ইন্টারনেট অব থিংসের নিরাপত্তা

আবু জাফর মো: সালেক

ইনফরমেশন সিকিউরিটি স্পেশালিস্ট, বিজিডি ই-গভ সার্ট, বাংলাদেশ কমপিউটার কাউন্সিল

বর্তমানে বিশ্বে মোবাইল ফোনের পর ইন্টারনেট সংযুক্ত দ্রব্যসামগ্রী (আইওটি– ইন্টারনেট অব থিংস) একটি বড় বিপ্লব। বিশ্বে প্রতিনিয়ত নতুন নতুন কমপিউটিং ডিভাইস ইন্টারনেটে সংযুক্ত হচ্ছে। কিছুদিন আগেও শুধু ডেস্কটপ, সার্ভার, নোটবুক, মোবাইল ফোন ইত্যাদিতে ইন্টারনেটে যুক্ত হওয়ার ক্ষমতা ছিল। কিন্তু এখন আমাদের চারপাশের প্রায় সবকিছুরই ইন্টারনেটের সাথে যুক্ত হওয়ার ক্ষমতা রয়েছে। এটা হতে পারে ঠিক এই মুহূর্তে আপনার পরিধেয় হাতঘড়িটা বা অন্য যেকোনো কিছু। ইন্টারনেটে যুক্ত হওয়ার ক্ষমতাসম্পন্ন এসব যন্ত্রের (ইন্টারনেট অব থিংস) সংখ্যা উত্তরোত্তর বাড়ছে।

আইওটি ডিভাইসগুলোর ইন্টারনেটে যুক্ত হওয়ার পেছনে মূল কারণ হলো এরা ক্লাউড সার্ভারে তথ্য পাঠাতে পারে এবং এটি ব্যবহারের জন্য যেকোনো জায়গা থেকে অ্যাক্সেস করা যায়। ইন্টারনেটের মাধ্যমে ক্লাউড সার্ভারে তথ্য পাঠানোর ক্ষেত্রে দুটি পদ্ধতিতে ইন্টারনেটে যোগাযোগ স্থাপন করতে পারে– তারের সংযোগে বা তারহীন সংযোগ দিয়ে। আপনি দূরবর্তী কোনো জায়গায় থেকেও আপনার মোবাইল ফোনের মাধ্যমে বাসার অথবা কর্মস্থলের নিরাপত্তা ক্যামেরাটি চেক করতে পারবেন, ফোন স্ক্রিনে একটিমাত্র বাটন টিপে এবং সেন্সর ব্যবহার করেই আপনার ওয়াটার পাম্পের পানির স্তর চেক করতে পারবেন অথবা ওয়াটার পাম্পটি সুবিধামতো বন্ধ বা চালু করতে পারবেন। সেক্ষেত্রে ইন্টারনেট সংযুক্ত আইওটি ডিভাইসগুলোর নিরাপত্তার বিষয় লক্ষ রাখা উচিত। আইওটি দ্রব্যসামগ্রীর সবচেয়ে ঝুঁকিপূর্ণ দিক হচ্ছে, সঠিকভাবে সেটআপ না করলে এর মাধ্যমে ব্যক্তিগত নিরাপত্তায় বিঘ্ন ঘটতে পারে। উদাহরণস্বরূপ, একটি স্মার্ট মিটার যা বিলিং অথবা রিয়েল টাইম পাওয়ার গ্রিড অপ্টিমাইজেশনের জন্য ইউটিলিটি সার্ভিসেস কোম্পানিকে পাওয়ার ব্যবহারকারীর ডাটা পাঠাতে সক্ষম। এই ডাটা বা তথ্য যদি কোনো উপায়ে অবৈধ ব্যবহারকারীর কাছে পৌঁছে যায়, তাহলে অপরাধপ্রবণ ব্যক্তি গ্রাহকের বিদ্যুৎ ব্যবহারের মাত্রা দেখে বুঝতে পারে কোন বাসা ফাঁকা আছে এবং সে তার অভিপ্রেত অপরাধ সংঘটনের চেষ্টা চালাতে পারে।

প্রতিবছর সংযুক্ত ডিভাইসগুলোর বাড়ার সাথে সাথে নিরাপত্তা ঝুঁকিও খুব দ্রুত বেড়ে যাচ্ছে। আইওটি ডিভাইসগুলোর বড় নির্মাতাদের (সিসকো, এরিকসন, আইডিসি, এবিআই, ফরেস্টার এবং গার্টনার ইত্যাদি) দেয়া পূর্বাভাস অনুযায়ী ২০২০ সালের মধ্যে ২৫-৫০ বিলিয়ন ডিভাইসের মধ্যে ইন্টারনেটের সংযোগ দেয়ার পূর্বাভাস দিয়েছে এবং সেই সাথে এই সংস্থাগুলোর আইওটি ডিভাইস সংক্রান্ত অর্থনৈতিক প্রভাবের পরিমাণ দাঁড়াবে ২-৬ ট্রিলিয়নের মতো। আইওটি যন্ত্রাদি ও প্ল্যাটফর্মের সমান্তরাল বৃদ্ধি ইন্টেলিজেন্স সংস্থা অনুযায়ী সাইবার সিকিউরিটি বিষয়গুলোর ওপর প্রভাব ফেলছে। বড় নির্মাতা সংস্থা ভবিষ্যতে আরো অ্যাক্সেস নিয়ন্ত্রণ, অনুপ্রবেশের প্রতিরোধ, পরিচয় শনাক্তকরণ এবং ভাইরাস ও ম্যালওয়্যার সুরক্ষা করার জন্য বিনিয়োগ করবে। ছোট ছোট ক্ষেত্র থেকে শুরু হয়ে বাসা, ব্যবসায়, শিল্প, পরিবহন, স্বাস্থ্যসহ বিশ্বব্যাপী বিভিন্ন খাতে আইওটি যন্ত্রাধি ছড়িয়ে পড়ছে। আইওটি প্রযুক্তিগুলোর ক্ষেত্রে যেসব নিরাপত্তা ত্রুটি দেখা যায়, তা আস্তে আস্তে বিস্তৃত প্ল্যাটফর্মেও ছড়িয়ে পড়তে পারে। এক্ষেত্রে সর্বাধিক প্রচলিত কিছু ডিভাইসের নিরাপত্তা ত্রুটিই এখানে আলোচনা করা হয়েছে।

আইওটি সম্পর্কিত সাইবার ক্রাইমের মধ্যে ২০১৬ সালে ডিন কোম্পানির ওপর ডি-ডস আক্রমণ চালায় সাইবার অপরাধীরা। ডিন কোম্পানি টুইটার, সাউন্ড ক্লাউড, স্পটিফাই, রেডিডটসহ বিভিন্ন সিস্টেমকে ডিএনএস সেবা দেয়। ডি-ডস আক্রমণের মূল উদ্দেশ্য ইন্টারনেট সেবা ব্যাহত করা, যাতে ব্যবহারকারী তার প্রয়োজন অনুযায়ী নির্দিষ্ট ওয়েবসাইটগুলোতে প্রবেশ করতে না পারে। এটি একটি সমন্বিত আক্রমণ, যেখানে বিশ্বের বিভিন্ন জায়গা থেকে একাধিক কমপিউটার ▸

ব্যবহার করা হয়। নিয়ম অনুয়ায়ী কমপিউটারগুলোর অপারেটিং সিস্টেম ম্যালওয়্যার দিয়ে আক্রান্ত হয়। সঠিক সময়ে ম্যালওয়্যারটি সক্রিয় করা হয় এবং কমপিউটারকে বটনেটে (দূরবর্তী মেশিনের একটি নেটওয়ার্ক) সংযুক্ত করা হয় এবং এভাবেই ডি-ডস আক্রমণ ঘটে। যদিও ডি-ডস আক্রমণ নতুন নয়, তারপরও ডিনের আক্রমণের ক্ষেত্রে এটি একটি নতুন মাত্রা যোগ করে। কেননা, ডিন কোম্পানিতে ডি-ডস আক্রমণ কোনো কমপিউটারের মাধ্যমে ঘটেনি, এটা ঘটেছিল নিরাপত্তা ক্যামেরা অথবা নেটওয়ার্ক সংযুক্ত স্টোরেজ ডিভাইসের মাধ্যমে। ২০১৬ সালের ২০ সেপ্টেম্বর ফ্রান্সের ক্লাউড কমপিউটিং কোম্পানি OVH-এ মিরাই বটনেট দিয়ে ডি-ডস আক্রমণ করে প্রতি সেকেন্ডে ১ টেরাবিট ডাটা পাঠিয়ে এর স্বাভাবিক কার্যক্রম ব্যাহত করেছিল। গবেষকদের মতে, এসব সাইবার আক্রমণের সময় ৬ লাখের বেশি আইওটি ডিভাইস ব্যবহার করা হয়েছিল।

২০১৭ সালের মার্চ মাসে নির্মাতা প্রতিষ্ঠান ডাহুয়া (Dahua) ইন্টারনেট সুবিধাসম্পন্ন নিরাপত্তা ক্যামেরা ও ডিজিটাল ভিডিও রেকর্ডার তৈরি করে বাধ্য হয়েছিল তাদের নির্মিত বিভিন্ন পণ্যের নিরাপত্তা ত্রুটি দূর করে সফটওয়্যারগুলোকে আপডেট করতে। কারণ, এ নিরাপত্তা দুর্বলতাগুলো আক্রমণকারীকে লগইন প্রক্রিয়াটি এড়িয়ে খুব সহজেই দূরবর্তী প্রক্রিয়ার নিয়ন্ত্রণ লাভে সহায়তা করে। শুধু সফটওয়্যারের আপডেটের মাধ্যমেই তারা তাদের নিরাপত্তা ত্রুটি দূর করতে পেরেছিল, কিন্তু এ প্রক্রিয়াটি সম্পন্ন করতে গিয়ে কোম্পানির ভাবমূর্তি ক্ষুণ্ন হয়েছিল।

অনেক সংযুক্ত ডিভাইসগুলোতে আমরা গতানুগতিক ইউজার নেম ও পাসওয়ার্ড ব্যবহার করে ইন্টারনেটে প্রবেশের অনুমতি পাই, যা খুব সহজেই নিরাপত্তায় বিঘ্ন ঘটাতে পারে। যদিও আইওটি ডিভাইসগুলো দেখতে ছোট, তবুও আমাদের মনে রাখা উচিত এদেরও প্রসেসর, সফটওয়্যার এবং হার্ডওয়্যার আছে– যা ম্যালওয়্যার দিয়ে আক্রান্ত হয়ে নিরাপত্তা ত্রুটি ঘটাতে পারে, যেমন দেখা যায় কমপিউটারের ক্ষেত্রে।

আইওটি ডিভাইসের নিরাপত্তা ব্যবস্থা ও বিভিন্ন সাইবার অপরাধের পরিপ্রেক্ষিতে নিচে উল্লিখিত চেকলিস্টটি আইওটি ডেভেলপারদের অনুসরণ করা অত্যন্ত গুরুত্বপূর্ণ–

* গতানুগতিক ডিফল্ট পাসওয়ার্ড দিয়ে পণ্য তৈরি করবেন না, পণ্যটি প্রস্তুতকালে এর প্রতিটি ডিভাইসের জন্য একটি জটিল পাসওয়ার্ড ব্যবহার করুন।

* কোনো যন্ত্রে গ্রাহকের জন্য ডিবাগ অ্যাক্সেস রাখা উচিত নয়। যদিও ডিবাগ অ্যাক্সেসের ক্ষেত্রে জটিল পাসওয়ার্ড ব্যবহার করা হয়, তারপরও এর নিরাপত্তায় বিঘ্ন ঘটতে পারে।

* একটি আইওটি ডিভাইস ও ক্লাউডের মধ্যে সব ধরনের যোগাযোগ এনক্রিপ্ট করা প্রয়োজন। এক্ষেত্রে SSL/TLS ব্যবহার করতে হবে।

* কোনো ব্যক্তিগত ডাটা (উদাহরণস্বরূপ ওয়াইফাই পাসওয়ার্ড) যেন হ্যাকার খুব সহজেই অ্যাক্সেস করতে না পারে– এ ব্যাপারটি নিশ্চিত করুন। ব্যক্তিগত তথ্য সংরক্ষণের জন্য এনক্রিপশন ব্যবহার করুন।

* যেকোনো ওয়েব ইন্টারফেসটিকে এসকিউএল ইনজেকশন (SQL injection) এবং ক্রস সাইট স্ক্রিপটিং (cross-site scripting) ইত্যাদি হ্যাকিং কৌশলগুলোর বিরুদ্ধে সুরক্ষিত রাখার জন্য আদর্শ ব্যবস্থা নেয়া উচিত।

* সব আইওটি ডিভাইসে স্বয়ংক্রিয়ভাবে ফার্মওয়্যার (Firmware) আপডেট সুবিধা রাখা উচিত এবং আপডেটগুলো প্রয়োগ করার আগে অবশ্যই যাচাই করে নেয়া উচিত।

ভোক্তাদের উচিত তাদের ক্রয় করা আইওটি পণ্যের নিরাপত্তার ব্যাপারে সুনিশ্চিত হওয়া এবং ডেভেলপারের পাশাপাশি একজন ভোক্তারও উপরোল্লিখিত বিষয়গুলোর দিকে লক্ষ করা। আইওটি ডিভাইসগুলো ক্ষুদ্র এবং সীমিত ক্ষমতাসম্পন্ন। তাদের কর্মসঞ্চালনের জন্য প্রয়োজনীয় প্রক্রিয়াকরণ ক্ষমতা এবং মেমরি খুব সীমিত। প্রচুর পরিমাণে তথ্য আইওটি ডিভাইসগুলো তৈরি করে এবং বিশ্লেষণের জন্য ক্লাউডে স্থানান্তর করে। উৎপাদনকারী এবং সেই সাথে আইওটি ডিভাইস ব্যবহারকারীকে তাদের ডিভাইসগুলোর পেছনে সময় ব্যয় করতে হবে এবং তাদের লক্ষ রাখতে হবে ডিভাইসগুলো কোন ধরনের ডাটা সংগ্রহ করে, কাদের সাথে কোন ধরনের ডাটা বিনিময় করছে এবং তথ্যগুলো কীভাবে গ্রহণ করছে ও পাঠাচ্ছে। উপরন্তু, যেখানে ডাটা সংরক্ষণ করা হয় তার নিরাপত্তা সুরক্ষা দৃঢ় করতে হবে। যথাসময়ে সফটওয়্যার আপডেট করা এবং ডিভাইসের সাথে সংযুক্ত অ্যাপগুলো কমপিউটার ডিভাইসের পাশাপাশি আপ-টু-ডেট করতে হবে এবং এটা অবশ্যই করণীয়। আইওটি ডিভাইসের নিরাপত্তা বাড়ানোর জন্য উন্নত নিরাপত্তা ক্ষমতাসম্পন্ন অপারেটিং সিস্টেম, সফটওয়্যার এবং হার্ডওয়্যার নির্বাচন করাতে হবে।

প্রায় এক দশক আগে শুধু আমাদের কমপিউটার এবং কয়েক বছর আগে থেকে আমাদের স্মার্টফোনের সুরক্ষা নিয়ে কাজ করতে হচ্ছে, বর্তমানে আমাদের গৃহস্থালি, গাড়ি, পরিধেয়, এমনকি আমাদের মেডিক্যাল রিপোর্টগুলোর সুরক্ষার ব্যাপারেও উদ্বিগ্ন হতে হচ্ছে। কারণ, হ্যাকার যেকোনো দূরবর্তী জায়গায় থেকে যেকোনো ডিভাইসের মাধ্যমে ক্ষতিসাধন করতে পারে। এক্ষেত্রে আইওটি ডিভাইস নির্মাতা এবং ব্যবহারকারীকে হ্যাকারের মতোই চিন্তা করতে হবে এবং ডিভাইসগুলো এমনভাবে তৈরি করতে হবে,