comviva
A TECH MAHINDRA COMPANY

Navigating the **Complexities of Telecom Security** with **CPaaS**

Executive Summary

In today's digital era, telecom players provide businesses with the information highways that carry personal data, financial data, health data, and other forms of sensitive data. With the rise of the tech-savvy consumer, the age of PBX and siloed communication has come to pass. In response, telcos have done away with their legacy portfolios and replaced them with cloud communication solutions and Communication Platform as a Service (CPaaS) offerings.

This, however, also makes them the prime target of malicious actors. Threats abound in the bold new world of cloud and API-driven communication networks that carry **A2P**, **P2A**, **P2P**, and **M2M** traffic. What this means, is that telcos will need to double down on data security to protect the interests of enterprises and their customers alike.

In this whitepaper, we observe the key threats in the evolving landscape of telecom, why AI will be crucial to combat security risks and fraudulent activity across networks, and the key practices you can adopt to secure and tamper-proof your CPaaS and cloud-based services.

The Evolving Threat Landscape in Telecom

The communication networks that drive today's digitally powered world are infinitely more complex than they were in the pre-internet era. Not only do they carry different types of traffic, but also more and more sensitive data in the form of financial information, one-time passwords, health metrics, and Personal Identifiable Information (PII).

Cloud-based services like CPaaS enable telcos to move this information via multiple protocols, within and across channels. Although such tools have become essential in an omnichannel world, they have also become the foremost targets of attackers.

In fact, communications was the **3rd most targeted sector in 2021**,[1] with the type of attacks gaining unprecedented complexity. In the first quarter of 2022 alone, the telecom industry was the target of nearly 1,500 attacks.[2] Through each attack, massive volumes of sensitive data can be compromised, as evidenced by a single instance of security lapse which left millions of SMS messages exposed to unrestricted access.[3]

1 https://www.darkreading.com/attacks-breaches/corporate-networks-saw-50-more-attacks-per-week-in-2021-

2 https://www.fiercetelecom.com/telecom/single-telecom-accounted-20-ddos-attacks-q1-lumen-finds

3 https://techcrunch.com/2019/12/01/millions-sms-messages-exposed/

Data Breaches and Fraud

An increasingly expensive affair for telcos and customers

It is not surprising then, that each event of data breach can cost dearly to telecom organizations – not only in the form of regulator-imposed fines but also erosion of consumer trust and loss of reputation in the market. Moreover, organizations also incur the operational burden of investigating and responding to breaches, legal fees, and revenue losses through lost customers. A Statista report estimates that these costs can amount to **$9.48m in an average data breach in the United States**.

Similarly, fraudulent activity across communication networks cost nearly $48bn to customers, and $44bn to communication providers in 2020.[4] Frauds can not only hit the customers' pockets directly, they can also be targeted at telecom organizations. Fraudulent activity that targets telecom organizations typically exploits network loopholes – some common tactics include grey routes, SIM boxing, smishing, and other network manipulation techniques. Moreover, telecom frauds also result in revenue leakages, which amounted to a whopping $92bn in 2020.[5]

An Overview of Threat Vectors and Fraud Risks in Telecom

It is not just the cost of frauds and data breaches that's rising over the years, but also their complexity and variety. Here are some of the key data security risks underpinning the modern telecom landscape:

- CPaaS deployments are prone to API security issues like **exposure of credentials** that compromise the API infrastructure, **API abuse**, or security vulnerabilities in the CPaaS code itself.
- Vulnerable APIs may be targeted through **SQL injection** or **cross-site scripting (XSS)** attacks, which enable attackers to execute foreign queries or code within trusted environments.
- CPaaS integrations with 3rd parties can also turn into a vulnerability if they are not secured. So can **unsecured voice and data flow**, especially in 5G networks, which are software-based.
- **Artificial Inflated Traffic (AIT)** is a tactic where attackers generate a high volume of fake traffic via websites or mobile apps. In fact, estimates suggest that 20% of CPaaS traffic could be attributed to AIT phishing.[6]
- In some cases, **logs of CPaaS data** flow and store operations contain sensitive information, which can be compromised if left unsecured.

Similarly, fraudulent activity is becoming varied and complex too.

Some of the key categories include:

GREY ROUTES
Making use of unsanctioned, cheaper routes for A2P traffic.

IDENTITY THEFT
Involves theft of personal data to gain control of the financial accounts of the victim through smishing or other means.

SIM FARMING
Exploiting channels that are cheaper than traditional A2P to inflate the results of business messaging.

SIM BOXING
A SIM farming technique used in grey routes, it is used to make international calls at cheaper rates by disguising them as local calls.

SIM SWAPPING
The attacker steaks the SIM card (usually an eSIM) and uses it to commit subscription fraud or for financial gains.

Compliance Mandates Data Security in the Modern Telecom Landscape

With the growing activity of malicious actors and the scope of security risks, regulations like the GDPR are tightening scrutiny and imposing greater obligations on telcos. These moves come in the form of obligations like:

- Notifying customers about data breaches within a set time-period.
- Ensuring data portability to respond to customers' requests for copies of their personal data.
- Payment of heftier fines in the case of a breach of sensitive personal data.

In a way, regulations are acting as a positive force urging telcos to adopt stronger security practices and privacy-by-design principles within their service offerings.

4 https://riskandassurancegroup.org/rag-rafm-survey-2020/#report

5 https://riskandassurancegroup.org/rag-rafm-survey-2020/#report

6 https://www.livemint.com/news/india/cpaas-firms-combat-ait-phishing-attacks-11687886821968.html

Evolving Data Security to Combat Modern Threats in Telecom

All of these factors point to the need for doubling down on data security in the telecom industry. However, such interventions must come in the form of targeted techniques that uniquely address each threat vector, and more sophisticated mechanisms for addressing modern risks within software-coded, high-velocity networks.

An Overview of Threat Vectors and Fraud Risks in Telecom

A number of approaches are available to prevent fraud and ensure data security in telecom and CPaaS. Here are the major ones:

ENCRYPTION  Encryption leverages cryptographic techniques to ensure that the data at rest, and in transit can be accessed only by the intended parties

REDACTION  This can be leveraged to mask sensitive information in logs, and to render data points like phone numbers unreadable to unauthorized parties

AUTHENTICATION  Authentication techniques are used to ensure that the person or the application accessing data or communication bridges is really who they claim to be

ZERO-TRUST  Zero trust is a technical design principle in which no party (be it applications, code, devices, or users) is trusted until they have been verified

ACCESS CONTROL  This technique goes hand in hand with zero trust. It is used to limit what users or an application can access and to confer the least degree of required privileges

DLP TECHNIQUES  Data Loss Prevention (DLP) is a collection of tools and processes that prevent the loss, misuse, and unauthorized transfer of sensitive and confidential data

IDR PROCESSES  Incident Detection and Response (IDR) plans are backed by processes and tools that are followed in the case of a breach, with the goal of restoring systems to a secure state, and limiting the scope of the damage

Artificial Intelligence

A game changer for telecom security and fraud prevention

One of the key challenges involved in securing modern telecom networks (especially CPaaS frameworks) is the volume, velocity, and variety of data traffic flowing through them. This makes it impossible to secure software-orchestrated networks with legacy techniques, wherein a team of security professionals alone cannot ensure adequate security across the communication network.

In this regard, Artificial Intelligence (AI) has proven invaluable to telecom businesses – so much so, that modern offerings like CPaaS solutions cannot be secured without them. The growing size of investments in the technology is a testament to its success, as the market for AI in telecom fraud prevention will reach ~$15bn by 2027.[7]

7 https://www.telecomreview.com/articles/reports-and-coverage/6237-fighting-telecom-fraud-with-ai

How AI Enables Fraud Detection in Telecom

One of the key challenges in detecting fraud is the changing nature of fraudulent activity. It is not possible to target each technique individually, because threat actors may resort to numerous schemes, some of which have never been used before. That's why manual processes (used by 30%) and rule-based fraud detection (used by 28%) are not effective in addressing fraudulent activity today.[8]

This is where AI comes into the picture. By observing and 'learning' the state of the network, flow of data, and access patterns during normal behavior, it can detect anomalous activity in the event of fraud. Self-learning and evolving AI algorithms can learn new patterns of fraudulent activity, and detect changing schemes of fraud used by attackers.

The upsides of AI in fraud prevention and data security in telecom are numerous. Here are the key impact areas:

TIME TO DETECT FRAUD

AI can help detect fraudulent activity up to 150% faster, and learn and notify of new fraud schemes up to 200% faster.[9]

TIME TO RESPOND

By automating manual processes monitoring for suspicious activity or figuring out a response plan against a data breach, AI can reduce the time to respond to a breach.

SECURITY POSTURE

AI enables telcos to detect security vulnerabilities like pending software patch updates, unsecured code, or malware across the contours and endpoints of the communication network.

REVENUE LEAKAGE

AI deployments bring a positive impact on telecom revenues, by enabling them to detect gray route calling, fake SIMs, and phishing attacks quickly.

LASTING RETURNS

The life cycle of AI-powered fraud prevention applications spans multiple years, and the results improve continuously over the period of deployment of the solution.

COMPREHENSIVE SECURITY

AI-powered fraud prevention leverages up-to-date information on evolving attack and fraud patterns from across the globe, and delivers comprehensive security against these risks.

By leveraging AI for fraud prevention and data security, telecom providers can plug nearly 2.22% of their annual revenues that are lost to fraudulent activity.[10] In addition, it can also help them stay compliant with new data privacy regulations like the GDPR while protecting the interests of end consumers and their enterprise customers alike.

Telecom Security Best Practices

That said, AI is deployed alongside veteran security teams to collectively combat data security risks and fraudulent activity. Networks and communication patterns will grow more complex, varied, and faster in the future. In 5G networks, users will consume over 2.7x more data,[11] and M2M traffic will grow to 50% of the overall traffic by 2025.[12] Moreover, the proliferation of conversational interfaces and embedded communication bridges in business applications will further diversify the type of traffic handled by CPaaS solutions.

Naturally, telecom security will need to evolve to prevent, detect, and mitigate risks in this increasingly complex landscape. Moreover, as threat actors begin to use GenAI and ML techniques to orchestrate attacks, the baseline of security will need to move higher up.

---

8 https://www.pipelinepub.com/Innovation-2022/AI-powered-fraud-management-prevention-detection-prevention-systems-5G-IoT/2

9 https://www.techrepublic.com/article/how-ai-fights-fraud-in-the-telecom-industry/

10 https://www.pipelinepub.com/Innovation-2022/AI-powered-fraud-management-prevention-detection-prevention-systems-5G-IoT

11 https://www.pipelinepub.com/Innovation-2022/AI-powered-fraud-management-prevention-detection-prevention-systems-5G-IoT

12 https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html#:~:text=The%20share%20of%20Machine%2DTo,devices%20and%20connections%20by%202023.

To this end, consider these practical steps to improve data security in CPaaS deployments and cloud-based communication networks:

Implement stronger authentication measures

Go beyond passwords. Implement a two-factor or multifactor authentication (2FA or MFA) to ensure that a user is really who they claim to be.

Encrypt data at rest and in motion

In software-orchestrated networks (and in analog networks, too), it is crucial to secure sensitive data while it is stored, and as it is in motion – to prevent breaches and eavesdropping attacks.

Keep all software up to date at all times

Known vulnerabilities remain a primary ransomware attack vector, which is why it is crucial to keep software up to date at all times. Leverage automation to notify your teams of pending updates regularly.

Arm your teams with AI monitoring and fraud detection tools

Manual processes and hard-coded fraud detection will never be able to combat sophisticated attempts of fraud and data breaches – or at least until it is too late. Arm them with modern, AI-based tools to detect anomalous activity.

Collaborate with security experts to audit your systems

If your organization lacks the security expertise required to assess your CPaaS deployment, join hands with experts in CPaaS security. They can help you assess your CPaaS security posture and help you close the gaps based on the findings.

Authenticate everything and trust nothing

Leverage zero trust strategies and the principle of least privilege in designing CPaaS solutions. Authenticate each user and device every time, and trust nothing by default. Moreover, don't offer more privileges to a user or a service than necessary.

Test and audit security controls regularly

Modern CPaaS systems evolve significantly over time – both in the number and type of systems they are integrated into, and in the way they are configured. That's why security testing and audits of security controls should be carried out regularly.

Understand your liability in shared responsibility models

CPaaS platforms will usually be deployed over a cloud provider's infrastructure, or in hybrid models. In such deployments, it is essential to understand the elements of the architecture that are secured by the cloud provider, and what you are responsible for.

Evolve processes to detect and weed out risks faster

Develop standard incident response plans, and devise a phishing investigation pipeline to respond to security incidents faster.

Audit your CPaaS deployment regularly

Because security risks keep evolving over time, it is important to audit your CPaaS deployment regularly. Assess your systems based on the latest security standards, and evolve your security strategy based on the results.

Next Steps

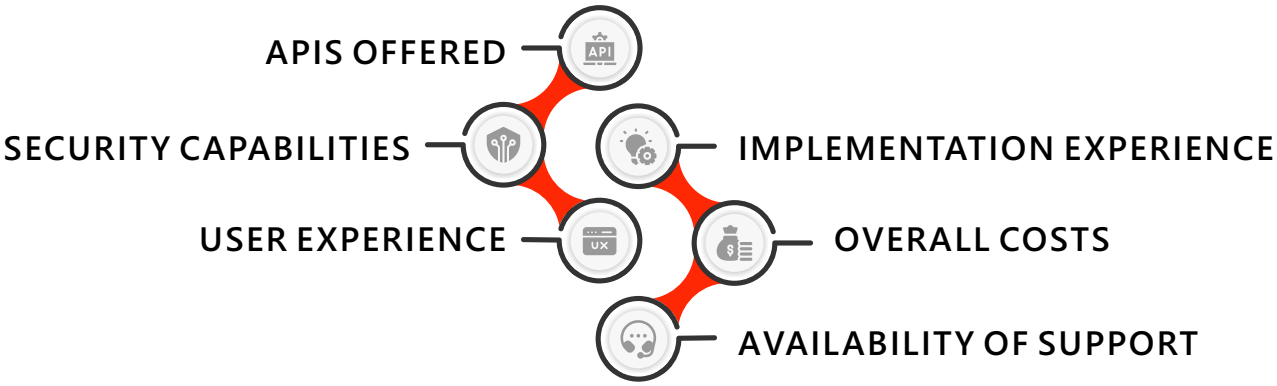
Ensuring security and preventing fraud is only going to become more challenging for telcos from here on. However, a lot is at stake – from revenue leakage to customer trust and reputation, data security will become a key determinant of success for telecom players in the market.

The good news is telecom organizations can exploit highly effective techniques to plug security loopholes and detect sophisticated fraud schemes. AI will be essential in this evolving data security landscape of telecom, where CPaaS solutions will orchestrate massive volumes of diverse traffic. In conjunction with strategies like zero trust, advanced authentication, and role-based access, telecom players can achieve holistic outcomes by advancing their data security maturity.

A Few Words on Selecting the Right CPaaS Provider

Telcos face a crucial decision in choosing the appropriate CPaaS solution. Moving forward, platforms integrated with AI-driven data security and fraud prevention will play a vital role in their operations.

Nevertheless, it is essential to maintain a broader perspective. In this regard, here are five key dimensions on which telecom players should assess CPaaS providers:



- **APIs offered:** The solution should offer core capabilities to not just implement, but orchestrate omnichannel communications with ease. Having a comprehensive set of communication APIs at hand is essential to achieve that goal. Additionally, ask your developers if the API specifications follow best security practices.
- **Security capabilities:** The CPaaS provider should ideally have AI-based data security and fraud prevention capabilities baked into the solution. If your organization is subject to data security and privacy regulations, ask your CPaaS provider (and their customers) if their solution complies with those regulations.
- **Implementation experience:** The solution should be easy to implement – in other words,

  a. comprehensive and easy-to-follow documentation,

  b. a smooth onboarding experience, and

  c. availability of APIs in the languages used at your organization

  should be a part of your preliminary selection criteria when searching for a CPaaS solution.
- **User experience:** In addition to being developer-friendly, the CPaaS implementation should fit seamlessly into the workflows of non-technical users. It's likely that these users will interact with customers in real-time, so any shortcomings will directly impact your customers' experience.
- **Overall costs:** While the cost of the solution will be a key selection criteria for most buyers, pay attention to any ongoing costs (maintenance of integrations, or hosting costs) that you may have overlooked.
- **Availability of support:** Look for providers that not only offer self-help tools (like video tutorials, explainers, and how-tos), but also quick human support for when things go south. CPaaS solutions power critical customer processes, and the ability to have issues fixed quickly is essential.

Comviva is disrupting the telecom landscape with cutting-edge communication capabilities and AI-powered security with Comviva Ngage, a bespoke CPaaS solution. Discover what Comviva Ngage can do for you by scheduling a call today!

comviva
A TECH MAHINDRA COMPANY

Comviva simplifies business complexity. Our innovative portfolio of digital solutions and platforms brings greater choice, faster time to market and flexibility, to better meet the evolving needs of our customers as they drive growth, transform, and bring efficiency. From maximizing customer lifetime value to enabling large-scale digital transformation, we partner globally with organizations in the communications and financial industry to solve problems fast and transform for tomorrow. Comviva solutions have been deployed by over 130 Communication Services Providers and Financial Institutions in more than 90 countries and have delivered the benefits of digital and mobility to billions of people around the world. Comviva is a completely owned subsidiary of Tech Mahindra and a part of the Mahindra Group.

For more information, visit us at **www.comviva.com**

www.comviva.com