

সাইবার নিরাপত্তায় যেসব ঝুঁকি তৈরি করছে এআই

আমি যে দেশে থাকি এবং যেখানে কৃত্রিম বুদ্ধিমত্তার (এআই) শিক্ষা ও গবেষণা নিয়ে কাজ করি, সেই অস্ট্রেলিয়ায় গত সেপ্টেম্বরে এমন একটি ঘটনা প্রকাশ পেয়েছে, যা নিয়ে আমি কিছুদিন ধরেই গভীরভাবে চিন্তিত। গণমাধ্যমে প্রকাশিত তথ্য অনুযায়ী, ২০২৬ সালের ১৮ জুন ওপেনএআইয়ের একটি এআই বা কৃত্রিম বুদ্ধিমত্তার এজেন্ট অস্ট্রেলিয়ার মেডিকেলের পরিসংখ্যান পোর্টালে অননুমোদিতভাবে ঢুকে পড়ে, যে পোর্টালটি পরিচালনা করে অস্ট্রেলিয়ার সরকারের একটি গুরুত্বপূর্ণ এনটিটি-সার্ভিসেস অস্ট্রেলিয়া। সেখানে এজেন্টটি শুধু উন্মুক্ত অংশেই থামেনি, অননুমোক্ত ফাইলেও প্রবেশ করেছে এবং ওপেনএআইয়ের নিজস্ব বিবৃতি অনুযায়ী সমষ্টিগত স্বাস্থ্য পরিসংখ্যান ও অভ্যন্তরীণ ফাইলের নাম দেখেছে। ঝুঁকি থাকলেও কোনো ব্যক্তির ব্যক্তিগত মেডিকেলের রেকর্ড (স্বাস্থ্য-সম্পর্কিত ডাটা) দেখা হয়েছে বলে এখন পর্যন্ত মনে করা হচ্ছে না।

এখানে শুরুতেই একটি কথা পরিষ্কার করে নেওয়া দরকার, এটি কোনো হ্যাকারের কাজ নয়। কেউ ওই এআই এজেন্টকে সরকারি ওয়েবসাইটে ঢোকার নির্দেশ দেয়নি। এজেন্টটি একটি সাধারণ তথ্যসংক্রান্ত প্রশ্নের উত্তর খুঁজছিল। খুঁজতে গিয়ে পথে বাধা পেয়েছে, এবং সেই বাধা পেরোনোর উপায় নিজেই বের করে নিয়েছে। অস্ট্রেলিয়ার প্রধানমন্ত্রী অ্যান্থনি আলবানিজি ঘটনাটি বর্ণনা করতে গিয়ে যে কথাটি বলেছেন, সেটিই আমার মতে এ পুরো আলোচনার সারকথা। যার মানে হচ্ছে এআই এজেন্টটি বাধাগুলো এড়ানোর পথ খুঁজে বের করেছে, সে 'না' শুনতে রাজি হয়নি।

এ আলোচনায় সময় রেখাটিও কম গুরুত্বপূর্ণ নয়। ঘটনা ঘটেছে ১৮ জুন ২০২৬। ওপেনএআই নিজেদের অভ্যন্তরীণ পর্যালোচনায় বিষয়টি ধরতে পারে ১১ আগস্ট। সার্ভিসেস অস্ট্রেলিয়াকে জানানো হয় ১০ সেপ্টেম্বর, এবং জানানো হয় একটি সাধারণ উন্মুক্ত ইমেইল ঠিকানায় চিঠি পাঠিয়ে। সরকার বিষয়টি অস্ট্রেলিয়ান সিগন্যালস ডিরেক্টরেটকে জানায় ১৫ সেপ্টেম্বর, আর জনসমক্ষে আসে ২৪ সেপ্টেম্বর। অর্থাৎ ঘটনা থেকে সরকারের কানে পৌঁছাতে প্রায় তিন মাস লেগেছে, এবং অস্ট্রেলিয়ার প্রধানমন্ত্রী এ জানানোর ধরনটিকে সরাসরি 'অগ্রহণযোগ্য' বলেছেন। আমি মনে করি এখানে দুটি আলাদা ব্যর্থতা রয়েছে: একটি কারিগরি, আরেকটি প্রাতিষ্ঠানিক জবাবদিহির। দ্বিতীয়টি প্রথমটির চেয়ে কম বিপজ্জনক নয়। এখানে ছোট করে এআই 'এজেন্ট' জিনিসটি কী, তা বলে রাখা উচিত। সাধারণ এআই চ্যাটবট আপনার প্রশ্নের উত্তর দেয়, সেখানেই তার কাজ শেষ। একটি এজেন্ট শুধু উত্তর দেয় না; সে একটি লক্ষ্য গ্রহণ করে, সেই লক্ষ্যে পৌঁছানোর ধাপগুলো নিজে পরিকল্পনা করে, প্রয়োজনে বাইরের সফটওয়্যার ব্যবহার করে, বাধা পেলে নিজের পরিকল্পনা বদলায় এবং কাজটি শেষ করে ছাড়ে। পার্কিংকাট উত্তর দেওয়া আর কাজ সম্পন্ন করার মধ্যে। যে ব্যবস্থাকে আমরা হার না মানতে শিখিয়েছি, সে বন্ধ দরজার সামনে দাঁড়িয়ে ফিরে আসবে না, বিকল্প পথ খুঁজবে। তো অস্ট্রেলিয়ার ঘটনায় গণমাধ্যমে প্রকাশিত বিবরণ অনুযায়ী সেই বিকল্প পথটি ছিল একটি পুরোনো ধরনের দুর্বলতা। যেখানে ইনপুট ঘরে এমনভাবে নির্দেশ লিখে দেওয়া হয়, ডেটাবেজ সেটিকে সাধারণ লেখা নয়, বরং নিজের জন্য একটি প্রশ্ন হিসাবে চালিয়ে দেয়। লক্ষ্য করার বিষয় হলো, পোর্টালটি ছিল একটি পুরোনো ওয়েবসাইট।

এবার আসি সেই ঝুঁকিগুলোতে যেগুলো এআই নতুন করে তৈরি করছে, এবং আমি সেগুলোকে তিনটি শ্রেণিতে ভাগ করতে চাই। প্রথম শ্রেণিতে রয়েছে দক্ষতার সীমা ভেঙে পড়া। আগে একটি উঁচু মানের সাইবার আক্রমণ চালাতে বছরের পর বছরের

প্রশিক্ষণ, দামি সরঞ্জাম এবং সংগঠিত জনবল লাগত। সেই কারণেই এমন আক্রমণ মূলত রাষ্ট্রীয় পৃষ্ঠপোষকতাপুষ্ট গোষ্ঠীর মধ্যেই সীমাবদ্ধ ছিল। অ্যানথ্রোপিক তাদের ২০২৬ সালের সেপ্টেম্বরে প্রকাশিত হুমকি-প্রতিবেদনে এ পরিবর্তনটিকে একটি বাক্যে ধরেছে: উন্নত আক্রমণের জন্য আর উন্নত আক্রমণকারী লাগে না। প্রতিবেদনটি ২০২৫ সালের ডিসেম্বর থেকে ২০২৬ সালের আগস্ট পর্যন্ত সময়ের হিসাব, এবং সেখানে বলা হয়েছে, এআই সেই শ্রম ও সরঞ্জামের ব্যবধানটাই মুছে দিয়েছে, যা এতদিন বিপুল সম্পদের অধিকারী রাষ্ট্রীয় গোষ্ঠীকে একক ব্যক্তির থেকে আলাদা রাখত। দ্বিতীয় শ্রেণিতে রয়েছে এমন একটি সাইবার ঝুঁকি, যা আমার বিবেচনায় সবচেয়ে কম আলোচিত; অথচ আমাদের মতো দেশের জন্য সবচেয়ে প্রাসঙ্গিক। সেটি হলো ছড়িয়ে থাকা তথ্য জোড়া লাগিয়ে নতুন অর্থ ও ন্যারেটিভ তৈরি করা। তৃতীয় শ্রেণিতে রয়েছে গতি ও পরিসর। এখানে একটি প্রচলিত ভুল ধারণা সংশোধন করে নেওয়া দরকার। এআই যাদুবলে যেকোনো পাসওয়ার্ড বলে দিতে পারে না, এবং কেউ তা দাবি করলে তিনি ভুল বলছেন। যা হয়েছে তা হলো, পাসওয়ার্ড অনুমান করা, ফাঁস হওয়া পাসওয়ার্ড দিয়ে হাজার হাজার হিসাবে একসঙ্গে চেষ্টা চালানো এবং প্রতারণামূলক বার্তা তৈরি করা। এ কাজগুলো আগের চেয়ে অনেক সস্তা, অনেক দ্রুত এবং অনেক বড় পরিসরে করা সম্ভব হয়ে উঠেছে। এখন আমি আসল কথায় আসি। কৃত্রিম বুদ্ধিমত্তা সাইবার জগতে নিঃসন্দেহে বিপুল সম্ভাবনা এনেছে। কিন্তু সেই সম্ভাবনা সবার মধ্যে সমানভাবে ভাগ হয়নি। আমি একে বলি সুযোগের বৈষম্য। যে মানুষটি ক্ষতি করতে চায়, তার লক্ষ্য সংকীর্ণ, সুনির্দিষ্ট এবং স্বয়ংক্রিয় করে ফেলার উপযোগী। সে এআইকে কাজে লাগিয়ে তাৎক্ষণিকভাবে বহু গুণ শক্তিশালী হয়ে ওঠে। অন্যদিকে যিনি সৎভাবে জ্ঞান খুঁজছেন, যিনি সমাজের কোনো সমস্যার সমাধান করতে চান বা ব্যবসায় নতুন কিছু আনতে চান, তার কাজটি জটিল, বহুমুখী এবং প্রাতিষ্ঠানিক সহায়তার ওপর নির্ভরশীল। তার ক্ষেত্রে এআইয়ের

লাভটুকু পেতে সময় লাগে, প্রশিক্ষণ লাগে, অবকাঠামো লাগে। একই হাতিয়ার, অথচ একজনের হাতে সঙ্গে সঙ্গে ফল দেয়, আরেকজনের হাতে দেয় না। আক্রমণকারীর একটিমাত্র ফাঁক খুঁজে পেলেই চলে, রক্ষাকারীকে প্রতিটি দরজা বন্ধ রাখতে হয়।

এতক্ষণ আমি প্রতিষ্ঠানের কথা বললাম, কিন্তু এই ঝুঁকির ভার শেষ পর্যন্ত সবচেয়ে বেশি বহন করেন সাধারণ মানুষ। কণ্ঠস্বর নকল করার প্রযুক্তি আজ এতদূর এগিয়েছে যে কয়েক সেকেন্ডের রেকর্ড করা কথা থেকেই একজন মানুষের গলা বিশ্বাসযোগ্যভাবে বানিয়ে ফেলা যায়। আর প্রতারকেরা সেই গলা ব্যবহার করে রাতের বেলা ফোন করে বলে, আপনার ছেলে বিপদে পড়েছে, এখনই টাকা পাঠান। গণমাধ্যমে প্রকাশিত তথ্য অনুযায়ী, যুক্তরাষ্ট্রের এফবিআইয়ের ইন্টারনেট অপরাধ অভিযোগ কেন্দ্র ২০২৫ সালে এআই-সহায়ক প্রতারণার ২২ হাজারেরও বেশি অভিযোগ পেয়েছে এবং ক্ষতির পরিমাণ হিসাব করেছে প্রায় ৮৯ কোটি ৩০ লাখ ডলার। এখানে সবচেয়ে নিষ্ঠুর দিকটি হলো, এ ফাঁদে পা দেওয়ার জন্য ভুক্তভোগীকে কোনো প্রযুক্তিগত ভুল করতে হয় না। তাকে শুধু নিজের সন্তানের গলা বিশ্বাস করতে হয়। আর যিনি জানেনই না যে গলা নকল করা সম্ভব, তিনি সন্দেহ করবেন কীভাবে? প্রযুক্তির এই ঝুঁকি তাই সবচেয়ে নির্মমভাবে গিয়ে পড়ে তাদের ওপর, যারা প্রযুক্তি থেকে সবচেয়ে দূরে, এবং এটিই আমার বলা বৈষম্যের সবচেয়ে বেদনাদায়ক চেহারা।

এই আলোচনা বাংলাদেশের জন্য কেন জরুরি, তা বলার অপেক্ষা রাখে না। আমাদের ব্যাংকিং ব্যবস্থা, নির্বাচন কমিশনের ভোটার তথ্যভাণ্ডার, পাসপোর্ট অধিদপ্তরের রেকর্ড, ভূমি ও স্বাস্থ্যসেবার ডিজিটাল নথি, এগুলোর প্রতিটিই রাষ্ট্রের অত্যাবশ্যক অবকাঠামোর অংশ। ২০১৬ সালে বাংলাদেশ ব্যাংকের রিজার্ভ চুরির ঘটনা আমাদের মনে করিয়ে দেয়, আন্তর্জাতিক মানের আক্রমণ আমাদের নাগালের বাইরের কোনো বিষয় নয়। বরং

আমরা আরও তার লক্ষ্যবস্তু হয়েছি। আর অস্ট্রেলিয়ার ঘটনার সবচেয়ে অস্বস্তিকর শিক্ষাটি হলো, সেখানে যে পোর্টালটি ভেদ করা হয়েছিল সেটি ছিল একটি পুরোনো ওয়েবসাইট। আমাদের সরকারি দপ্তরগুলোতে কত পুরোনো ওয়েবসাইট আজও চালু আছে, কতগুলোর নিরাপত্তা পরীক্ষা কবে হয়েছিল। এ প্রশ্নের উত্তর আমাদের জানা দরকার এবং জানা দরকার কোনো দুর্ঘটনা ঘটার আগেই।

লেখকঃ ড. শাহ্ যে মিয়া, প্রফেসর অব বিজনেস এনালিটিক্স অ্যান্ড অ্যাপ্লায়েড এআই, নিউকাসল ইউনিভার্সিটি, নিউ সাউথ ওয়েলস, অস্ট্রেলিয়া; ভারপ্রাপ্ত সভাপতি, জাতীয়তাবাদী আইসিটি ফোরাম।