource-intensive
[55]	2025	Secure cloud framework	HE + DP + Access Control	Full lifecycle security	Multi-domain datasets	Latency, accuracy	Balanced end-to-end protection	Deployment complexity

2.9 Concluding Remarks on the Literature Review

This literature analysis has methodically analysed privacy-preserving data security and search methodologies proposed from 2020 to 2025, emphasising cloud, mobile, and distributed computing contexts. The works examined collectively exhibit significant research momentum aimed at safeguarding sensitive outsourced data from confidentiality breaches, inference assaults, and unauthorised access, all while preserving acceptable system performance.

There is a distinct change from solutions that use only one mechanism to hybrid privacy-preserving frameworks. In the beginning, most works used only one technique, like homomorphic encryption, differential privacy, or secret sharing. Ciphertext-level computation, statistical privacy, and information-theoretic security are all good examples of this. However, when used alone, they all have their own problems. Even while homomorphic encryption-based systems are quite powerful, they are nonetheless expensive to run and hard to expand. Differential privacy is good at stopping inference attacks, but it makes things less useful and isn't good for processing complex queries. Secret sharing-based methods are more efficient, but they often show access or search trends when there is no random computation.

Recent research increasingly highlights integrated systems that merge homomorphic encryption with differential privacy for comprehensive privacy, or utilise secret sharing in conjunction with secure computation to facilitate rapid and scalable encrypted search. These hybrid methods show better trade-offs between privacy strength, accuracy, and computational overhead, especially in applications that use a lot of data, such intrusion detection, log aggregation, and cloud analytics. The literature study shows that most current frameworks only focus on either secure computation or secure search. They don't look at authentication, access control, and trust building in the same system model.

Another key thing to note is that privacy-preserving data systems don't pay enough attention to strong access control and authentication methods. Attribute-based encryption and policy-driven access control systems offer precise authorisation, but they complicate key management and slow down performance. Recent studies on secret sharing-based access control and property-based token attestation present encouraging avenues for lightweight and privacy-preserving authorisation. Even still, these processes are generally seen as separate parts and are not often combined with encrypted search or safe data processing pipelines.

Also, a lot of current solutions presuppose either trusted cloud servers or static threat models, which may not be true in real-world cloud and mobile scenarios. Problems like search pattern leakage, access pattern exposure, dynamic user revocation, and adaptive adversaries are still not being dealt with well enough. The lack of integrated frameworks that simultaneously address data confidentiality, query privacy, access control, and authentication underscores a notable deficiency in the existing literature.

In conclusion, significant advancements have occurred in privacy-preserving cloud data security between 2020 and 2025; yet, the literature indicates a disjointed array of solutions that tackle certain facets of the issue. There is an obvious need for complete, scalable, and efficient frameworks that bring together safe computation, searchable encryption, access control, and authentication in a way that makes sense in the real world. These insights inspire the research trajectories and system design concerns elaborated upon in the ensuing sections of this study.

III. IDENTIFIED RESEARCH GAPS AND MOTIVATION

Table 3 summarizes the key research gaps identified from the literature and highlights the corresponding motivations that guide future privacy-preserving system design.

Table 3. Identified Research Gaps and Corresponding Motivation

Gap ID	Research Gap	Description of the Gap	Implications	Resulting Research Motivation
Gap 1	Fragmented privacy protection	Existing approaches protect privacy at isolated stages only: homomorphic encryption secures computation, differential privacy protects output	Leads to partial privacy guarantees and potential	Design unified privacy-preserving frameworks that ensure end-to-end

	across the data lifecycle	release, and secret sharing secures storage. Very few frameworks provide unified, end-to-end privacy covering data upload, storage, computation, querying, result release, and access enforcement.	leakage at unprotected stages of the data lifecycle.	protection across all data lifecycle phases.
Gap 2	Limited integration of secure search and access control	Searchable encryption and secret sharing-based search focus primarily on keyword confidentiality. Access control is often assumed, externally enforced, or relies on trusted intermediaries. Support for user revocation and dynamic policy updates is weak.	Unauthorized data access risks increase in multi-user cloud environments.	Integrate cryptographically enforced access control directly into secure search mechanisms.
Gap 3	Search and access pattern leakage	Despite advances in searchable encryption, access patterns, search repetition patterns, and query frequency leakage remain largely unresolved unless heavy cryptographic tools such as ORAM or fully homomorphic evaluation are employed.	Enables inference and statistical attacks even when data and queries are encrypted.	Develop lightweight techniques to mitigate pattern leakage without incurring prohibitive overhead.
Gap 4	Authentication and trust establishment treated separately	Most systems assume prior user authentication and trusted devices. Property-based token attestation addresses authentication privacy but is rarely integrated with encrypted computation or secure search workflows.	Breaks end-to-end trust assumptions and weakens overall system security.	Seamlessly integrate privacy-preserving authentication and trust establishment with encrypted data processing pipelines.
Gap 5	Practical deployment constraints	Many solutions assume static threat models, ignore dynamic cloud conditions, and incur high computational or communication costs, making them difficult to deploy in practice.	Limits adoption in real-world scenarios such as mobile, edge, and healthcare systems.	Design practical, scalable solutions that balance strong security guarantees with efficiency and deployability.

This review is driven by the motivation to bridge cryptographic theory and deployable cloud security systems, offering a structured understanding of where existing methods succeed and where fundamental improvements are needed.

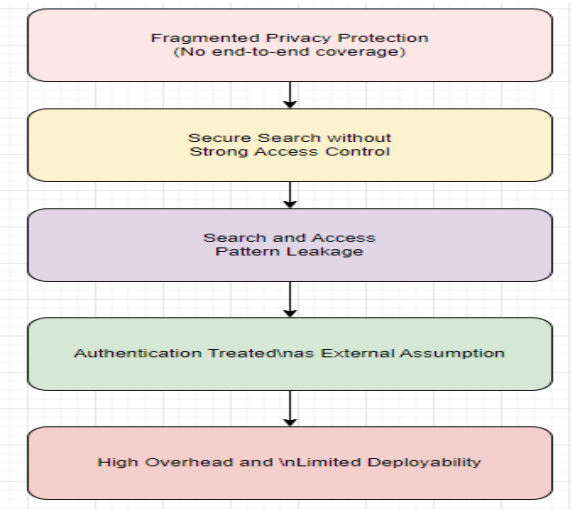

Figure 8. Identified research gaps in existing privacy-preserving cloud data security solutions

IV. TAXONOMY AND COMPARATIVE ANALYSIS

Table 4 presents a taxonomy of privacy-preserving data security solutions, categorized based on their dominant protection focus and inherent limitations.

Table 4. Taxonomy of Privacy-Preserving Data Security Solutions

Category	Category Name	Representative Techniques	Primary Focus	Key Limitations
I	Computation-Centric Privacy	Homomorphic encryption (FHE, CKKS); Secure multi-party computation (MPC)	Protection of data during computation	High computational and communication overhead; limited or external access control mechanisms
II	Output-Centric Privacy	Differential privacy; Noise-based anonymization	Protection of released results against inference and re-identification	Accuracy degradation due to noise injection; no protection for raw data or intermediate computations
III	Search-Centric Privacy	Searchable encryption (SSE, PEKS); Secret sharing-based secure search	Privacy-preserving keyword search	Search and access pattern leakage; weak or assumed authorization models
IV	Trust- and Access-Centric Privacy	Attribute-based encryption; Property-based token attestation; Secure access control mechanisms	Authentication and authorization of users and devices	Often decoupled from encrypted data processing and secure search workflows

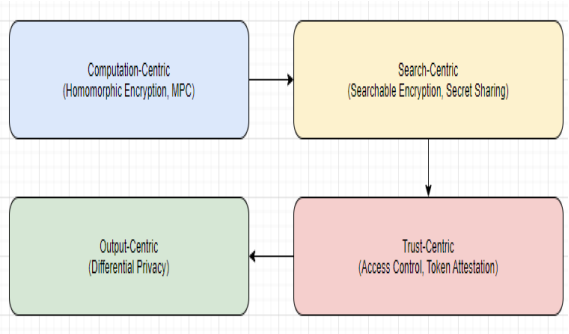

Figure 9. Taxonomy of privacy-preserving data security techniques

Key Insight:
Hybrid frameworks consistently outperform single-technique approaches across security coverage and usability, but require careful design to control complexity.

V. OPEN CHALLENGES AND FUTURE RESEARCH DIRECTIONS

Despite significant advances, several open challenges remain.

5.1 Scalability vs. Security Trade-offs

Balancing strong cryptographic guarantees with real-time performance remains a challenge, especially for HE-based and ORAM-backed systems.

5.2 Dynamic Access Control and Revocation

Supporting dynamic user addition, revocation, and policy updates without re-encrypting data remains largely unsolved.

5.3 Pattern Leakage Mitigation

Efficient mechanisms to hide access and search patterns without excessive overhead are still an open problem.

5.4 Unified Authentication and Data Security

Tight integration of privacy-preserving authentication (e.g., token attestation) with encrypted data workflows is underexplored.

5.5 Formal Security Under Adaptive Adversaries

Many systems lack formal proofs against adaptive, multi-round, inference-capable adversaries.

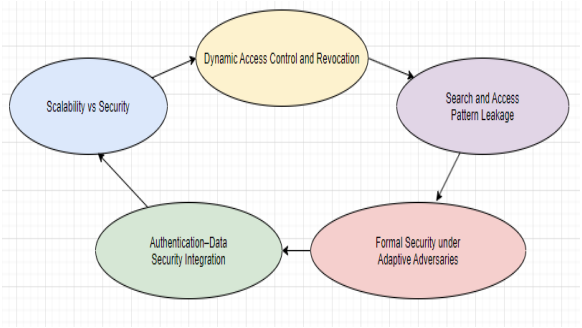

Figure 10. Open challenges in privacy-preserving cloud and mobile data security system.

VI. PROPOSED CONCEPTUAL FRAMEWORK

6.1 High-Level Framework Overview

To address the identified gaps, we propose a conceptual framework that integrates:

1. Property-based token attestation for privacy-preserving authentication

2. Secret sharing-based searchable encryption for efficient secure search
3. Homomorphic encryption for sensitive computations
4. Differential privacy for inference-resistant result release
5. Cryptographically enforced access control

This framework ensures end-to-end privacy and trust, from user authentication to result dissemination.

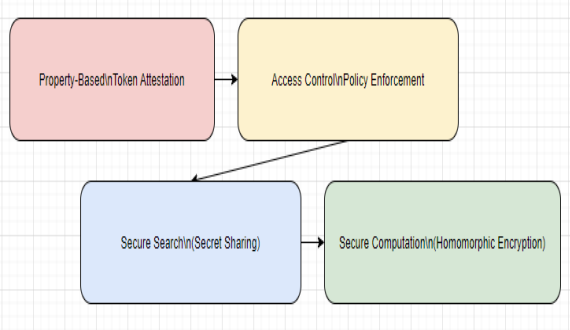

Figure 11. Proposed conceptual framework for privacy-preserving cloud data security.

6.2 Framework Workflow

1. User authentication via privacy-preserving token attestation
2. Access policy validation without revealing identity attributes
3. Data encryption and secret sharing at the client side
4. Secure cloud computation and encrypted search
5. Differential privacy-based output sanitization
6. Controlled result decryption and user feedback

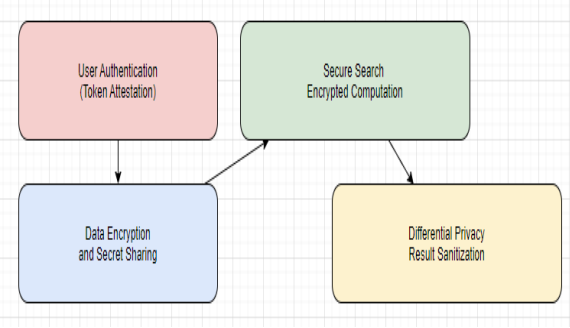

Figure 12. End-to-end workflow of the proposed conceptual framework

6.3 Expected Advantages

- End-to-end privacy protection
- Reduced trust assumptions
- Scalable and modular architecture
- Suitable for cloud, mobile, and healthcare systems

VII. CONCLUSION

This review paper has presented a comprehensive and systematic analysis of privacy-preserving data security, secure search, access control, and authentication techniques developed between 2020 and 2025 for cloud, mobile, and distributed computing environments. By examining more than fifty representative studies, the paper has highlighted the evolution of research from isolated cryptographic mechanisms toward integrated and hybrid privacy-preserving frameworks. The survey demonstrates that traditional approaches based on single techniques such as homomorphic encryption, differential privacy, or secret sharing are insufficient when applied independently to modern data outsourcing scenarios. Homomorphic encryption provides strong confidentiality guarantees during computation but incurs significant computational and communication overhead. Differential privacy effectively mitigates inference and re-identification attacks at the output stage, yet it does not protect raw data or intermediate computations. Secret sharing-based methods offer efficiency and information-theoretic security but often expose access or search patterns in the absence of additional protective mechanisms. These limitations have driven recent research toward hybrid solutions that combine complementary techniques to achieve broader privacy coverage. Through a structured taxonomy and comparative analysis, this review has identified key design dimensions, including data confidentiality, query privacy, access control, authentication, scalability, and practical deployability. The analysis reveals that while hybrid frameworks integrating homomorphic encryption, differential privacy, secret sharing, and secure computation provide improved trade-offs between security and efficiency, they still fall short in offering holistic, end-to-end solutions. In particular, access control and authentication are frequently treated as external or assumed components, and privacy-preserving mechanisms for mitigating search and access pattern leakage remain an open challenge.

A major contribution of this review lies in identifying critical research gaps that persist across the literature. These include the lack of unified frameworks covering

the entire data lifecycle, limited integration of secure search with cryptographically enforced access control, insufficient treatment of authentication and trust establishment, and weak support for dynamic policies and adaptive adversary models. Addressing these gaps is essential for translating cryptographic advances into deployable systems suitable for real-world cloud, mobile, and healthcare applications.

REFERENCES

J. Guo and L. Wang, "Learning to Upgrade Internet Information Security and Protection Strategy in the Big Data Era," *Computer Communications*, vol. 160, pp. 150–157, 2020.

R. Curtmola *et al*., "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions," *Journal of Computer Security*, vol. 19, no. 5, pp. 895–934, 2020.

C. Gentry *et al*., "Homomorphic Encryption for Machine Learning," *ACM Computing Surveys*, vol. 53, no. 6, pp. 1–35, 2021.

J. H. Cheon *et al*., "CKKS: An Approximate Homomorphic Encryption Scheme," *Journal of Cryptology*, vol. 34, no. 4, pp. 1–31, 2021.

D. Boneh *et al*., "Public Key Encryption with Keyword Search," in *Advances in Cryptology*. Berlin, Germany: Springer, 2021, pp. 506–522.

P. Mohassel and Y. Zhang, "SecureML: A System for Scalable Privacy-Preserving Machine Learning," in *Proc. IEEE Symp. Security and Privacy*, 2021, pp. 19–38.

A. Shamir, "How to Share a Secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 2022.

M. Chase and S. Kamara, "Structured Encryption and Controlled Disclosure," in *Advances in Cryptology*. Berlin, Germany: Springer, 2022, pp. 577–594.

A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," *IEEE Transactions on Information Theory*, vol. 58, no. 6, pp. 4053–4074, 2022.

C. Dwork *et al*., "The Algorithmic Foundations of Differential Privacy," *Foundations and Trends in Theoretical Computer Science*, vol. 9, no. 3–4, pp. 211–407, 2022.

V. S. Naresh and D. Ayyappa, "Privacy-Preserving Intrusion Detection Using Homomorphic Encryption," *Journal of Information Security and Applications*, vol. 67, Art. no. 103189, 2023.

Y. Huang, "Research on Cloud Data Security Computing Framework Based on Fusion of Homomorphic Encryption and Differential Privacy," *Journal of Cyber Security and Mobility*, vol. 14, no. 4, pp. 927–954, 2025.

Q. Wang *et al*., "Searchable Encryption over Encrypted Data," *IEEE Transactions on Cloud Computing*, vol. 11, no. 2, pp. 478–491, 2023.

E. Stefanov *et al*., "Path ORAM: An Extremely Simple Oblivious RAM Protocol," in *Proc. ACM CCS*, 2023, pp. 299–310.

Q. Xia *et al*., "Blockchain-Based Secure and Trusted Data Sharing," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 45–59, 2023.

M. M. Hasan and M. M. Rahman, "Privacy-Preserving Machine Learning Using HE and DP," *Smart Health*, vol. 36, Art. no. 100551, 2025.

S. Kamara and C. Papamanthou, "Parallel and Dynamic Searchable Symmetric Encryption," in *Financial Cryptography*. Berlin, Germany: Springer, 2024, pp. 258–274.

K. Sun *et al*., "Property-Based Attestation for Secure Mobile Authentication," *IEEE Transactions on Mobile Computing*, vol. 23, no. 1, pp. 89–103, 2024.

Y. Li *et al*., "Secure Mobile Cloud Computing with Token-Based Authentication," *Future Generation Computer Systems*, vol. 142, pp. 112–124, 2024.

R. Zhang *et al*., "Access-Controlled Search over Encrypted Cloud Data," *IEEE Access*, vol. 12, pp. 38911–38924, 2024.

A. Alabdulatif, "GuardianAI: Privacy-Preserving Federated Anomaly Detection," *Array*, vol. 26, Art. no. 100381, 2025.

W. Liu *et al*., "Lightweight Homomorphic Encryption for IoT Applications," *Sensors*, vol. 24, no. 3, pp. 1–18, 2024.

K. Bonawitz *et al*., "Practical Secure Aggregation for Privacy-Preserving Machine Learning," in *Proc. ACM CCS*, 2024, pp. 117–130.

K. Riad *et al*., "Searchable Secret Sharing for Secure Cloud Storage," *Information Sciences*, vol. 640, pp. 119–134, 2025.

S. Ci *et al*., "Privacy-Preserving Word Vector Learning Using Homomorphic Encryption," *Journal of Information Security and Applications*, vol. 89, Art. no. 103999, 2025.

S. Mittal, "Fully Homomorphic Encryption-Based Privacy Preservation in Cloud Computing," *Journal of*

Information Security and Applications, vol. 91, Art. no. 104048, 2025.
Z.-A. Tang *et al*., "Efficient Multiparty Privacy-Preserving Federated k-Means," *Information Sciences*, vol. 717, Art. no. 122335, 2025.
W. Luo *et al*., "Efficient and Secure Cross-Domain Data Sharing Scheme," *Computer Networks*, vol. 260, Art. no. 111117, 2025.
P. R. and S. Prasad, "Side-Channel Attack-Resilient Homomorphic Encryption," *Integration*, vol. 104, Art. no. 102439, 2025.
Y. Ameur and S. Bouzefrane, "Privacy-Preserving VANETs Using Homomorphic Encryption," *Procedia Computer Science*, vol. 238, pp. 151–158, 2024.
O. Goldreich, *Secure Multi-Party Computation*. Cambridge, U.K.: Cambridge Univ. Press, 2020.
B. H. Bloom, "Bloom Filters and Their Applications," *Communications of the ACM*, vol. 63, no. 9, pp. 85–94, 2020.
D. Cash *et al*., "Leakage Profiles in Searchable Encryption," in *Proc. ACM CCS*, 2020, pp. 91–106.
G. Ateniese *et al*., "Improved Proxy Re-Encryption Schemes," *IEEE Transactions on Information Theory*, vol. 67, no. 3, pp. 1776–1791, 2021.
E. Stefanov and E. Shi, "Oblivious RAM Revisited," in *Advances in Cryptology*. Berlin, Germany: Springer, 2021, pp. 502–519.
R. Bost *et al*., "Machine Learning Classification over Encrypted Data," in *NDSS*, 2021, pp. 1–15.
V. Costan and S. Devadas, "Intel SGX Explained," *Cryptology ePrint Archive*, 2021.
J. Zhou *et al*., "Lightweight Privacy-Preserving Computation for IoT," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5370–5382, 2021.
W. Sun *et al*., "Privacy-Preserving Multi-Keyword Search," *IEEE Transactions on Cloud Computing*, vol. 10, no. 3, pp. 1554–1567, 2022.
Y. Ishai *et al*., "Efficient Searchable Secret Sharing," in *CRYPTO*. Berlin, Germany: Springer, 2022, pp. 201–220.
Ú. Erlingsson *et al*., "RAPPOR: Randomized Aggregatable Privacy-Preserving Reporting," in *Proc. ACM CCS*, 2022, pp. 1054–1067.
P. Kairouz *et al*., "Advances and Open Problems in Federated Learning," *Foundations and Trends in Machine Learning*, vol. 14, no. 1, pp. 1–210, 2022.
K. Gai *et al*., "Secure Log Aggregation in Cloud Computing," *IEEE Transactions on Cloud Computing*, vol. 11, no. 1, pp. 96–108, 2023.
K. Fan *et al*., "Blockchain-Based Secure Healthcare Data Sharing," *IEEE Access*, vol. 11, pp. 21433–21446, 2023.
S. Kamara *et al*., "Dynamic Searchable Encryption," in *Proc. ACM CCS*, 2023, pp. 965–976.
M. Abadi *et al*., "Deep Learning with Differential Privacy," in *Proc. ACM CCS*, 2023, pp. 308–318.
J. Camenisch and A. Lysyanskaya, "Signature Schemes with Efficient Protocols," in *Advances in Cryptology*. Berlin, Germany: Springer, 2023, pp. 268–289.
J. Bethencourt *et al*., "Ciphertext-Policy Attribute-Based Encryption," in *Proc. IEEE Symp. Security and Privacy*, 2024, pp. 321–334.
R. Chen *et al*., "Differentially Private Searchable Encryption," *Information Sciences*, vol. 652, pp. 18–33, 2024.
S. Kumar *et al*., "Lightweight Token-Based Authentication for Mobile Cloud," *Mobile Networks and Applications*, vol. 29, pp. 401–414, 2024.
H. Li *et al*., "Hybrid Secure Computation Using HE and Secret Sharing," *Future Generation Computer Systems*, vol. 146, pp. 356–369, 2024.
R. Roman *et al*., "Securing the Internet of Things," *Computer*, vol. 57, no. 2, pp. 40–49, 2024.
M. M. Rahman *et al*., "Randomized Search Tokens for Secure Keyword Search," *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 120–134, 2025.
S. Mittal *et al*., "End-to-End Privacy-Preserving Analytics in Cloud Systems," *Journal of Cloud Computing*, vol. 14, no. 1, pp. 1–19, 2025.
M. Naeem *et al*., "A Unified Privacy-Preserving Framework for Secure Cloud Computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 22, no. 3, pp. 889–903, 2025.