|| Volume 2|| Issue 6 || December 2017 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

Biometric-Based Secure Data Transmission in Cloud Computing: A Comprehensive Review of Techniques, Algorithms, and Security Frameworks

Pradeep Kundlik Deshmukh

Associate Professor, Department of Computer Engineering,

Government College of Engineering, Awasari - Kh, Pune, Maharashtra, India pkdeshmukh9@gmail.com

---

Abstract: Cloud computing has become a paradigm shift which allows ubiquitous, on demand access to shared computers. Nevertheless, the delegation of sensitive data to remote clouds servers attracts deep concerns on the data confidentiality, user authentication, access control and privacy protection. Another aspect that has been gaining momentum as a measure to strengthen security on the cloud is biometric based authentication because it intrinsically has the element of uniqueness and non-repudiation. The paper offers a general survey of the biometric-based secure data transmission methods that have been invented in recent decade, including fingerprint based privacy-preserving data transmission protocols, attribute-based encryption (ABE) schemes, identity-based encryption (IBE) schemes with revocation support, and public auditing schemes to ensure integrity of cloud data. We conduct a systematic survey of the cryptographic primitives such as homomorphic encryption, garbled circuits, ciphertext-policy ABE and convergent key management and examine how they can be applied to the cloud security space. The table of the structured literature, the description of algorithms, and a multi-dimensional comparative analysis have been presented. The paper has found continuing shortcomings in existing methods, which consist of high-computational cost, absence of biometric fit jointly, and restricted revocation services, and describes a hybrid IBEABEFingerprint architecture as a fusion path. The review is a compilation of available sources on cloud security, data privacy, and biometric authentication by researchers and practitioners.

Keywords: *Biometric Authentication, Cloud Security, Attribute-Based Encryption, Identity-Based Encryption, Privacy-Preserving Protocols, Homomorphic Encryption, Secure Data Transmission, Public Key Infrastructure, Fingerprint Recognition, Access Control*

I. INTRODUCTION

Cloud computing has undergone a fast shift in becoming a fledgling idea to the essential infrastructure of the present digital ecosystems. Both businesses and academic institutions, as well as individuals, use cloud platforms to store, process, and transmit enormous amounts of data. The various paradigms, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are all indicative of not local computation but rather virtualised resources that are controlled remotely. These models, in spite of their economic and operational merits, change the parameters of trust that have traditionally been used to govern data security.

The historical context of storing data on a physical medium and ensuring its physical security is no longer applicable when the data owner entrusts a third-party cloud service provider (CSP) with physical custody of data. They can attack the cloud itself, abuse poorly set up access policies, or intercept data during transit. Besides, even the well-intentional yet compromised CSP can be considered a threat to the privacy of users. Such fears are magnified in areas where data sensitivity takes centre stage like in the healthcare sector, finance, defence and personal communications.

Authentication, which is the assurance of the identity of an entity, is the initial defence in any security architecture. The classical password-based authentication has been negatively known to have many weaknesses: passwords can be stolen, guessed, or forgotten. Multi factor authentication enhances strength at the expense of usability. Biometric authentication uses physiological or behavioural attributes of fingerprints, iris patterns, facial geometry, voice, etc. which are intuitively hard to duplicate or transmit. Bio-metrics, combined with cloud security systems, hold a bright future of authenticating at the highest level of security and ease.

Nevertheless, the biometric data is sensitive in itself. Biometric templates are not changeable in case of compromise as opposed to passwords. Information storage and transmission of biometric data on or in cloud infrastructure must be treated with unparalleled caution then requiring cryptographic measures that maintain biometric privacy and simultaneously do not interfere with biometric matching utility. Biometric authentication and cloud security intersect, and thereby, create a fertile and difficult research area.

Coupled with the authentication problem is the cloud security environment, which has issues of checking over data integrity (making sure that the data stored has not been distorted in any way), fine-grained access control

(figure out who can access what data and under what circumstances), efficient key management (distributing keys and revoking keys in a cloud-scale environment), and searchable encryption (being able to query encrypted data without de-encryption). All these sub-problems have received a deep amount of research and interplay is even more complex.

The paper provides a detailed overview of methods and frameworks created to cope with these interconnected problems with special reference to literature written by researchers. We consider biometric privacy protecting protocols, attribute-based encryption (ABE) variations, identity-based encryption (IBE) and revocation, public auditing schemes and convergent key management approaches. Through a synthesis of the findings in these fields, we will present a unified source to researchers and practitioners that will clarify the state of the art, reveal the limitations, and offer directions in which further research is to proceed.

The rest of this paper is structured in the following way. Section II includes a critical review of the literature related, which is supplemented with a table of structured summary. Section III outlines the important algorithms and techniques found in the literature. Section IV provides a comparative study of the examined schemes in several evaluation dimensions. Section V gives a synthesis discussion and the paper is closed by the observations over open challenges and future research directions in Section VI.

II. LITERATURE REVIEW

The references to biometric security and cloud data protection include a series of strands that overlap each other in many ways. This review is arranged into four major topics (A) Biometric Privacy-Preserving Authentication, (B) Attribute-Based Encryption and Access Control, (C) Identity-Based Encryption and Key Management, and (D) Cloud Data Integrity and Public Auditing. In both places, we discuss groundbreaking and exemplary works in this decade.

A. Biometric Privacy-Preserving Authentication

One of the most problematic issues in the development of cloud services was recognized to be the privacy of the biometric data in the clouds. One of the earliest homomorphic encryption (HE)-based privacy-preserving fingerprint authentication protocols was suggested by Barni et al. [1]. Their scheme uses the FingerCode representation - a fixed length feature-vector, obtained using images of the fingerprints, that facilitates any efficient matching within the encrypted domain. The protocol is based on a multi-party computation model so that the server and the client are not informed about the biometric data of the other party. The authors were able to show that the biometric representation (in terms of Finger Codes) allowed maintaining the computational cost of HE operations at a practical level.

Hei and Du [2] discussed biometric security in another respect of securing implantable medical devices (IMDs). Their 2-level secure control access system relies on simple physiology (level one) and full recognition of the iris (level two) to identify caregivers wishing to communicate with IMDs. This hierarchy of security provides a balance between the strength of security and the latency of the IMD energy constraints and the emergency response needs. As the protocol recorded near-zero false rejection rates, as well as, false acceptance rates, it proved to be a viable protocol. Nevertheless, the scheme was intended to be used in the context of the IMD and cannot be extended to a cloud data access case easily.

Huang et al. [3] have established effective protocols of privacy-saving biometric identification via the application of garbled circuits, a method of cryptography in which two parties co-process a function without displaying their individual input. Instead of dealing with the easier verification problem, the authors dealt with the identification problem, which is which enrolled identity a query biometric is a part of. They proposed a new backtracking protocol to enable effective oblivious data retrieval, which uses 824 less bandwidth than previously seen. Their use in matching fingerprints showed that garbled circuit based biometric identification was practically feasible.

B. Attribute-Based Encryption and Access Control

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) was developed by Bethencourt, Sahai, and Waters [4] in 2007 and is a milestone in the encrypted data access control, since it provides finer access control. In CP-ABE, the data is ciphertext with an access policy provided as a Boolean formula on the attributes, and the decryption key of a user provides a coding of his or her attribute set. The attempt to decrypt is successful provided that the attributes of the user meet the policy. CP-ABE is conceptually similar to role-based access control (RBAC) but directly works with ciphertext, which is appropriate when using the untrusted cloud server model.

Later developments were developed using CP-ABE to mitigate its main shortcomings: decryption time is proportional to policy complexity, and the original system lacks user attribute privacy. An anonymous ABE scheme was suggested by Zhang et al. [5], in which the attribute information is hidden in the ciphertexts. They proposed a match-then-decrypt form of paradigm where a lightweight matching step is used to find out without decryption whether a key of a user meets the policy in the ciphertext. This drastically limits the unneeded decryption attempts in mobile cloud environments, whereby the computational capacities are limited.

Li et al. [6] dealt with the issue of computing decryption with ABE outsourcing. Their protocol allows users to route the computationally expensive part of the decryption process to the cloud server, and get back a decrypted ciphertext (partially) that needs a minor final step. A checkability mechanism was added to make sure that the delegation is conducted honestly by the server. Individually, Hahn, Changhee, et al. [7] suggested an attribute-based data-sharing scheme that is optimised to share data with mobile users who have limited resources without impacting the online traffic by computing encryption parameters offline.

C. Identity-Based Encryption and Key Management

- Boneh and Franklin introduced identity-based encryption (IBE), which streamlines the construction of a public key infrastructure by allowing arbitrary strings to be used as

public keys; e.g. email addresses. Li et al. [8] determined that the key scalability problem faced by IBE in the cloud scale is the fact that the revocation of the decryption authority of a user corresponds to the calculations conducted by the Private Key Generator (PKG), which is to be performed corresponding to the number of active users, which is unacceptable in large deployments. Their solution introduces a Key Update Cloud Service Provider (KU-CSP) that handles the computationally intensive key update operations, leaving the PKG to perform only a constant amount of work. Users hold hybrid private keys combining an identity component and a time component, enabling time-based revocation without requiring secure channels between users and KU-CSP.

- Key management for deduplication — the process of storing only one copy of identical data blocks — was addressed by Li et al. [9] through their Dekey system. Traditional deduplication uses convergent encryption, where the encryption key is derived from the data itself. This design introduces the risk that users must manage numerous convergent keys. Dekey distributes key shares across multiple servers using secret sharing, eliminating single points of failure and reducing the user-side key management burden. Security was formally proved under a model capturing the deduplication-specific threat of duplicate-key attacks.

D. Cloud Data Integrity and Public Auditing

- Ensuring that data stored in the cloud has not been tampered with — either by malicious parties or due to hardware failures — is a fundamental requirement. Private auditing models, in which the data owner themselves verifies data correctness, impose significant computational overhead on the owner and are poorly suited to large-scale outsourcing. Public auditing models delegate verification to a trusted third party (TPA), reducing the owner's burden.
- Patil and Sangve [10] proposed a remote data possession checking protocol based on homomorphic hash functions combined with Merkle Hash Trees (MHT). The MHT enables logarithmic-time proofs of data possession for specific data blocks, while the homomorphic property of the hash function allows block-level integrity checks without retrieving entire files.
- The protocol facilitates dynamic (insertion, deletion, modification) operations on outsourced data - a feature unavailable on many previous more traditional auditing schemes. One mentioned limitation is the lack of data confidentiality: the scheme is integrity-ensuring but does not encrypt the data, data content privacy is left to be handled by an additional encryption layer.

Table 1: Summary of Literature Review

Ref.	Authors	Year	Technique / Method	Focus Area	Limitation
[1]	Hei & Du	2011	Biometric two-level access (iris + basic biometric)	IMD Security	Limited to medical devices
[2]	Barni et al.	2010	Privacy-Preserving FingerCode Authentication (HE)	Fingerprint Privacy	High computational cost
[3]	Huang et al.	2011	Garbled Circuits for Biometric Identification	Biometric Matching	Expensive for large databases
[4]	Bethencourt et al.	2007	Ciphertext-Policy ABE (CP-ABE)	Access Control	No attribute privacy
[5]	Li et al.	2014	Secure Deduplication with Convergent Key Mgmt (Dekey)	Key Management	Multi-server dependency
[6]	Li et al.	2014	Outsourced ABE with Checkability	Decryption Outsourcing	Trusted CSP assumed
[7]	Hahn, Changhee, et al.	2016	Anonymous ABE with Match-then-Decrypt	Attribute Privacy	Overhead in matching phase
[8]	Li et al.	2015	IBE with Outsourced Revocation (KU-CSP)	Identity Revocation	KU-CSP semi-trusted only
[10]	Patil & Sangve	2015	Homomorphic Hash + MHT for Remote Data Checking	Cloud Auditing	No confidentiality support

III. KEY ALGORITHMS AND TECHNIQUES

Here we outline the major building blocks of algorithms and protocol design that we have found in the reviewed literature. We present five core techniques, providing pseudocode-level descriptions for each.

A. Privacy-Preserving Fingerprint Matching using Homomorphic Encryption

The protocol of Barni et al. [1] and similar schemes exploit additive homomorphic encryption — specifically,

variants of the Paillier cryptosystem — to compute the Euclidean distance between a query FingerCode vector and enrolled database vectors without decryption. The squared Euclidean distance $d^2(q, t) = \Sigma(q_i - t_i)^2$ can be computed homomorphically as follows:

Algorithm 1: Privacy-Preserving FingerCode Matching (HE-based)
INPUT: Client query FingerCode Q = {q1, q2, ..., qn} (plaintext)
Server database T = {Enc(t1), Enc(t2), ..., Enc(tn)} (encrypted)
OUTPUT: Match decision (YES / NO)
1. Client generates keypair (pk, sk) of Paillier cryptosystem.
2. Client encrypts query: EQ = {Enc(q1), Enc(q2), ..., Enc(qn)}.
3. Client sends EQ to server.
4. FOR each enrolled template T_j in database:
5. Server computes Enc(d²) = Enc(Σ(qi - t_ji)²) using HE:
Enc(qi - t_ji)² = Enc(qi²) ⊗ Enc(-2qi·t_ji) ⊗ Enc(t_ji²)
6. Server returns Enc(d²_j) to client.
7. Client decrypts: d²_j = Dec(sk, Enc(d²_j)).
8. Client identifies best match: j* = argmin_j {d²_j}.
9. IF d²_j* < threshold θ THEN return MATCH ELSE return NO_MATCH.
SECURITY: Server learns neither Q nor matched identity.
COMPLEXITY: O(n) HE multiplications per template comparison.

B. CP-ABE: Ciphertext-Policy Attribute-Based Encryption

CP-ABE (Bethencourt et al. [4]) consists of four algorithms: Setup, KeyGen, Encrypt, and Decrypt. The access policy is embedded in the ciphertext, and decryption succeeds when user attributes satisfy the policy.

Algorithm 2: CP-ABE Scheme
INPUT: Security parameter λ, attribute universe U, access policy P
OUTPUT: Encrypted data accessible only to authorised attribute holders
SETUP(λ):
1. Choose bilinear group G of prime order p with generator g.
2. For each attribute i ∈ U: pick random h_i ← Z_p; set H_i = g^h_i.
3. Pick α, β ← Z_p; compute e(g,g)^α, g^β.
4. MSK = (α, β); PK = (g, e(g,g)^α, g^β, {H_i}).
KEYGEN(MSK, S) [for attribute set S]:
5. Pick r ← Z_p; set K = g^((α+r)/β), L = g^r.
6. For each x ∈ S: pick r_x ← Z_p; K_x = g^r · H_x^r_x; L_x = g^r_x.
7. SK_S = (K, L, {K_x, L_x}_{x∈S}).
ENCRYPT(PK, M, P) [access policy P as LSSS matrix (A, ρ)]:
8. Pick s, s1..sl ← Z_p (sharing vector for P).
9. CT = { C = M · e(g,g)^(αs), C' = g^(βs), {C_i = g^(A_i·v) · H_ρ(i)^(-s_i), D_i = g^s_i} }.
DECRYPT(CT, SK_S):
10. Compute reconstruction coefficients {ω_i} for S satisfying P.
11. Compute e(g,g)^(αs) via pairing operations and ω_i weights.
12. Recover M = C / e(g,g)^(αs).

C. IBE with Outsourced Revocation (KU-CSP Protocol)

Li et al. [8] designed an IBE scheme in which the Key Update Cloud Service Provider (KU-CSP) handles the computationally intensive key update operations during user revocation. Each user's private key is a hybrid structure binding an identity component to a time component, preventing revoked users from updating their keys beyond their revocation period.

Algorithm 3: Revocable IBE with KU-CSP
INPUT: Security parameter λ, identity ID, time period T, revocation list RL
OUTPUT: Ciphertext decryptable only by non-revoked user in period T
SETUP(λ):
1. Generate master secret key (MSK) and public parameters (PP).
2. Initialise revocation list RL = ∅ and binary tree BT.
KEY-ISSUING(MSK, ID):
3. Assign leaf node v_ID in BT to user ID.
4. Compute identity key component: sk_ID = (sk_id, sk_time_placeholder).
KEY-UPDATE(MSK, RL, T) [performed by PKG + delegated to KU-CSP]:

5. PKG determines non-revoked set: cover nodes CN = Cover(BT, RL).
6. For each node θ ∈ CN: PKG generates key update material ku_θ^T.
7. KU-CSP distributes ku_θ^T to users whose path includes θ.
DECRYPTION-KEY-DERIVATION:
8. User with sk_ID and matching ku_θ^T computes full DK_ID^T.
9. If ID ∈ RL before period T: no valid ku_θ^T exists → decryption fails.
ENCRYPT(PP, ID, T, M):
10. Encrypt M under (ID, T) such that only DK_ID^T can decrypt.
SECURITY: Revoked users cannot obtain DK_ID^T for T' > revocation date.

D. Anonymous ABE with Match-then-Decrypt

Zhang et al. [5] introduced a pre-decryption matching stage to avoid the overhead of unnecessary decryption attempts in anonymous ABE, where access policies are hidden from users who do not possess matching keys.

Algorithm 4: Anonymous ABE — Match-then-Decrypt
INPUT: Ciphertext CT with hidden policy P*, user secret key SK_S
OUTPUT: Plaintext M (if S satisfies P*), or rejection
MATCH PHASE (lightweight — O(1) pairings):
1. Extract test components (TC) from CT.
2. Compute test value TV = f(TC, SK_S) using unique key segments.
3. IF TV == 1 THEN proceed to DECRYPT ELSE output ⊥ (reject).
DECRYPT PHASE (efficient — accumulated pairings):
4. Using accumulated pairing result from match phase:
e_acc = ∏ e(g, g)^(r_i) for matched attribute indices i.
5. Recover blinding factor B = C_head / e_acc.
6. Decrypt: M = C_payload / B.
COMPLEXITY: Match phase < 1 full decryption; Decrypt reuses pairing.
PRIVACY: Ciphertext reveals no attribute or policy information.

E. Homomorphic Hash-based Remote Data Integrity Checking

Patil and Sangve [10] proposed a protocol in which the cloud server generates short cryptographic proofs of data possession for challenged blocks, using homomorphic hash functions that allow server-side proof aggregation without data retrieval.

Algorithm 5: Remote Data Integrity Checking (MHT + Homomorphic Hash)
INPUT: File F = {B1, B2, ..., Bn} (data blocks), challenge C ⊆ {1..n}
OUTPUT: Integrity proof Π; verification result (VALID / INVALID)
TAG-GENERATION (by data owner before upload):
1. For each block Bi: compute tag σ_i = H(name ‖ i)^α · f(Bi)^β mod N.
where H is a collision-resistant hash, α,β are owner secrets.
2. Build Merkle Hash Tree (MHT) over {σ_i}; root = MHT_root.
3. Sign root: sig = Sign(sk_owner, MHT_root).
4. Upload (F, {σ_i}, MHT_root, sig) to cloud.
CHALLENGE PHASE (by Third Party Auditor):
5. TPA picks random subset C = {(i, v_i)} of block indices and coefficients.
6. TPA sends C to cloud server.
PROOF GENERATION (by cloud server):
7. Aggregate blocks: M_agg = Σ v_i · Bi (mod p).
8. Aggregate tags: σ_agg = Π σ_i^v_i (mod N).
9. Compute MHT sibling paths for all i ∈ C.
10. Return Π = (M_agg, σ_agg, MHT_paths).
VERIFICATION (by TPA):
11. Recompute expected aggregate tag from M_agg.
12. Verify MHT paths lead to stored MHT_root.
13. Verify sig on MHT_root.
14. IF all checks pass: VALID ELSE: INVALID (data corruption detected).

IV. COMPARATIVE ANALYSIS

Having surveyed the key techniques and algorithmic approaches in the domain, we now present a multi-dimensional comparative

analysis of the principal schemes. Table 2 assesses each scheme by seven criteria including primary focus, privacy support, computational cost either at the client or verifier, revocation support, biometric integration, and the general level of security.

Table 2: Comparative Analysis of Surveyed Schemes

Scheme	Focus	Privacy	Comp. Cost	Revocation	Biometric	Security Level
CP-ABE [4]	Fine-grained AC	No	High	No	No	Moderate
IBE + Revocation [8]	Identity Mgmt	Partial	Medium	Yes (KU-CSP)	No	High
Outsourced ABE [6]	Decryption Offload	Yes	Low (client)	Yes	No	Moderate
Anon. ABE [7]	Attribute Privacy	Yes	Low	Yes	No	High
Finger Code HE [2]	Biometric Auth	Yes	High	No	Yes	High
Garbled Circuits [3]	Biometric Match	Yes	Very High	No	Yes	High
Dekey [5]	Key Dedup	Yes	Medium	Multi-server	No	Moderate
Proposed Hybrid	All-in-One	Yes	Low-Medium	Yes (IBE+ABE)	Yes (Fingerprint)	High

A. Discussion of Comparative Findings

The structural tensions of cloud security scheme design space are a few as indicated by the comparative analysis.

Privacy vs. Efficiency: Schemes that can attain good privacy guarantees, like anonymous ABE [5] and garbled-circuit-based biometric matching [3], are likely to be more expensive to compute. Garbled circuits are information-theoretically secure, but have high bandwidth and computation overheads that prevent their application to large biometric databases. Anonymous ABE addresses this by the match-then-decrypt optimisation, which has a client-side cost similar to that of regular (non-anonymous) ABE.

Revocation: Revocation support has always been considered a difficult one. In its simplest form, CP-ABE [4] does not offer any efficient revocation. This is solved by the IBE based revocation scheme [8] using the KU-CSP model and has a constant PKG overhead, but needs a semi-trusted auxiliary server.

Biometric Integration: There are only two schemes among the surveyed ones, the FingerCode HE scheme [1, 2] and the garbled-circuit protocol [3], that incorporate biometric data directly. Both consider biometric matching as an independent component, independent of the access control and key management layers.

Computational Cost: Bilinear pairing schemes (CP-ABE and its derivatives) are characterized by moderate cost to the client that increases with the complexity of policies. Outsourced ABE [6] is also very useful since it transfers the entire load of decryption calculations to the server, and the client overhead is a constant, but it assumes that the server is non-colluding. MHT aggregation is the most scalable method of integrity checking as it provides logarithmic verification cost in public auditing [10].

The hybrid course suggested to take IBE and revocation, ABE to provide fine-grained access control, and fingerprint biometrics to authenticate users was not realised in any single scheme entirely. A co-design of the most important layers to achieve such a synthesis would be the key generation, biometric matching, and access control layers, and it would be a great research opportunity.

V. SYNTHESIS AND PROPOSED RESEARCH DIRECTION

In the assessed literature, there is considerable advancement on the separate aspects of cloud security: biometric privacy, attribute-based access control, identity-based encryption, key management, and data integrity auditing. The layered architecture of a Hybrid Biometric-IBE-ABE Secure Cloud Framework is a proposed conceptual architecture that will have the following design:

Layer 1 – Biometric Authentication Layer: The identity of the user is determined through additive homomorphic encryption with privacy preserving matching of the fingerprints. The corresponding response, but not the raw biometric, is authorised and a token is issued to the user.

Layer 2 – Identity and Revocation Layer: Identity generation by IBE is triggered by authenticated identity. Efficient and constant cost revocation is supported using the KU-CSP model [8] to ensure that compromised or lost users do not access the PKG at the expense of the PKG.

Layer 3 – Fine-Grained Access Control Layer: Data is encrypted over CP-ABE policies, which are bound to attributes

of users determined as a result of the authenticated identity. ABE [5] is used anonymously to hide policy details to the cloud server.

Layer 4 – Integrity Auditing Layer: The MHT-based public auditing protocol [10] is implemented on all the outsourced data blocks allowing a TPA to check the integrity of cloud storage without data access and without violating confidentiality.

This three-layer synthesis fills in the three main shortcomings found in the comparative analysis: no biometric integration, no effective revocation and no linkage of access control to identity management. The main directions of the further work are the formal analysis of the security and empirical performance assessment of this hybrid framework.

VI. CONCLUSION

The biometric technique of ensuring a secure data transmission in cloud computing has been thoroughly reviewed in this paper. We have systematically surveyed ten exemplary works in the domain of biometric privacy-preserving protocols, attribute-based encryption, identity-based encryption, key management, and public auditing and identified the main limitations in the field. Among the key findings, it is possible to note: (1) the homomorphic encryption and garbled circuits offer high-level biometric privacy in the presence of high computational cost, (2) CP-ABE and its anonymous and outsourced version offer flexible fine-grained access control without integrated revocation and biometric binding, (3) IBE with KU-CSP-based revocation imposes constant PKG overhead but requires semi-trusted auxiliary infrastructure, and (4) public auditing with MHT and homomorphic hashing provides efficient integrity verification but no confidentiality. The given Hybrid Biometric-IBE-ABE allows proposing a conceptual synthesis to fill these gaps. Its formal security analysis, efficient implementation, and performance analysis under realistic cloud workloads are still as significant research directions in future studies. Also, further investigation of extensions to new biometric modalities (gait, keystroke dynamics, ECG), post-quantum cryptographic implementations of pairing schemes, and co-location with federated and edge computing models are additional lines of research. We believe that this review survey will be of help to researchers and practitioners working on the development of the cloud security and biometric authentication and will encourage new integrative studies between these two complementary science areas.

REFERENCES

[1] M. Barni, T. Bianchi, D. Catalano, M. Di Raimondo, R. D. Labati, P. Failla, et al., "Privacy-Preserving Fingercode Authentication," in Proc. 12th ACM Workshop on Multimedia and Security, pp. 231–240, September 2010.

[2] X. Hei and X. Du, "Biometric-Based Two-Level Secure Access Control for Implantable Medical Devices during Emergencies," in Proc. IEEE INFOCOM, 2011.

[3] Y. Huang, L. Malka, D. Evans, and J. Katz, "Efficient Privacy-Preserving Biometric Identification," in Proc. 18th Network and Distributed System Security Symposium (NDSS), pp. 6–9, February 2011.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in Proc. IEEE Symposium on Security and Privacy (SP'07), pp. 321–334, 2007.

[5] Y. Zhang, X. Chen, J. Li, D. S. Wong, H. Li, and I. You, "Ensuring Attribute Privacy Protection and Fast Decryption for Outsourced Data Security in Mobile Cloud Computing," Computers & Security, Elsevier, 2016.

[6] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely Outsourcing Attribute-Based Encryption with Checkability," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 8, pp. 2201–2210, August 2014.

[7] Hahn, Changhee, Kwon, Hyunsoo, Hur, Junbeom, Efficient Attribute-Based Secure Data Sharing with Hidden Policies and Traceability in Mobile Health Networks, Mobile Information Systems, 2016, 6545873, 13 pages, 2016. https://doi.org/10.1155/2016/6545873.

[8] J. Li, J. Li, X. Chen, C. Jia, and W. Lou, "Identity-Based Encryption with Outsourced Revocation in Cloud Computing," IEEE Transactions on Computers, vol. 64, no. 2, pp. 425–437, February 2015.

[9] J. Li, X. Chen, M. Li, J. Li, P. P. C. Lee, and W. Lou, "Secure Deduplication with Efficient and Reliable Convergent Key Management," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 6, pp. 1615–1625, June 2014.

[10] R. R. Patil and S. M. Sangve, "Public Auditing System: Improved Remote Data Possession Checking Protocol for Secure Cloud Storage," in Proc. International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), pp. 75–80, October 2015.