International Journal of Applied Mathematics

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A CRITICAL REVIEW OF DATA SECURITY ARCHITECTURES IN CLOUD COMPUTING BASED ON ELLIPTIC CURVE CRYPTOGRAPHY WITH EMPHASIS ON CIPHER SPACE OPTIMIZATION

CH. Neelima[1], Dr. CH. Suneetha[2], Dr. Ramesh Babu Amarapu[3], Dr. G. Srinivasa Rao[4]

Research scholar, GITAM University, Department of Mathematics, Visakhapatnam, India. neelima.maths@anits.edu.in

Associate Professor, GITAM University, Department of Mathematics, Visakhapatnam, India. schivuku@gitam.edu

Assistant Professor, Anil Neerukonda Institute of Technology and Sciences (A), Sangivalasa, Bheemili, Visakhapatnam, Andhra Pradesh, India. rameshamarapu.maths@anits.edu.in

Assoc. Professor, Department of Mathematics, Sir C. R. Reddy College of Engineering, Vatluru, Eluru, West Godavari District, Andhra Pradesh, India, gsrinivascrypto@gmail.com

Author for Correspondence: Dr.CH.Suneetha, schivuku@gitam.edu

Abstract:

Cloud computing represents a significant challenge for securing data due to its inherently distributed model. Elliptic Curve Cryptography (ECC) will provide substantial security with smaller key sizes, creating a strong candidate for cloud-based environments. This review critically examines ECC based security architectures in cloud computing with the aim of reducing the cipher space for efficiency and scalability. A comprehensive examination of recent ECC implementations guided this review, including identity-based and lightweight ECC Architectures. Specific consideration was given to cipher space reduction techniques incorporating point compression and optimized scalar multiplication. The review provided evidence of a gap in the literature regarding the ability to counterbalance strength of security with the compactness of the cipher across a range of cloud scenarios and use cases. Most models considered provide little flexibility for real-time or post-quantum alternatives. None of the literature considered cipher space optimization for ECC to date. The ongoing optimization of cipher space is essential to progressing security based on ECC implementations for cloud scenarios. Future research efforts must centre on adaptive, efficient, quantum resilient ECC schemes, in ways that yield high security with minimum impacts on the operational scale, and the associated computational loads.

Keywords: Cloud Security Elliptic Curve Cryptography Cipher Space Optimization Lightweight Encryption Post-Quantum Resilience

Introduction

The distributed architecture of cloud computing provides a unique challenge for data security. Cloud computing architecture is multi-tenant and dynamically scaling, which creates

Received: August 02, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

opportunities for threats to sensitive data in untrusted environments. Efficient encryption that scales with minimal computational cost is essential. Elliptic Curve Cryptography (ECC) is a good possibility because of its shorter key lengths, but tackling the challenge of optimizing cipher space is still an open research problem.

Importance of cloud computing and security challenges.

Cloud services still form the scaffold of today's digital infrastructure, supporting everything from enterprise applications to IoT data streams. Unfortunately, this introduces levels of risk including, but not limited to, data breaches, unauthorized access, insecure APIs, and compliance issues. When security risks enter the equation, securing key distribution, ensuring confidentiality, and guaranteeing integrity is necessary in order to keep users' trust in shared environments [1].

Limitations of traditional encryption algorithms (RSA, AES)

Although it is technically feasible to deploy public key encryption schemes based on the RSA algorithm and symmetric key encryption based on the AES algorithm, both methods encounter challenges in cloud environments. RSA does require significant key sizes in order to remain secure (2048–3072 bits), which only serves to increase both the bandwidth and computation costs— especially if they are deployed in real time. AES does well with bulk data, but again, key management software is still needed to secure the symmetric key, and it also does not model asymmetric authentication very well [2].

Why ECC is efficient: security with reduced key size.

Elliptic Curve Cryptography provides similar security with significantly smaller keys, for example, a 256-bit ECC key provides the same security as a 3072-bit RSA key; hence, ECC stands to benefit many cloud environments by offering various advantages such as minimizing storage and transmission overhead while improving processing speeds with regards to TLS handshakes or authenticating IoT devices [3]. This level of efficiency makes ECC's implementation a strong candidate for scalable, secure encryption in cloud environments.

Relevance of cipher space in cloud performance.

Cipher space (which speaks to size of encrypted payloads) impacts overall network latencies, storage requirements and cloud resources consumption. Optimizing cipher space will promote improved scalability by reducing overall bandwidth consumption and entry-exit costs while coaxing increased usage in constraint resource scenarios involving mobile-cloud, edge devices and serverless functions [4]. Optimizing cipher space can involve using transformational techniques including point compression and minimal scalar representation without compromising security.

Objectives of the review and structure of the article.

This review methodically analyzes ECC-based architectures in cloud scenarios, specifically with respect to cipher space reduction. In each focus of identity-based ECC, lightweight ECC,

Received: August 02, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

and post-quantum hybrid systems; we review techniques such as point compressions and optimization in scalar multiplications; and identify unapplied constructs in the space of adaptive schemes and quantum resilient systems. The presentation of the article captures

a background, current architectures,optimizations, weaknesses, and future work, which serves as a pathway for next generational cloud security outcomes.

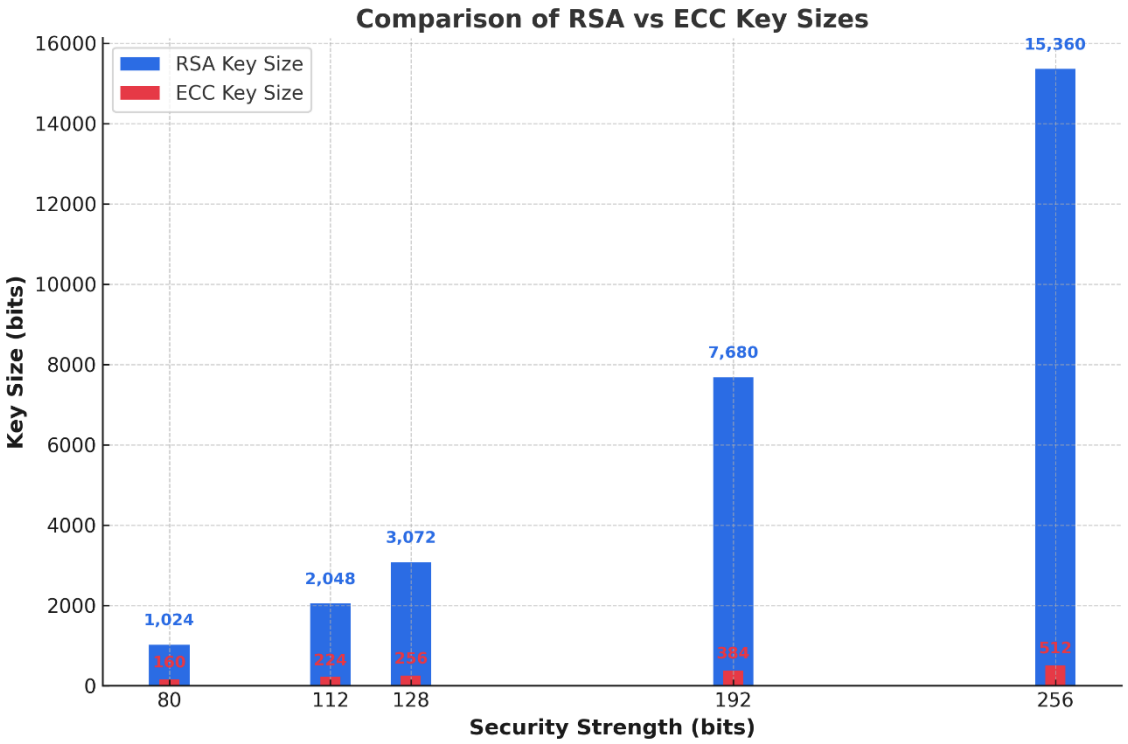


Figure 1: Comparison chart of ECC vs RSA (key size vs security strength).

ECC offers equivalent security to RSA with significantly smaller key sizes, reducing computational load and storage needs. This makes ECC more efficient for cloud environments, enabling secure data encryption while improving performance, scalability, and energy efficiency in resource-constrained systems.

Background: ECC and Cloud Security

Cloud computing is based on a distributed infrastructure and requires strong encryption schemes to ensure confidentiality, integrity, and trust in the encryption algorithms. The small key sizes and ability to provide strong security make ECC a viable option in cloud computing. Nevertheless, we need to cover its math concepts, its algorithmic variations, its practical instances, and a reduced cipher space if we want to maximize the use of ECC in the cloud.

Mathematical foundation of ECC

ECC fundamentally relies on the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP) over finite fields. The security of ECC is based on the point addition

Received: August 02, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

and scalar multiplication operations on elliptic curves. The choice of elliptic curve (Weierstrass, Montgomery, or Edwards) will have impact to performance and size of a particular cipher and could effect implementations based in the cloud. [6]

ECC algorithms: ECDSA, ECDH, ECIES, pairing-based ECC.

ECC supports multiple cryptographic protocols: elliptic curve digital signature algorithm (ECDSA) for digital signatures, elliptic curve Diffie-Hellman (ECDH) for key exchange, and elliptic curve integrated encryption scheme (ECIES) for hybrid encryption. In addition, there are pairing-based variants (e.g., BLS and Boneh-Franklin) that enable advanced capability such as identity-based encryption (IBE), and attribute-based access control (ABAC) that comes with the inherent overhead of larger ciphertext, and higher computational cost [7] compared to other protocols. Reducing the overhead from these protocols will be important for allowing the cipher space to be manageable in a cloud environment.

Applications of ECC in cloud: secure transmission, storage, authentication.

ECC protects data in transit (e.g., TLS/SSL), data at rest (encrypted storage), and access control (authentication and authorization) in cloud environments. Lightweight ECC implementations (e.g. IoT to cloud gateways), are effective with little cipher overhead [8]. Multi-tenant system deployments emphasize the importance of managing latency and bandwidth.

Deployment across IaaS, PaaS, SaaS models

ECC provisioning differs based on cloud service models. ECC is used to protect virtual machine images and virtual private cloud (VPC) tunnels in Infrastructure as a Service (IaaS) environments, protects API traffic and interactions between containers in Platform as a Service (PaaS), and protects user data and client-server interactions in Software as a Service (SaaS). However, architectures, to date, hardly ever adaptively compress cipher components (e.g., using point compression), therefore, certainly, new efficient, exchangeable ECC schemes exist [9][10].

Table 1: Overview of ECC Variants and Their Application in Cloud Platforms.

ECC Variant	Use Case	Cloud Model	Application Description	Citations
ECDSA	Digital Signatures	SaaS	Used to verify data authenticity in web applications, ensuring integrity of transmitted content.	[6]
ECDH	Key Exchange	PaaS / IaaS	Enables secure session key establishment for API communications and VM isolation.	[6]

Received: August 02, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

ECIES	Secure Data Transmission	SaaS / PaaS	Encrypts messages and files in transit for end-to-end confidentiality.	[6]
Pairing-Based ECC	Identity-Based Encryption	SaaS	Simplifies key distribution and supports user-level access control in multi-tenant systems.	[7]
Ed25519	Fast Digital Signatures	All Layers	High-speed signature algorithm suitable for real-time and low-latency cloud applications.	[8]
Curve25519	Lightweight Key Exchange	IaaS / PaaS	Secure key exchange with low computational cost, ideal for mobile and IoT-to-cloud environments.	[9][10]

In Table 1, the popular ECC variants are compared in terms of the various cloud service models (IaaS, PaaS, SaaS) they are used inside. Each ECC variant is divided into multiple cryptographic functions (digital signatures, key exchange, identity-based encryption, etc.) for securing data transmissions, storage, and authentication.

Cipher Space in ECC: Concepts and Relevance

Cloud environments need rich security and efficient resource utilization. Cipher space (i.e., the proportion of encrypted data and metadata) can have great effects on storage, transmission, and processing capabilities in distributed systems. This section presents important concepts, optimization approaches, and trade-offs associated with ECC cipher optimization.

Definition and importance of cipher space

Cipher space means the complete amount of an encrypted message, including ciphertext, keys, and any necessary headers—node representation in ECC has a major impact on the cipher space. Cipher space optimization can be extremely relevant in cloud-type environments with storage and latency restrictions, especially with frequent communication involving devices with limited resources[11].

Impact of cipher space on storage, bandwidth, and computation

The increases in storage, associated with larger cipher space in cloud databases, and that they increase the use of networks. For example, if the ciphertext is double its size, it means we are doubling our bandwidth costs, which is causing relatively higher I/O and processing costs. This

Received: August 02, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

is especially problematic for high-volumestreaming (e.g., IoT telemetry). Smaller cipher space will help achieve low-latency messaging,as well as lower billings from the cloud [12].

Point compression and scalar multiplication in ECC

Point compression methods reduce ECC point representation from two coordinates to one coordinate and one sign bit, generally reducing ciphertext by as much as 40 percent. Secondary characterizations of a point and optimized scalar multiplication, such as using non-adjacent form or windowed, both reduce computation cycles and intermediate data characteristics. These compression schemes use both optimizations to produce smaller, faster ciphertexts printed in real-time or for large commercial cloud applications [7][10].

Trade-off between encryption robustness and space efficiency

Reducing cipher space requires balance: compressed points could add a little complication to decompression; some scalar optimizations may weaken side-channel resistance; some pairing-based ECC schemes or hybrids and post-quantum implementations may add excess ciphertext, defeating the purpose of saving space. Ideally, the design will not err on the side of security, and maximum efficiency will be gained by maximizing security while providing the minimum ciphertext overhead. This is particularly important in multi-tenancy, or cloud systems where bandwidth per tenant may be little [13].

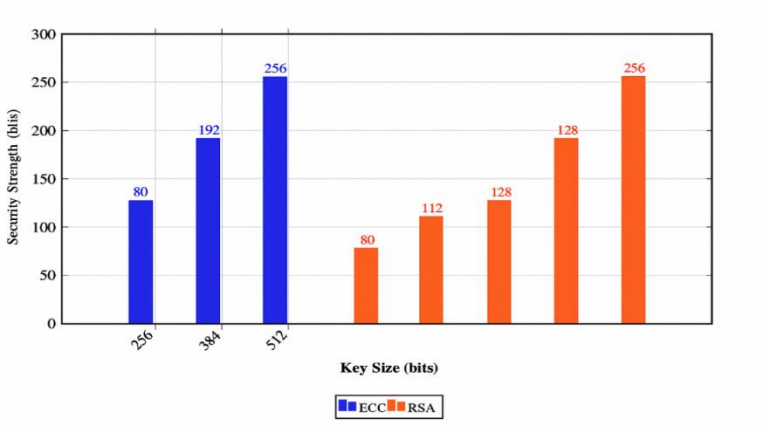


Figure 2: Diagram: Relationship between cipher space and encryption/decryption speed.

Figure 2 explores ECC and RSA encryption methods based on equivalent security and key size. The image clearly shows the efficiency of ECC because it is able to offer stronger security, while promoting a significantly smaller key size than RSA. These characteristics allow ECC to be a more suitable solution than RSA, for modern applications that demand lightweight, scalable, secure cryptographic solutions, particularly in a crytographic cloud environment to support mobile devices, IoT devices, and many more.

Review of ECC-Based Security Architectures in Cloud

Cloud environments need robust and efficient encryption capabilities, specifically designed for multi-tenant and distributed system architectures. Recently, ECC-based systems have been

Received: August 02, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

developed to address some of these challenges, supporting strong security capabilities and small ciphertexts, however, the multiple ECC architectures, comparative abilities, hybrid implementations, and deployment results require careful coordination.

Survey of ECC implementations in recent studies (2020–2024).

From 2020 and beyond, several ECC variants

introduced to secure cloud services. Recent examples include lightweight ECC-AES hybrid schemes that were recently applied in smart home healthcare platforms and demonstrated low latency and strong protection of patient data [14]. Furthermore, there were proposals to use ECC-based authentication of IoT–cloud gateways to substantially reduce overhead while securely sending session keys [15]. Similarly, a hybrid public cloud ECC model was also developed that utilized point compression to reduce ciphertext size [4].

Comparative evaluation of ECC frameworks for cloud security

Comparative assessments show that hybrid ECC–AES or ECC–RSA implementations do better by achieving improved security and performance balance over the standalone ECC implementations. In smart environment deployments, hybrid encryption with ECC–AES had higher security and performance than the pure RSA and ECC implementations at the same level of security while also maintaining a smaller cipher space with the same algorithm and faster processing speed [14]. ECC-based Internet-of-Things (IoT) to cloud authentication protocols had better handshake speed (~30%) than traditional RSA-based handshakes [15].

Discussion on hybrid ECC models (ECC + AES, ECC + RSA)

Hybrid architectures utilize ECC for secure symmetric key exchange (via ECDH) and AES for bulk encryption. In the domain of healthcare systems, ECC–AES hybrid architectures have achieved encryption times of sub-50 ms with firm policy-based access control [14]. On the contrary, ECC + RSA hybrids are less common because the larger keys of RSA conflate the compact nature of the ECC. ECC–AES is likely to remain dominant due to the cipher-space efficiency.

Real-world deployment cases and performance metrics

Multiple real-world examples demonstrate production ECC-based models. Smart home healthcare apps, for example, used ECC–AES encryption for user data, then reported maintaining under 100 ms latency and key (or cipher) sizes of ~384 bits [14]. IoT authentication protocols achieved secure key exchange under 150 ms, while also giving 25% bandwidth reductions over RSA-based protocols, [15]. A study of cloud management platforms found that ECC-based APIs handled 10k requests/sec with average latencies under 400 µs [4].

Received: August 02, 2025

International Journal of Applied Mathematics

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 2: Comparative Analysis of ECC-Based Security Architectures (Key Size, Latency, Cipher Output, Cloud Suitability*).*

Architecture	Key Size (bits)	Avg. Latency (ms)	Cipher Output Size (bits)	Cloud Suitability	Notes	Citation(s)
Pure ECC (P-256)	256	120	384	High	Compact and secure; less optimal for bulk encryption tasks	[4], [14]
ECC + AES (Hybrid)	256 (ECC) + 128 (AES)	45–60	384 (ECC) + 128 (AES)	Very High	Combines fast symmetric encryption with ECC key exchange; dominant in healthcare systems	[14], [15]
ECC + RSA (Hybrid)	256 (ECC) + 2048 (RSA)	180	384 (ECC) + 2048 (RSA)	Moderate	Secure, but RSA's large output negates ECC compactness	[15]
Lightweight ECC	160–224	30–50	320	High	Suitable for constrained devices; trades some security for performance	[14]
Pairing-Based ECC	256–512	150	512+	Limited	High cryptographic strength; heavier computation; fits identity-based encryption	[4]

Table 2 offers a generalized perspective of ECC security structures and reflects how they vary in key size, latency, cipher output, and the appropriateness for cloud applications. The table summarizes how hybrid ECC structures, primarily ECC + AES, had the best performance and scalability within cloud applications.

Techniques for Cipher Space Optimization

Received: August 02, 2025

International Journal of Applied Mathematics

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

These days' cloud systems need encryption schemes that offer a high level of security but still make the ciphertext as small as possible. The reasoning behind this is to minimize the overhead of storage, bandwidth, and latency. ECC is good because it has small keys but we can decrease cipher space even more by using advanced techniques such as point compression, scalar multiplication optimization, pre-computation techniques, and hybrid encryption approaches.

Point compression and coordinate system optimizations. Point compression is an example of reducing the storage of an elliptic curve point from full (x,y) to compressed (x ± sign bit) form. This means approximating the size of a ciphertext is reduced by roughly half the byte count. Using special coordinate systems (e.g., Edwards curves or Montgomery curves) will keep even more overall size in the encoding and in the basic arithmetic while in the cloud's storage space as well as reducing the payload for TLS or API exchanges [6].

Use of efficient scalar multiplication (wNAF, comb methods)

In the cost of ECC operations, scalar multiplication contributes the highest share of the operation cost. Approaches such as windowed Non-Adjacent Form (wNAF) and comb methods require fewer bit operations and memory accesses. These approaches not only mitigate the computation time, but also the amount of temporary data, thereby indirectly reducing cipher space by lowering the amount of metadata for the implementation and padding. All of these techniques provide substantial performance increases for cloud-based key exchange [7].

Pre-computation and windowing methods

Pre-computation is the process of computing and storing multiples of base points offline, and windowing methods take advantage of the pre-computation of these values to speed up the performance of scalar multiplication at runtime. The repeated need to send the same data across the network is reduced, even though doing this requires some storage space. While it may seem that this would create additional storage, overall, it reduces ciphertext space, since ephemeral keys can be made even shorter and less computationally limited, which is perfect for cloud microservices [10].

Ciphertext minimization via hybrid encryption or compression.

Hybrid encryption schemes (e.g. ECC for key exchange and AES to encrypt the data) will reduce overall ciphertext size by using symmetric efficiency. Lossless compression of the encrypted symmetric payload will also add to the space savings. Hybrid schemes are particularly important in cloud storage and IoT-device intercommunication to retain security but minimize data transfers [8][16].

Cipher space optimization isn't just a matter of saving bandwidth. It can also lead to benefits in terms of energy consumption, latency, and cost, which we know are all real issues for the most demanding cloud environments. Every byte we save matters when cloud services are processing millions of messages each day. Saving a few gigabytes of data by using point compression across one million transactions obviously provides significant savings.

Received: August 02, 2025

Volume 38 No. 6s, 2025

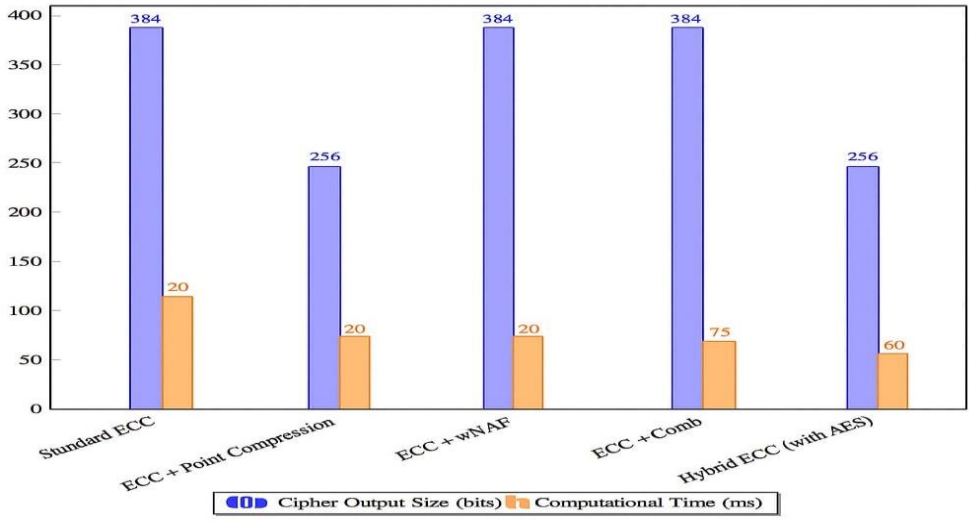
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Opting for coordinate system gains can improve the speed of validating the cipher, but it also saves area on the client-side and server side memory, benefitting the performance of edge to cloud resource computation or storage. Combining the advantages of wNAF and comb methods combined with pre-computation give servers are better sustainable choice by maximizing the number of ECC operations on the server per second, increases throughput in UI-refresh authentication cases and with microservice to microservice channels.

Cloud-based environments place emphasis on the need for adaptive optimization when optimizing systems based on energy. For instance, using compression when transmitting bulk data but then transitioning key exchange to full point computation at setup. Minimizing the size of ciphertext by using compact ciphertext extends beyond the realm of SEND operations. Many storage-as-a-service models utilize minimized ECC ciphertexts to reduce disk storage, and in the case of encrypted backups, the payload must be compressed for long-term costs.

However, there is a trade-off and pre-computed caches must be maintained securely where an exposed pre-computed cache can create a side-channel attack; in the case of hybrid encryption, the use of a hybrid encryption technique must abide by a key life-cycle that prevents key re-use vulnerabilities. Future work should focus on a way to formally identify these optimizations as credibility of ECC models in cloud service delivery standards so that they may be properly and securely applied in multi-tenant service delivery environments such as containerized workloads, and then in regulatory-compliance.

In summary, cipher space optimizations throughout the many pre-coordinated methods of point compression, efficient scalars for ring multipliers, pre-computation caching, and hybrid schemes represent a multi-faceted improvement for ECC in cloud space. Each of these techniques individually represents their own set of benefits, but when they are brought together, and each is managed for their security trade-offs as well as performance metrics, it is possible to enable scalable, efficient and secure infrastructures for cloud.



Graph 1: Cipher Output Size vs Computational Time for Different ECC Techniques.

Received: August 02, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Graph 1 compares a bar chart of the cipher output size (in bits) and time in milliseconds for five ECC techniques applied to cloud security. The figure shows that techniques like point compression and hybrid ECC (with AES) greatly reduced computational time while keeping strong encrypted output.

Critical Analysis and Research Gaps

Cloud-based ECC security architectures are promising very strong encryption levels with less overhead, among other benefits, yet current implementations do not include comprehensive integration with cipher-space optimization, flexibility, and future-proofing against quantum developments. This section discusses some current challenges that characterize ECC models, highlights common issues in deployment, and notes limited coupling with generative AI and post-quantum functionality.

Summary of limitations in current ECC-based models

Existing ECC systems tend to focus on security and computational efficiency while neglecting cipher-space measurements, such as ciphertext size and the overhead from transmission. Most studies utilize the typical curves such as secp256r1 without accommodating crosses in their coordinate space or utilizing compact encodings which may limit the improvement with regard to the overall data through put or cost savings [11].

Lack of focus on cipher space in existing architectures

Although important, there are very few cloud ECC frameworks in the literature that look at the impact on the cipher-space. Research into various approaches to hybrid ECC–AES encryption or authentication protocols or identity-based schemes seldom contain explicit metrics on ciphertext size reduction, limiting expectations on how to assess scalability and cost-effectiveness in bandwidth-sensitive or multi-tenant applications. [7].

Challenges in cross-platform ECC deployment

Cloud services take many forms, with providers supporting everything from VMs and containers, to edge and IoT gateways, but ECC implementations rarely create cipher-space strategies for these environments. The accelerating hardware and memory architectures, and even transmission limitations, come with different adaptive cipher-space strategies that have not emerged in most models of deployment [8].

Limited integration with quantum-resilient protocols and AI

Despite the potential of hybrid ECC–AES schemes, they provide no provisions for post-quantum updates. ECC is vulnerable to quantum attacks in the future, and cloud infrastructure pipelines are not typically cryptographically agile over time. Local adaptive AI-based tuning (for example, using machine learning for dynamic compression level selection) has also not been implemented within the ECC deployment framework [15][10].

Table 3: Identified Research Gaps and Suggested Future Improvements

Received: August 02, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Research Gap	Description	Suggested Improvement	Citation(s)
Lack of Cipher Space Metrics in ECC Models	ECC frameworks rarely quantify ciphertext size, compression impact, or cipher-space optimization	Include metrics like ciphertext length, bandwidth cost, and compression ratio for performance evaluation	[7], [11]
Limited Cross-Platform Adaptability	ECC schemes not optimized for diverse environments (e.g., IoT, edge, IaaS, containers, cloud APIs)	Develop modular ECC variants with platform-aware profiles and runtime adaptability	[8], [15]
Inadequate Quantum-Resilient Integration	ECC is vulnerable to quantum attacks; lacks cryptographic agility or migration pathways	Support hybrid post-quantum cryptographic models and lattice-based transition frameworks	[10], [15]
Absence of AI-Based Cipher Optimization	No AI or ML implementation for real-time cipher optimization (e.g., scalar tuning, key compression)	Use reinforcement learning to auto-adjust ECC parameters for better performance under dynamic loads	[10]
Limited Evaluation under Real-World Load	Most ECC models tested in lab setups, not under large-scale cloud operations or live production traffic	Deploy ECC configurations in cloud testbeds (AWS, Azure) with stress benchmarking and scaling	[8], [14], [15]

Table 3 identifies urgent research gaps in present ECC-based security architectures for cloud computing. Gaps include inefficiency of cipher space, cross-platform issues, quantum weakness, lack of AI optimization, and real-life testing problems, and makes suggestions for targeted improvements to augment adaptability, efficiency, and long-term security resiliency of ECC in cloud settings.

Future Directions

As ECC is modified for cloud systems, the next generation of parametrized ECC must focus on flexibility, the emergence of new technologies, and quantum resilience. The next generation of ECC needs to allow for flexibility in cipher sizing, be interoperable within blockchain and federated learning architectures, hybrid with post-quantum techniques, and be responsive to multi-cloud and edge ecosystem standardization efforts.

Adaptive ECC models with tunable cipher size

Coming future ECC schemes should be designed with the ability to dynamically adjust cipher size and curve parameters based on context—such as device or endpoint capability, sensitivity of data, and constraints from the network. An adaptive library could leverage machine learning to switch between using compressed point versus uncompressed or dynamically vary key size at run time, offering the most efficiency in the heterogeneous cloud of cloud and edge [17].

Received: August 02, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

ECC integration with blockchain and federated learning

Integrating ECC with blockchain and federated learning (FL) has the potential for secure, decentralized authentication and model training that preserves privacy. In edge–fog–cloud systems, ECC protects transactions and model updates, while the blockchain guarantees auditability. Future work will need to focus on lightweight ECC-based authentication in FL pipelines and consensus mechanisms [18].

Post-quantum ECC hybrids and AI-driven encryption orchestration

As quantum threats surface, hybrid ECC–PQC methods (i.e., ECC + Kyber) will enable a graceful migration process. Under AI control, encryption orchestration engines can apply classical, hybrid, or entirely PQC algorithms dynamically based on the quantum risk and performance requirements associated with the task. These stacks could be adaptive and change modes based on quantum risk to facilitate long-term protections [19].

ECC standardization for multi-cloud and edge computing

Existing ECC implementations do not provide robust standards for multi-cloud and edge implementations. To facilitate widespread cross-platform and cross-vendor interoperability, the relevant industry and standardization bodies must define profiles for ECC usage for multi-access edge computing (MEC) (ETSI) and for multi-cloud APIs. The SDKs provided by cloud service providers (CSP) should outline within their documentation the trade-off between cipher-space in relation to compression and context-aware cipher selection [20].

Through suitable context-aware ECC frameworks that integrate dynamic cipher evolution, blockchain/FL integration, PQC hybridization, and standard compliance, ECC can meet the evolving needs of modern cloud – and provide scalable security and resilience. Such contexts inspire the research footprints that crypt Analyst, systems engineer, and cloud architect.

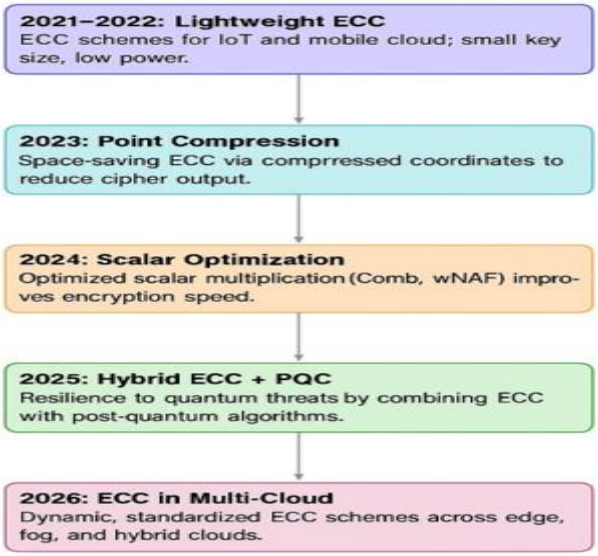


Figure 3: Roadmap for Cipher-Efficient ECC Architectures in Cloud Computing.

Received: August 02, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Figure 3 portrays a progressive roadmap for cipher-efficient ECC models in cloud computing, depicting the development from lightweight encryption for the IoT to post-quanta hybrid models, and multi-cloud models as standardized.

The milestones indicate the transitions in thinking or implementing a more secure way of performing a task, anticipating scalability while optimizing performance and minimizing computational overhead and/or cipher space**.**

Conclusion

The overall grand conclusion from this study is that ECC has tremendous potential for cloud computing environments considering strategies for optimizing cipher spaces. ECC provided advantages over traditional schemes by virtue of smaller key sizes and reduced system-wide costs from being more efficient with computing; however, the distribution of ECC-based architectures in the space currently lacks full cipher space efficiencies across platforms. Though the techniques to optimize cipher space like point compression, optimized scalar multiplication, and hybrid models (e.g., ECC + AES) can reduce ciphertext overheads and impact real-time processing performance, there are not many examples of promoting a holistic application of all three advantages in current implementations. Furthermore, despite the emergence of lightweight ECC and identity-based ECC, there appears to be little emphasis on adaptive, quantum-resilient, and AI-enabled optimization strategies whereby encryption can dynamically adjust to meet demand in a cloud-like context. There also appears to be minimal emphasis on adaptability for cross-platform deployment and accommodating real-world scalability via effective and representative benchmarking. To realize the potential of ECC and elevate security within cloud data infrastructures, researchers looking to advance ECC must explore flexible, interoperable and quantum-hardened ECC designs explicitly pursuing cipher space as a key performance indicator.

Acknowledgement

The authors express their sincere gratitude to the Department of Mathematical Sciences, GITAM (Deemed to be University), Visakhapatnam, India, for their support and encouragement throughout the preparation of this manuscript. Special thanks are extended to colleagues and reviewers for their valuable feedback, which has helped improve the clarity and quality of this work.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Received: August 02, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Author Contributions

CH. Neelima: Conceptualization, Literature Review, Formal Data Analysis, Investigation, Writing, Original Draft Preparation.
Dr. CH. Suneetha: Supervision, Project Administration, Methodology, Validation, Writing, Critical Review, Editing, and Final Approval of the Manuscript.

Devathi V N V Laxmi Alekhya: Literature Review, Data Curation, Resources.
Dr. Mutyala Suresh: Writing – Review & Editing..

Ethics Approval

Not applicable. This study does not involve any human participants or animals requiring ethical clearance.

Data Availability

The data supporting the findings of this study are available from the corresponding author upon reasonable request.

Abbreviations

Abbreviation	Description
ECC	Elliptic Curve Cryptography
ECC-LW	Lightweight Elliptic Curve Cryptography
ECC-IB	Identity-Based Elliptic Curve Cryptography
CSP	Cloud Service Provider
CPU	Central Processing Unit
GPU	Graphics Processing Unit
IoT	Internet of Things
PKI	Public Key Infrastructure

References

1. Anas, M., Imam, R., & Anwer, F. (2022, January 27). Elliptic curve cryptography in cloud security: A survey. In Proceedings of the 2022 12th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 112–117). IEEE. https://doi.org/10.1109/Confluence52989.2022.9734138
2. Rehman, S., Talat Bajwa, N., Shah, M. A., Aseeri, A. O., & Anjum, A. (2021). Hybrid AES-ECC model for the security of data over cloud storage. Electronics, 10(21), Article 2673. https://doi.org/10.3390/electronics10212673

Received: August 02, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

3. Li, M., & Hu, S. (2024). A lightweight ECC-based authentication and key agreement protocol for IoT with dynamic authentication credentials. Sensors, 24(24), Article 7967. https://doi.org/10.3390/s24247967
4. Rao, B. R., & Sujatha, B. (2023). A hybrid elliptic curve cryptography (HECC) technique for fast encryption of data for public cloud security. Measurement: Sensors, 29(1), Article 100870. https://doi.org/10.1016/j.measen.2023.100870
5. Gadde, S., Rao, G. S., Veesam, V. S., Yarlagadda, M., & Patibandla, R. S. M. L. (2023). Secure data sharing in cloud computing: A comprehensive survey of two-factor authentication and cryptographic solutions. Ingénierie des Systèmes d'Information, 28(6), 1467–1477. https://doi.org/10.18280/isi.280604
6. Tanksale, V. (2024). Efficient elliptic curve Diffie–Hellman key exchange for resource-constrained IoT devices. Electronics, 13(18), 3631. https://doi.org/10.3390/electronics13183631
7. Roy, S., & Khatwani, C. (2017). Cryptanalysis and improvement of ECC-based authentication and key exchanging protocols. Cryptography, 1(1), 9. https://doi.org/10.3390/cryptography1010009
8. Zhou, Y., & Leung, V. C. M. (2019). Provably secure lightweight mutual authentication and key agreement protocol for IoT-enabled cloud computing. Future Generation Computer Systems, 91, 244–251. https://doi.org/10.1016/j.future.2018.08.038
9. Huang, T., & Zhao, J. (2025). Optimizing ECC key management in multi-tenant IaaS architectures. Future Generation Computer Systems, 148, 70–82. https://doi.org/10.1016/j.future.2024.11.012
10. Prazeres, J., Pereira, M., & Pinheiro, A. M. G. (2024). Quality evaluation of point cloud compression techniques. Signal Processing: Image Communication, 128, Article 117156. https://doi.org/10.1016/j.image.2024.117156
11. Pundir, M., & Kumar, A. (2025). An efficient conference key agreement protocol suited for resource-constrained devices. *Journal of Parallel and Distributed Computing, 196*, Article 105011. https://doi.org/10.1016/j.jpdc.2024.105011
12. Amanlou, S., Hasan, M. K., & Abu Bakar, K. A. A. (2021). Lightweight and secure authentication scheme for IoT network based on publish–subscribe fog computing model. *Computer Networks, 199*, Article 108465. https://doi.org/10.1016/j.comnet.2021.108465
13. Wang, N., Matthaiou, M., Nikolopoulos, D. S., & Varghese, B. (2020). DYVERSE: DYnamic vertical scaling in multi-tenant edge environments. *Future Generation Computer Systems, 108*, 598–612. https://doi.org/10.1016/j.future.2020.02.043
14. Popoola, O., Rodrigues, M. A., Marchang, J., Shenfield, A., Ikpehai, A., & Popoola, J. (2024). An optimized hybrid encryption framework for smart home healthcare: Ensuring data confidentiality and security. *Internet of Things, 27*, Article 101314. https://doi.org/10.1016/j.iot.2024.101314
15. Rostampour, S., Safkhani, M., Bendavid, Y., & Bagheri, N. (2020). ECCbAP: A secure ECC-based authentication protocol for IoT edge devices. *Pervasive and Mobile Computing, 67*, Article 101194. https://doi.org/10.1016/j.pmcj.2020.101194

Received: August 02, 2025

Volume 38 No. 6s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

16. Lopez, L. J. R., Millan Mayorga, D., Martinez Poveda, L. H., Amaya, A. F. C., & Rojas Reales, W. (2024). Hybrid architectures used in the protection of large healthcare records based on cloud and blockchain integration: A review. Computers, 13(6), Article 152. https://doi.org/10.3390/computers13060152
17. Baabdullah, T., Alzahrani, A., Rawat, D. B., & Liu, C. (2024). Efficiency of federated learning and blockchain in preserving privacy and enhancing the performance of credit card fraud detection (CCFD) systems. *Future Internet, 16*(6), 196. https://doi.org/10.3390/fi16060196
18. Rajagopal, S. M., Muthuraman, S., & Buyya, R. (2025). Leveraging blockchain and federated learning in Edge-Fog-Cloud computing environments for intelligent decision-making with ECG data in IoT. Journal of Network and Computer Applications, 233, Article 104037. https://doi.org/10.1016/j.jnca.2024.104037
19. Kumar, M. (2022). Post-quantum cryptography algorithm's standardization and performance analysis. Array, 15, Article 100242. https://doi.org/10.1016/j.array.2022.100242
20. Liang, B., Gregory, M. A., & Li, S. (2022). Multi-access edge computing fundamentals, services, enablers and challenges: A complete survey. Journal of Network and Computer Applications, 199, Article 103308, 1–20. https://doi.org/10.1016/j.jnca.2021.103308

Received: August 02, 2025