IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, June 2025
Impact Factor: 7.67

Secure Data Transfer in Cloud Computing Using the Elliptic Curve Diffie–Hellman (ECDH) Algorithm

Mr. Pradeep Nayak*[1], Lohit M Patgar*[2], Farhan*[3], Pranam*[4], Ravikumar*[5]
Department of Information Science and Engineering[1-5]
Alva's Institute of Engineering and Technology, Mijar, Karnataka, India-

Abstract: *Cloud computing provides flexible and scalable data storage and processing, but ensuring secure data transfer remains a critical challenge. Traditional RSA-based cryptographic key exchange systems, while reliable, are increasingly burdened by lengthy key generation times and large key sizes. Elliptic Curve Diffie–Hellman (ECDH) has emerged as a powerful alternative, offering equivalent security with smaller key sizes, lower computational overhead, and substantially faster execution—often 10× faster in shared-secret calculations and ~60× faster in key generation compared to RSA kumarasenau.medium.com.Comparative benchmarks showing ECDH-based schemes outperform RSA counterparts in encryption latency and resource use .Hybrid encryption frameworks (e.g., ChaCha20+ECDH) achieving 2 ms encryption time and 15.8 ms key generation, far surpassing RSA/AES and Blowfish/ECC alternatives researchgate.net.We also evaluate curve selection strategies, security enhancements like perfect forward secrecy, public key validation, and the integration of ECDH with advanced symmetric encryption in large-scale cloud environments. Finally, we explore future directions involving post-quantum integration and blockchain-based integrity mechanisms, making a compelling case for ECDH as a modern, efficient, and secure protocol for protecting cloud data in transit*

Keywords: *Cloud computing*

I. INTRODUCTION

Cloud computing has transformed the digital landscape by offering scalable, on-demand access to processing power, storage, and applications over the internet. This model enables users and organizations to store, process, and share massive datasets without investing heavily in local infrastructure. However, entrusting data to remote cloud environments introduces serious security concerns, particularly regarding data in transit. Ensuring confidentiality, integrity, and authenticity is paramount, as cloud-stored information frequently traverses unsecured networks and multi-tenant environments.

Traditional cryptographic methods, such as RSA-based key exchange, provide strong security guarantees but are resource-intensive and exhibit performance bottlenecks, especially when key lengths reach 2048–3072 bits. These limitations impact latency, computational load, and scalability. To address these challenges, Elliptic Curve Diffie–Hellman (ECDH) has emerged as a powerful alternative. Leveraging the mathematical hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP), ECDH enables equivalent security with substantially smaller key sizes, resulting in significantly lower computational overhead blog.heycoach.in.

ECDH fits naturally into cloud contexts for several reasons:

• Efficiency: ECDH key-generation and shared-secret derivation typically require only milliseconds—dramatically faster than equivalent-strength RSA operations blog.heycoach.in.

• Compactness: A 256-bit ECC key offers similar security to a 3072-bit RSA key, reducing storage, bandwidth, and processing requirements .

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 5, June 2025 Impact Factor: 7.67

• Forward Secrecy: Using ephemeral ECDH (ECDHE), cloud systems can ensure that each session has a unique key, protecting past communications even if long-term keys are compromised ijcsit.com+11blog .cloudflare.com+11en.wikipedia.org+11.

Moreover, cloud providers are rapidly adopting ECDH-based protocols: for instance, popular platforms like AWS Payment Cryptography now support ECDH for secure key exchange in payment systems aws.amazon.com. Meanwhile, major web services (e.g., Cloudflare) and TLS libraries rely on ECDHE to offer fast and secure encrypted connections .

This paper reviews ECDH for secure data transfer in cloud computing, covering:

1. Mathematical framework and security foundations.
2. Performance comparisons with traditional RSA methods.
3. Hybrid implementation models (e.g., combining ECDH with symmetric ciphers like AES or ChaCha20).
4. Curve selection, forward secrecy, and real-world adoption.
5. Future directions, such as quantum-resistant and blockchain-integrated approaches.

By synthesizing theoretical underpinnings with practical benchmarks, implementation strategies, and emerging trends, this review aims to offer a well-rounded perspective on how and why ECDH is becoming a keystone for secure and efficient cloud data transfer.

II. LITERATURE SURVEY

An array of academic contributions underscores the effectiveness of ECDH in cloud environments, offering both performance and security advantages:

2.1 ECDH for Big Data Cloud Systems

Subramanian & Tamilselvan (2020) introduced an ECDH-based encryption scheme tailored for big data clouds. Their evaluation revealed encryption times approximately 70% faster than comparable RSA, MRSA, and MRSAC methods.

2.2 ChaCha20 + ECDH Hybrid Model

A 2025 benchmark study showed that combining ECDH with ChaCha20 yielded only 2 ms encryption latency and 15.8 ms key-generation time, significantly outperforming classic RSA/AES and Blowfish/ECC configurations.

2.3 ECC-Based Cloud Security Framework

Jia Cui et al. (2016) proposed a dual ECDH–ECC framework for authentication and data encryption in cloud services. They noted it provided both lower computation costs and enhanced speed, making it suitable for large-scale deployment.

2.4 ECC Survey for Cloud Security

Imam et al. (2022) presented a comprehensive overview of ECC procedures in cloud security, highlighting ECC's advantages in smaller key size, improved processing efficiency, and safer transmission relative to traditional RSA.

2.5 Hybrid Blowfish/AES With ECDH

A 2025 experimental setup involving Blowfish and AES, both keyed through ECDH, exhibited improved performance in encrypted search and data recovery — highlighting the applicability of ECDH throughout hybrid paradigms.

2.6 ECC + SHA 256 for Client–Cloud Assurance

Earlier works, such as Krishna et al. (2014), implemented ECDH with ECC encryption and SHA 256-based integrity checking in client–cloud systems, reporting faster key generation compared to RSA approaches.

III. IMPLEMENTATION IN CLOUD DATA TRANSFER

3.1 Hybrid Encryption Model

ECDH is typically employed to generate a symmetric session key (e.g., for AES or ChaCha20), which in turn encrypts bulk data. This hybrid solution enables secure key exchange with efficient data protection. A recent experiment employing ChaCha20 + ECDH had a key generation time of 15.8 ms and encryption time of 2 ms—well ahead of RSA/AES (2532 ms key generation) and Blowfish/ECC combinations

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, June 2025
Impact Factor: 7.67

IV. PERFORMANCE BENEFITS

4.1 Key Exchange Efficiency

Compared to RSA, ECDH delivers faster key operations: key generation and shared-secret computation are typically 60–70% faster, with lower CPU and memory overhead .A typical benchmark showed 187 ms decryption using ECC vs. 10,957 ms using RSA in cloud simulation environments

4.2 Balanced Operations

Unlike RSA's asymmetric workload, ECDH performs both public and private key operations in similar time, simplifying performance planning

V. ENHANCED SECURITY CONSIDERATIONS

5.1 Perfect Forward Secrecy

Using ephemeral ECDH (ECDHE) ensures fresh key exchange per session, preventing future decryption even if long-term private keys are compromised stackoverflow.com.

5.2 Curve Selection

• Curve25519/X25519: Known for speed, side-channel resistance, and widespread adoption
• Curve448/X448: Provides stronger security (~224-bit), suitable for applications requiring additional security
• Other curves like FourQ deliver high performance via efficient endomorphisms.

5.3 Public Key Validation

Although some implementations (such as Signal) bypass public-key verification, optimal practice is to reject zero or invalid shared secrets in order to prevent subgroup attacks research.kudelskisecurity.com.

VI. PERFORMANCE EVALUATION SUMMARY

Metric ECDH (ECC-256) RSA (3072 bit)
Key Gen~15–100 ms (curve-dependent) ~2000+ ms
Shared Secret ~2 ms ~≥ 1000 ms
Encryption ChaCha20/AES ~2–5 m AES similar Decryption ~2–5 ms ~small variance, CPU heavier

VII. CONCLUSION

In summary, Elliptic Curve Diffie–Hellman (ECDH) stands out as a highly effective and efficient key exchange mechanism for cloud-based secure data transfer. By leveraging the mathematical strength of elliptic curves, ECDH achieves RSA-equivalent security with dramatically smaller key sizes, which translates into 60–70% faster key generation and shared-secret computations, and millisecond-level encryption performance when paired with high-speed symmetric ciphers like AES or ChaCha20. The inclusion of ephemeral ECDH ensures strong forward secrecy—fortifying cloud systems against future key compromise—while careful selection of curves such as Curve25519 and Curve448 enhances resistance to side-channel attacks. A growing body of literature supports these findings, from big-data cloud deployments to hybrid encryption implementations, consistently demonstrating ECDH's superior performance, scalability, and flexibility. As cloud environments advance, combining ECDH with post-quantum algorithms and blockchain-based integrity frameworks offers a promising path forward. Given its robust security, efficiency, and adaptability, ECDH offers a compelling foundation for protecting data in transit within modern cloud architectures.

REFERENCES

[1]. Subramanian & Tamilselvan (2020): ECDH in big-data cloud systems (~70% faster)
[2]. Rebwar Khalid et al. (2025): ChaCha20 + ECDH benchmark (2 ms encryption, 15.8 ms key generation)
[3]. Jia Cui et al. (2016): ECDH/ECC-based cloud security framework

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, June 2025
Impact Factor: 7.67

[4]. Imam et al. (2022): Survey of ECC in cloud security
[5]. Krishna et al. (2014): ECDH + ECC + SHA 256 client–cloud assurance