

## The Rise of Indian SaaS Demand: Fueling Edge Data Centres and Transforming Businesses

Indian SaaS industry to reach 26\$ billion in revenues by 2026  
(Report By- Chiratae Ventures and Zinnov )



In recent years, the Indian Software-as-a-Service (SaaS) industry has witnessed an exponential growth trajectory, positioning itself as a key player on the global stage.

In a recent report published by Chiratae Ventures and Zinnov a management consulting & VC firm in June 2023 estimates that the Indian SaaS industry was set to grow to \$26 billion in terms of revenue by 2026. It becomes imperative to address the infrastructure requirements that come hand-in-hand with this remarkable expansion. Specifically, the demand for edge data centers is set to surge, ensuring the uninterrupted delivery of SaaS solutions across the country.

The SaaS revolution in India has been fueled by a combination

of factors. Firstly, the proliferation of cloud computing and the increasing adoption of digital technologies has provided a fertile ground for SaaS companies to flourish. Secondly, the entrepreneurial spirit, technical expertise, and cost-effective talent pool in India have attracted both domestic and international investors, leading to a vibrant ecosystem of SaaS startups and established players.

The rapid growth of the Indian SaaS industry has ushered in an era of innovation and efficiency across various sectors, including e-commerce, healthcare, finance, and more. Enterprises are increasingly turning to SaaS solutions for their scalability, cost-effectiveness, and ease of implementation. This

widespread adoption has created a surge in demand for edge data centers strategically located near the end-users, enabling low-latency, high-bandwidth connections and ensuring seamless service delivery.

Edge data centers, with their decentralized architecture and proximity to users, play a crucial role in supporting the expanding SaaS landscape. These data centers bring computing power closer to the source of data generation, reducing network latency and improving overall performance. With the rise of emerging technologies like Internet of Things (IoT), artificial intelligence (AI), and 5G, the need for real-time data processing and localized data storage is becoming increasingly vital. Edge

data centers are uniquely positioned to meet these demands efficiently.

To meet the anticipated surge in demand for edge data centers, it is essential for stakeholders to prepare proactively. Infrastructure providers, telecom companies, and cloud service providers must invest in expanding their edge data center networks across India. This will require collaboration with local governments and regulatory bodies to facilitate the establishment of new data center sites, ensuring the necessary power, connectivity, and cooling infrastructure are in place.

Additionally, efforts to enhance the skill sets of professionals in the data center industry should be intensified. Training programs, certifications, and educational

initiatives can help cultivate a talent pool equipped with the knowledge and expertise to manage and operate edge data centers effectively.

As the Indian SaaS industry continues its rapid ascent, the implications for edge data center demand are significant. By embracing this transformative growth and preparing for the future, India can solidify its position as a global hub for SaaS innovation, catering to the evolving needs of businesses and consumers alike.

In conclusion, the rise of the Indian SaaS industry presents a tremendous opportunity for economic growth and technological advancement. However, it is crucial to recognize the associated infrastructure requirements, particularly the demand

for edge data centers. By proactively addressing this demand and ensuring the necessary investments and preparations, India can maximize the potential of its SaaS industry and establish itself as a global leader in the digital economy.

Exciting times lie ahead for the Indian SaaS industry and its partnership with edge data centers, ushering in a new era of connectivity, innovation, and progress.

Vuenow Group is bridging the digital infrastructure gap for edge data centers, meeting the future demand of the SaaS industry. With their expertise and solutions, they ensure seamless connectivity, low latency, and efficient data processing, empowering businesses to thrive in the evolving digital landscape.

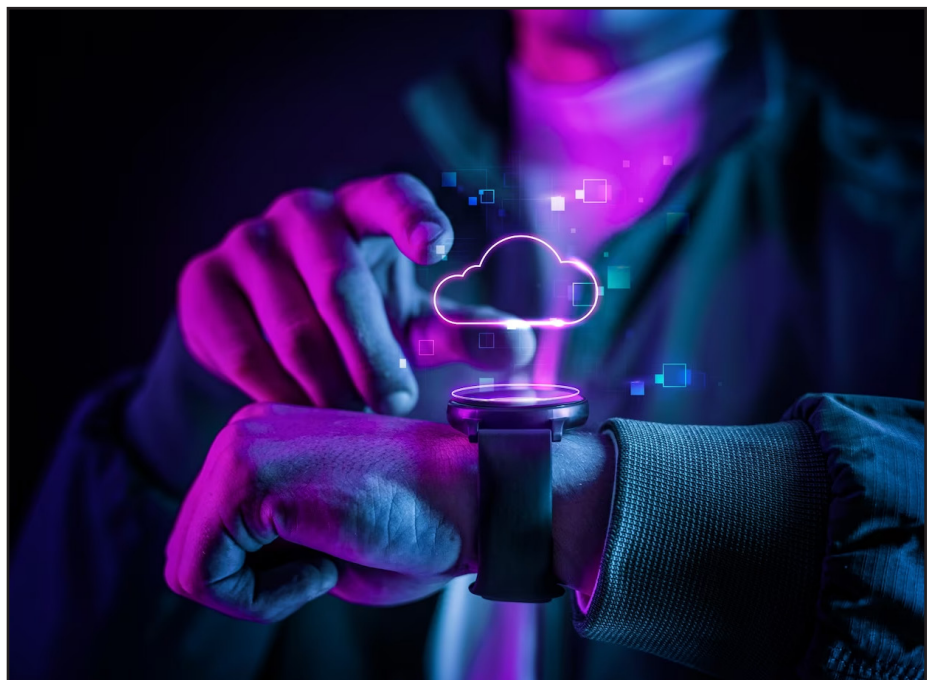
---

## Ensuring Security in Edge Computing with Post-Quantum Cryptography

As Edge computing gains prominence in addressing latency, bandwidth and privacy concerns, ensuring robust security measures becomes paramount. The exponential growth of IoT devices and the impending threat of quantum computers necessitate a long-term security solution. Post-quantum public-key cryptosystems offer a promising approach, leveraging hard mathematical encryption to protect sensitive data. Among these, lattice-based cryptography emerges as an efficient solution for implementing security measures in Edge computing centers and IoT devices.

### Challenges of Traditional IoT Models:

Traditional IoT models rely on sending vast amounts of data to the cloud for processing, leading to bandwidth constraints, increased latency, and security vulnerabilities. Edge computing, also known as FOG computing, aims to address these challenges by performing data processing at the edge devices themselves and only transmitting relevant data to the cloud. Edge computing centers minimize data transmission and latency issues while also enhancing privacy through anonymization of sensitive data.





## Securing Edge Devices:

Edge devices possess the capability to process and store sensitive user data, making them susceptible to various attacks. These attacks can occur either through the internet or via connected devices within the network. To counter these threats, a comprehensive and efficient security architecture is crucial. However, IoT devices are often resource-constrained, particularly in terms of RAM and computational capabilities.

Therefore, security algorithms must be lightweight and compatible with IoT devices. Public key techniques such as elliptic curves, Elliptic Curve Digital Signature Algorithm (ECDSA), and Elliptic Curve Diffie-Hellman (ECDH) offer advantages over traditional encryption algorithms, as they require smaller key lengths, less RAM, and reduced transmission bandwidth.

## The Rise of Post-Quantum Cryptography:

Modern public key cryptosystems rely on the hardness of mathematical problems such as the integer factoring problem and the discrete logarithm problem. However, quantum computers have the potential to break these algorithms, necessitating the development of post-quantum cryptography (PQC). PQC involves creating cryptographic systems based on mathematical problems that even quantum computers cannot easily solve.

Notably, lattice-based cryptography shows promise in PQC due to its efficient implementation on microcontrollers with 8 and 32-bit architectures.

Lattice-based cryptosystems combine strong security guarantees with high efficiency, small key sizes, and compact ciphertexts and digital signatures.

Notably, lattice-based cryptography shows promise in PQC due to its efficient implementation on microcontrollers with 8 and 32-bit architectures.

Lattice-based cryptosystems combine strong security guarantees with high efficiency, small key sizes, and compact ciphertexts and digital signatures.



## Standardizing Post-Quantum Cryptosystems:

Recognizing the need for quantum-resistant public key encryption algorithms, key agreement mechanisms, and digital signature schemes, the National Institute of Standards and Technology (NIST) initiated a call for proposals in 2016. This process aimed to standardize post-quantum cryptosystems and replace existing vulnerable systems like RSA. Organizations and individuals submitted their proposals, and it is estimated that a draft standard will be available between 2023 and 2025.

## Types of Post-Quantum Cryptography:

1. Hash-based digital signature schemes offer a secure alternative based on fewer assumptions and are expected to resist quantum computers. The classical Merkle Signature Scheme (MSS) employs a one-time signature and a Merkle tree for “many-time” signatures.
2. Multivariate cryptography relies on the Multivariate Quadratic Problem, which is NP-Complete. Decrypting an encrypted message without the secret key is challenging, even for a quantum computer. However, efficient solutions for certain polynomials are still being explored.
3. Code-based cryptosystems utilize error-correcting codes to create one-way functions. Their security is based on the difficulty of decoding a message containing random errors and recovering the code structure.
4. Lattice-based cryptosystems offer strong security guarantees, worst-to-average case reduction, high efficiency, and small key and ciphertext/signature sizes. They operate in polynomial time and are an excellent option for implementation in lot and Edge computing scenarios.






**VueNow**

**CONNECT**



 +91-120-6870800

 info@vuenow.in

 816, 8th Floor, iThum Tower A  
Sector 62, Noida, UP, India 201301

[www.vuenowonline.com](http://www.vuenowonline.com)