FROST & SULLIVAN

TRANSFORMATIONAL GROWTH LEADERSHIP

A CEO Perspective

Identity Security in the Age of AI Agents and Autonomous Digital Ecosystems:

A Conversation on AI-powered Authentication and Zero Trust Architectures

Lin Cheng-I
Chief Executive Officer, Keypasco

in conversation with

Rajarshi Dhar
Associate Director, Global Security Advisory, Frost & Sullivan, at the Cybersec India Expo 2026

In Collaboration with

Title Partner 63 SATS Cybertech
Cyber Sec India Expo
powered by heise

From digital banking and government platforms to AI-powered enterprise services, the rapid expansion of connected digital ecosystems is reshaping cybersecurity priorities. As cyber threats become more intelligent and credential-based attacks continue to rise, organizations are accelerating toward adaptive authentication, zero trust security, and identity-centric protection models.

In this exclusive Transformational Growth Leadership discussion, Lin Cheng-I shares how Keypasco is approaching the future of authentication through behavioral analysis, device-based identity verification, AI-driven risk assessment, and zero trust security architectures. Drawing on decades of experience across hardware authentication, software security, and global banking environments, he also discusses the evolution of multi-factor authentication (MFA), the growing role of AI in cybersecurity, and the importance of building ecosystem-driven security strategies for rapidly growing markets like India.

> "We believe authentication should go beyond passwords and credentials by combining behavior, device intelligence, and adaptive risk analysis into one comprehensive security model."
>
> — Lin Cheng-I, CEO, Keypasco

Why India Represents a Strategic Growth Opportunity

Rajarshi Dhar: *Keypasco has a strong global presence, but relatively speaking, your India presence is still evolving. What makes the Indian market strategically important for the company?*

Lin Cheng-I: India is an extremely attractive market for us because of both its scale and its rapid adoption of digital payment systems. The country has built one of the world's most advanced mobile payment ecosystems through UPI and related digital initiatives. At the same time, however, cyber fraud and financial security challenges are also increasing significantly.

We also saw a major opportunity emerge through the RBI's push toward reducing OTP dependency in financial services. Since authentication and identity security have been our core focus for decades, we believe this market transition creates a very strong opportunity for Keypasco.

Our company has been operating since 1987. Initially, we focused heavily on hardware authentication tokens and worked with approximately seventy-five banks globally. Over time, we shifted toward software-based authentication solutions, especially for the banking and financial services sector. Today, many banks around the world use our solutions.

In India specifically, we are focusing on three primary sectors: financial services, government, and enterprises. We see significant demand across all three because each of these environments requires secure digital access, identity protection, and scalable authentication capabilities.

Frost & Sullivan's **Transformational Growth Leadership Program** aims to honor visionary business leaders who possess the foresight and leadership acumen to drive positive change within their organizations. The leaders we celebrate hail from diverse sectors and company sizes, yet they all share an unwavering commitment to innovation and excellence.

The Evolution of MFA and Identity Security

Rajarshi Dhar: *Multi-factor authentication and identity services have existed for years. Why do you believe they are becoming even more critical today?*

Lin Cheng-I: When we first introduced our authentication solutions more than a decade ago, many customers were not even familiar with the term MFA. At that time, authentication was still heavily centered around passwords and OTPs.

Over the years, the market evolved from static authentication toward biometrics, adaptive authentication, and risk-based verification. However, we believed from the beginning that authentication should involve much more than simply combining passwords and OTPs.

Our philosophy has always been that authentication should incorporate multiple dimensions, including what you know, what you have, who you are, and what you do. That last element—behavior—is especially important because it enables much deeper contextual verification.

That is why, when we built our solution, we focused not only on replacing passwords but also on collecting behavioral and environmental parameters that could support adaptive risk analysis. We analyze device behavior, user behavior, environmental context, and usage patterns to determine whether an interaction should be trusted.

Today, the market refers to this approach as adaptive authentication or risk-based authentication, but these principles have been part of our platform architecture for many years.

Building Zero Trust Around Identity, Devices, and Risk

Rajarshi Dhar: *Organizations today are increasingly adopting zero trust architectures, especially in hybrid cloud environments. How does Keypasco approach zero trust security?*

Lin Cheng-I: For us, zero trust is much more than simply "never trust, always verify." We approach zero trust through several foundational pillars that work together as part of a broader security architecture.

The first pillar is identity verification. We combine multiple verification methods, including device intelligence, behavioral analysis, and integration with standards such as Fast IDentity Online (FIDO)-based authentication. One important differentiator is that we do not rely on traditional credential-based authentication models.

Most authentication systems in the market still depend heavily on credentials that can potentially be stolen or compromised. Our approach instead focuses on identifying the device itself and validating the relationship between the device and the user.

The second pillar is device verification. We collect and analyze multiple layers of information from the device environment, including hardware, software, firmware, network characteristics, and behavioral indicators. This helps us determine whether the device itself can be trusted.

The third pillar is AI-driven risk assessment. We combine rule-based analysis with AI-driven behavioral analysis to evaluate user activities, transactions, and login patterns dynamically.

The fourth pillar is secure network access through Software-defined Perimeter (SDP)-based architecture, where we minimize exposure to protected resources.

In addition, one of our most unique differentiators is our patented two-channel architecture, where service delivery and authentication are separated into independent channels. This significantly improves protection against attacks such as phishing, man-in-the-middle attacks, and browser-based attacks.

Using AI to Advance Authentication and Risk Intelligence

Rajarshi Dhar: ***AI is rapidly transforming cybersecurity. How is Keypasco leveraging AI within its solutions and innovation strategy?***

Lin Cheng-I: We have actually been using AI-driven concepts within our risk analysis engines for many years. Earlier, our systems relied primarily on rule-based risk analysis models with extensive profiling and transaction evaluation capabilities.

As AI technologies evolved, we integrated AI capabilities into our risk engines to improve behavioral analysis and predictive risk assessment. We use AI to analyze user behavior, evaluate transaction patterns, and predict the likelihood of risky activity before it progresses further.

More recently, we have also been working on what we describe as "zero knowledge" analysis in collaboration with researchers from Stanford University. The idea is to identify risks in payment transactions and digital environments without infringing on personal privacy or exposing sensitive information unnecessarily.

At the same time, we also see significant opportunities around AI agent security. As AI agents become more widely adopted, organizations will need strong authentication and identity frameworks capable of securing machine-driven interactions as effectively as human interactions.

Differentiating Through Passwordless and Device-centric Security

Rajarshi Dhar: ***The identity and MFA market is highly competitive today. What do you believe makes Keypasco different from other players in the market?***

Lin Cheng-I: The authentication market has existed for many years, and there are many established players globally. From the beginning, we knew we could not simply compete by offering the same approach as everyone else. We needed to build something fundamentally different.

One of the most important decisions we made early on was to avoid depending entirely on traditional credential-based authentication systems. Most authentication platforms use credentials as the core foundation for generating authentication tokens or OTPs. We believed this still created a major risk because credentials themselves remain attractive targets for attackers.

Instead, we chose to focus on device-centric authentication by leveraging unique characteristics and identifiers from the device itself. This allows us to use the user's own device as a trusted authentication mechanism while eliminating many of the risks associated with traditional credential models.

At the same time, we continue integrating emerging technologies, standards, and ecosystem capabilities into our platform. We collaborate with larger industry players, integrate broader authentication standards, and continuously evolve our platform while maintaining the uniqueness of our core architecture.

Building an Ecosystem-driven Growth Strategy in India

Rajarshi Dhar: *Partnerships are critical when entering a market like India. What kind of ecosystem and partnership strategy are you building locally?*

Lin Cheng-I: For us, partnerships are absolutely essential because India is a large and diverse market. We view ecosystem development as a foundational part of our go-to-market strategy.

First, we look for partners that understand evolving regulatory and security trends, especially in sectors such as banking and financial services. Second, we need strong channel partners because we are still relatively new in the Indian market and need local reach and customer engagement capabilities.

Third, we look for technical partners that can provide localized implementation and support services to customers. Beyond that, we also collaborate with hardware providers, enterprise solution providers, and industry-specific platform vendors so that our authentication capabilities can integrate directly into broader business environments.

Our goal is to build an ecosystem that spans industries, regions, and technology environments. We have already started collaborating with partners in the banking sector and integrating our solutions into banking platforms such as core banking systems. This allows us to scale not only across India but also into neighboring regions and international markets where similar platforms are deployed.

Preparing for the Next Era of AI-driven Security

Rajarshi Dhar: *Looking ahead over the next three to five years, what major transformation do you believe will reshape the cybersecurity market?*

Lin Cheng-I: One of the biggest changes we are already beginning to see is the rise of AI agents. During recent industry events like the RSA Conference, almost every company was discussing AI and AI-driven services.

Over the next three to five years, AI agents will become increasingly integrated into daily operations and digital environments. These systems will not simply support human activities—they will increasingly act independently and interact directly with systems, services, and other machines.

As this shift happens, authentication and security will evolve from human-centric models toward machine-to-machine trust models. Organizations will need entirely new approaches to securing AI-driven environments and autonomous interactions.

At the same time, quantum computing will become another major focus area over the longer term. Governments and industries globally are already beginning to prepare for the cybersecurity implications of quantum computing, especially within banking and government sectors.

Lin Cheng-I | CEO, Keypasco

Lin Cheng-I is the CEO and Co-Founder of Keypasco, a global cybersecurity company specializing in adaptive authentication, passwordless security, multi-factor authentication (MFA), and zero trust architectures. Since founding the company in 2012, he has led Keypasco's international expansion across Europe, Asia, the United States, and the Middle East, supporting organizations across banking, government, healthcare, and critical infrastructure sectors.

Lin brings a multidisciplinary background spanning engineering, consulting, finance, manufacturing, and cybersecurity. He began his career in hydraulic and civil engineering before transitioning into consulting and finance, where he developed expertise in mergers and acquisitions and strategic business development.

Under his leadership, Keypasco has developed expertise in device-centric authentication, behavioral intelligence, AI-driven risk analysis, and trust-based access management. The company holds international patents in device authentication, geolocation binding, and passwordless technologies, while actively advancing AI-powered fraud prevention and continuous authentication capabilities for autonomous digital ecosystems.

Rajarshi Dhar | Associate Director, Frost & Sullivan

Rajarshi Dhar serves as Associate Director for Global Security Advisory at Frost & Sullivan and is the subject matter expert for the Security Advisory practice across the Middle East, Africa, and South Asia. He specializes in cybersecurity, cloud technologies, and digital transformation, with expertise spanning growth consulting, market intelligence, and strategic advisory. Rajarshi holds an MBA in Marketing from the New Delhi Institute of Management and a Bachelor's degree in Electronics & Communication Engineering from North Maharashtra University.

Ready to Lead the Transformation?

- **Book a Growth Strategy Session:** Align your growth roadmap with Frost & Sullivan's Visionary Growth Pipeline™ Dialog.
- **Engage with Growth Experts:** Co-design AI-enabled, data-driven operating models that scale industry-specific and commercial impact.
- **Share Your Transformation Story:** Position your organization as a transformation leader through Frost & Sullivan's Transformational Growth Leadership platform.
- **Join the Growth Council:** Collaborate with industry leaders shaping the future of your ecosystem.
- **Nominate for Best Practices Recognition:** Be recognized for excellence in growth strategy, execution, and customer impact.
- **Demonstrate Industry Positioning on the Frost Radar™:** Benchmark your growth performance and innovation strength against industry competitors.
- **Activate Brand & Demand Growth:** Accelerate awareness, engagement, and revenue growth through integrated brand and demand generation strategies.

Annexure: Advancing Identity Security in the Era of AI and Zero Trust

As digital ecosystems continue expanding across banking, government, and enterprise environments, organizations are prioritizing adaptive authentication, identity-centric security, and zero trust architectures to secure users, devices, and digital interactions.

To support organizations navigating this transformation, Frost & Sullivan provides forward-looking intelligence across identity security, adaptive authentication, AI-driven cybersecurity, and zero trust transformation, including:

- Zero Trust Architecture: Next-generation Cybersecurity Framework for Digital Enterprises
- Growth Opportunities in AI-driven Cybersecurity and Digital Risk Intelligence
- AI-driven Identity and Access Management
- The Role of Identity Threat Detection and Response in Holistic Identity Security
- Zero-trust Browser Security Market, Global, 2025–2030

Together, these analyses reinforce the central themes explored in this Transformational Growth Leadership discussion: adaptive authentication, device-centric identity security, AI-driven risk intelligence, ecosystem-driven cybersecurity, and the future evolution of zero trust architectures.

YOUR TRANSFORMATIONAL GROWTH JOURNEY STARTS HERE

Frost & Sullivan's Growth Pipeline Engine, transformational strategies and best-practice models drive the generation, evaluation, and implementation of powerful growth opportunities.

Is your company prepared to survive and thrive through the coming transformation?

Join the journey. →

FROST & SULLIVAN