অনুসন্ধান

AI-ত গোপন তথ্য দিছে নেকি? ‘ডেটা নাথাকে’ বুলি প্রতিশ্রুতি দি ধৰা পৰিল চীনা AI MiniMax— ওলাল ব্যক্তিগত লিংক

‘ডেটা সংৰক্ষণ নহয়’ (Zero Data Retention) বুলি ভৰসা দি এআই ব্যৱহাৰকাৰীৰ গোপন তথ্য চোৰাংচোৱাগিৰি কৰাৰ এক চাঞ্চল্যকৰ ঘটনা ধৰা পেলাইছে আমেৰিকাৰ চাইবাৰ সুৰক্ষা সংস্থা ‘ড্রেগছ’ (Dragos)-এ। পাঁচ মাহ ধৰি প্রায় ২০ লাখ গোপন প্রম্প্ট পঠিয়াই চলোৱা এক অভিনৱ পৰীক্ষাত পোহৰলৈ আহে যে চীনা এআই কোম্পানী ‘মিনিমেক্স’ (MiniMax)-এ ব্যৱহাৰকাৰীয়ে গোপনীয় বুলি চিহ্নিত কৰা প্রায় দুই-তৃতীয়াংশ লিংক চুৰকৈ খুলি চাইছিল—আৰু তেনে এটা লিংক ২৪ দিন পাছত চীনৰ অফিচ চেট এপত বিয়পি পৰিছিল। এই ঘটনাই এতিয়া ভাৰতৰ ষ্টাৰ্টআপ, আইটি কোম্পানী আৰু সংবাদ প্রতিষ্ঠানসমূহৰ তথ্য সুৰক্ষাৰ ওপৰতো ডাঙৰ প্রশ্ন তুলিছে।

প্রকাশ: ২৮ নৱেম্বৰ ২০২৬, দুপৰীয়া ১২:০৮



MiniMax AI Data Leak: 'Zero Data Retention' Prompts Exposed (NewzNow Graphic)

আজিকালি চফটৱেৰ ডেভেলপাৰ, সাংবাদিক, অধিবক্তা বা ব্যৱসায়ীয়ে নিজৰ গুৰুত্বপূৰ্ণ কামত এআই (AI) ব্যৱহাৰ কৰাটো তেনেই সাধাৰণ কথা। যিকোনো গোপন ফাইল বা অফিচৰ তথ্য এআই-ত দিয়াৰ আগেয়ে বহুতেই এটা বিকল্প অন কৰি লয়—**‘জিৰ’ ডেটা ৰিটেনশ্যন’ (Zero Data Retention বা ZDR)**। সহজ

অর্থত ইয়াৰ প্ৰতিশ্ৰুতি এটাই: *আপুনি যি লিখিব, সেয়া কাম শেষ হোৱাৰ লগে লগে মচি যাব; কোম্পানীৰ হাতত একোৱেই জমা নাথাকিব।*

কিন্তু সেই ভৰসা কিমান মিছা হ'ব পাৰে, তাৰেই এক চাঞ্চল্যকৰ প্ৰমাণ পোহৰলৈ আহিছে পাঁচ মাহ ধৰি চলোৱা এক ডিজিটেল ফান্দত। যোৱা ২৬ নৱেম্বৰত *ৰয়টাৰ্ছ (Reuters)* তথা *ইউনাইট ডট এআই (Unite.AI)*-ৰ প্ৰতিবেদনত ফাদিল হৈছে যে আমেৰিকাৰ খ্যাতনামা চাইবাৰ সুৰক্ষা সংস্থা **ড্ৰেগছ (Dragos)**-ৰ মুখ্য গৱেষণা বিষয়া **এইচডি মূৰে (HD Moore)** চীনা এআই ষ্টাৰ্টআপ **মিনিমেক্স (MiniMax)**-ক হাতে-লোটে ধৰা পেলাইছে। ব্যৱহাৰকাৰীয়ে স্পষ্টকৈ তথ্য জমা নকৰিবলৈ কোৱাৰ পাছতো মিনিমেক্সে সেই গোপন লিংকবোৰ খুলি চোৱাৰ প্ৰমাণ ধৰা পৰিছে।

কেনেকৈ পতা হৈছিল এই ২০ লাখ প্ৰম্পটৰ গোপন ফান্দ?

২০২৬ চনৰ জুলাইৰ পৰা নৱেম্বৰ মাহলৈকে ড্ৰেগছৰ গৱেষকসকলে বিভিন্ন এআই সেৱাৰ ওপৰত এক গোপন পৰীক্ষা চলাইছিল। ইয়াৰ বাবে তেওঁলোকে প্ৰায় **২০ লাখ বিশেষ প্ৰম্পট** এআই মডেলসমূহলৈ পঠিয়াইছিল। প্ৰতিটো প্ৰম্পটৰ ভিতৰত লুকুৱাই থোৱা হৈছিল একোটা সম্পূৰ্ণ ব্যক্তিগত ৱেব লিংক (URL) আৰু 'কেনেৰী ক্ৰেডেন্সিয়েল' অৰ্থাৎ কিছুমান নকল গোপন পাছৱৰ্ড। ইণ্টাৰনেটত এই লিংকবোৰ আন ক'তো নাছিল—গতিকে বাহিৰৰ কোনো কম্পিউটাৰে যদি পাছত সেই লিংক খুলিবলৈ চেষ্টা কৰে, তেন্তে লগে লগে প্ৰমাণ হ'ব যে কোনোবাই গোপনে ব্যৱহাৰকাৰীৰ প্ৰম্পটটো চুৰ কৰি ৰাখিছে।

ফলাফল দেখি চাইবাৰ সুৰক্ষা বিশেষজ্ঞসকলৰ চকু কপালত উঠিল:

- **'তথ্য জমা নাথাকে' বুলি কোৱাৰ পাছতো চকুৰ আৰৰ খেল:** জুলাইৰ পৰা অক্টোবৰৰ ভিতৰত মিনিমেক্সৰ মডেললৈ পঠিওৱা আধাতকৈও বেছি প্ৰম্পটৰ গোপন লিংক কোনোবা স্বয়ংক্ৰিয় যন্ত্ৰই খুলি চাইছিল। তাতোকৈ ভয়ংকৰ কথা—যিবোৰ প্ৰম্পটত স্পষ্টকৈ **'কোনো তথ্য সংগ্ৰহ নকৰিব' বা Zero Data Retention** বুলি চিহ্নিত কৰা হৈছিল, তাৰ **প্ৰায় দুই-তৃতীয়াংশ** লিংকেই পঠিওৱাৰ দুদিন-তিনিদিন পাছত খুলি চোৱা হৈছিল।
- **ছিংগাপু�ৰৰ পথেৰে তথ্য সৰবৰাহ:** গৱেষক মূৰে *ৰয়টাৰ্ছক* জনাইছে যে মধ্যৱৰ্তী এপিআই (API) সেৱাৰ মাজেৰে পঠিওৱা লিংকবোৰ বাৰে বাৰে এটা **ছিংগাপু�ৰৰ ইণ্টাৰনেট সংযোগৰ** পৰা খোলা হৈছিল। মন কৰিবলগীয়া কথাটো হ'ল—কোনো স্বাধীন কোম্পানীয়ে নিজাকৈ চাৰ্ভাৰত এই মডেল চলালে তথ্য লিক হোৱা নাছিল; কেৱল যেতিয়াই অনুৰোধবোৰ মিনিমেক্সৰ নিজা ক্লাউডলৈ গৈছিল, তেতিয়াই এই কাণ্ড ঘটিছিল।
- **চীনৰ অফিচ চেটত ওলালগৈ গোপন লিংক:** এটা ঘটনাই সকলোকে স্তম্ভিত কৰিলে। ড্ৰেগছে মিনিমেক্সলৈ এটা গোপন লিংক পঠিওৱাৰ ঠিক **২৪ দিন পাছত** সেই একেটা লিংক বাইটডেন্স (ByteDance)-ৰ অফিচ চেট এপ **ফেইশু (Feishu)**-ৰ এটা গ্ৰুপত ওলাই পৰে—আৰু মাত্ৰ দুই মিনিটৰ ভিতৰতে **বেইজিং আৰু ছাংহাইৰ তিনিটা কম্পিউটাৰ আৰু তিনিটা স্মাৰ্টফোনত** সেই লিংকটো খোলা হয়। যিহেতু ড্ৰেগছে সেৱা প্ৰদানকাৰীৰ সৈতে লিংকটোৰ মাত্ৰ প্ৰথম আঠটা আখৰহে ভাগ-বতৰা কৰিছিল, সেয়েহে স্পষ্ট হৈ পৰিল যে কোনোবাই গোটেই প্ৰম্পটটোৰ সম্পূৰ্ণ নকল সাঁচি ৰাখিছিল।
- **ক'ড চুৰিৰ চেষ্টা আৰু মস্কোৰ সংযোগ:** যোৱা **২২ অক্টোবৰ, ২০২৬**-ত স্বয়ংক্ৰিয়ভাৱে লিংক খোলা বন্ধ হোৱাৰ পাছতেই গৱেষকসকলে লক্ষ্য কৰে যে মিনিমেক্সৰ প্ৰম্পটত উল্লেখ কৰা গোপন চফটৱেৰ ক'ডৰ

ভঁৰালবোৰ (repositories) নকল বা ক্লঁন কৰিবলৈ চেষ্টা চলোৱা হৈছে। তদুপৰি *ছিকিং আলফা (TradingView)*-ৰ উদ্ধৃতি অনুসৰি, মিনিমেক্সলৈ পঠিওৱা লিংকৰ সৈতে জড়িত হৈ **মস্কো অঞ্চলৰ** পৰাও কিছুমান অস্বাভাৱিক ইণ্টাৰনেট গতিবিধি ধৰা পৰিছিল—যদিও ইয়াৰ দ্বাৰা ৰাছিয়াৰ ভিতৰৰ পৰাই লিংক খোলা হৈছিল নে কোনো ক'ড চুৰি হৈছিল, সেয়া এতিয়াও নিশ্চিত হোৱা নাই।

ভাৰত আৰু অসমৰ ব্যৱসায়ৰ বাবে কিয় এয়া ডাঙৰ সতৰ্কবাণী?

আজি ভাৰতৰ অসংখ্য ষ্টাৰ্টআপ, আইটি কোম্পানী, কর্প'ৰেট প্রতিষ্ঠান আনকি সংবাদ গোষ্ঠীয়েও খৰচ কমাবলৈ একেলগে বহু এআই মডেল সংযোগ কৰা 'এপিআই ৰাউটাৰ' ব্যৱহাৰ কৰে। 'ডেটা জমা নাথাকে' বুলি ভাবি বহুতেই গ্রাহকৰ ব্যক্তিগত তথ্য, বিত্তীয় খচৰা বা কোম্পানীৰ গোপন চফটৱেৰ ক'ড এনে প্লেটফর্মত পেলাই দিয়ে। ড্রেগছৰ এই অনুসন্ধানে এটা ডাঙৰ কথা শিকাই দিলে—আপুনি কোনটো এআই মডেল ব্যৱহাৰ কৰিছে সেয়াই যথেষ্ট নহয়, আপোনাৰ তথ্যখিনি কোন দেশৰ চার্ভাৰলৈ গৈছে সেয়া জনাটোহে আচল কথা। নহ'লে ভাৰতীয় কোম্পানীসমূহ কেৱল কর্প'ৰেট তথ্য চুৰিৰেই নহয়, ভাৰতৰ **ডিজিটেল ব্যক্তিগত তথ্য সুৰক্ষা আইন (DPDP Act)** ভংগৰো গভীৰ বিপদত পৰিব পাৰে।

মিনিমেক্সে নিজৰ পক্ষত কি কৈছে?

যোৱা ২৪ নৱেম্বৰত *ইউনাইট ডট এআই*-ত প্রকাশিত এক বিবৃতিত মিনিমেক্সে স্বীকাৰ কৰে যে তেওঁলোকৰ কিছুমান ফৰৱার্ডেড এণ্ডপইণ্টত থকা আভ্যন্তৰীণ নিৰাপত্তা ব্যৱস্থাই চাইবাৰ ভাবুকি পৰীক্ষা কৰিবলৈ লিংক আৰু আইপি (IP) ঠিকনাবোৰ সুৰক্ষা লগত জমা কৰিছিল—য'ত ZDR ট্রেফিকো সোমাই পৰিছিল। কোম্পানীটোৰ দাবী যে তেওঁলোকে সম্পূর্ণ বার্তালাপ সাঁচি ৰখা নাই বা তৃতীয় পক্ষক তথ্য দিয়া নাই; জমা হোৱা লিংকবোৰ মচি পেলোৱা হৈছে আৰু বর্তমানৰ বি২বি (B2B) সেৱাত সেই ব্যৱস্থা বন্ধ কৰা হৈছে। অৱশ্যে ফেইখু চেটত গোপন লিংক ওলোৱা আৰু চফটৱেৰ ক'ড ক্লঁন কৰাৰ চেষ্টা সন্দর্ভত মিনিমেক্সে কোনো উত্তৰ দিয়া নাই।

তথ্যসূত্র আৰু কৃতজ্ঞতা স্বীকাৰ: মূল প্রতিবেদন *ৰয়টার্ছ (Investing.com যোগে)*, *Unite.AI* আৰু *TradingView / Seeking Alpha*

এই খবৰটো NewzNow-ত প্রথমে প্রকাশ হৈছিল। সম্পূর্ণ খবৰ, ভিডিঅ' আৰু আপডেটৰ বাবে চাওক:
newznow.in/news/7140/ai-t-gopon-tothy-dise-neki-deta-nathake-buli-protisruti-di-dhora-poril-sina-ai-m