

## چکیده فارسی

### ارائه چارچوب امنیت اینترنت اشیا در صنعت مراقبت سلامت

**مقدمه:** اینترنت اشیا یکی از مباحث روز فناوری در عصر جدید اطلاعات و ارتباطات می‌باشد که با فراگیر شدن کاربرد آن در صنایع مختلف به ویژه مراقبت سلامت مسئله امنیت و حریم خصوصی آن توجه زیادی را به سمت خود جلب نموده است و به موضوعی بحث برانگیز در این حوزه تبدیل شده است. لذا، وجود چارچوبی که بتواند تمامی ابعاد امنیت اینترنت اشیا اعم از الزامات، آسیب‌پذیری‌ها، تهدیدات و حملات و مکانیسم‌ها را پوشش دهد، امری ضروری تلقی می‌شود. پژوهش حاضر با هدف ارائه چارچوب امنیت اینترنت اشیا در صنعت مراقبت سلامت انجام شده است.

**روش پژوهش:** پژوهش حاضر از نوع کاربردی بوده که به روش ترکیبی (کیفی- کمی) و در چهار مرحله انجام شد. مرحله اول الزامات، آسیب‌پذیری‌ها، تهدیدات و حملات و مکانیسم‌های امنیت اینترنت اشیا با روش مرور نظام‌یافته شناسایی شد. مرحله دوم، وضعیت موجود امنیت اینترنت اشیا در ایران با روش کیفی از طریق مصاحبه با افراد مشخص شد. مرحله سوم (هم‌اندیشی خبرگان) در راستای طراحی چارچوب اولیه امنیت اینترنت اشیا در صنعت مراقبت سلامت با حضور شش نفر از متخصصان برگزار شد. در نهایت، چارچوب امنیت اینترنت اشیا در صنعت مراقبت سلامت با روش دلفی در دو دور توسط خبرگان اعتبارسنجی شد.

**یافته‌ها:** چارچوب ارائه شده در خصوص امنیت اینترنت اشیا در صنعت مراقبت سلامت در چهار بعد الزامات، آسیب‌پذیری، تهدیدات و حملات و مکانیسم طراحی شد. این چارچوب حاوی ۱۴ مؤلفه مربوط به بُعد الزامات امنیت اینترنت اشیا مبتنی بر اعتمادپذیری بود که در دو محور فرعی امنیت سایبری (محرمانگی، تمامیت، قابلیت دسترسی، حریم خصوصی، شناسایی و احراز هویت (تصدیق هویت)، کنترل دسترسی، قابلیت پاسخگویی، ممیزی و عدم انکار) و تاب‌آوری سایبری (قابلیت اطمینان، نگهداشت، ایمنی، قابلیت بقا و تحمل پذیری خطا و عملکرد) بود. بُعد آسیب‌پذیری‌های امنیت اینترنت اشیا متشکل از دو محور اصلی آسیب‌پذیری‌های ناشی از ویژگی‌های ذاتی فناوری (شامل: شش محور فرعی با ۲۰ مؤلفه) و بُعد آسیب‌پذیری‌های امنیتی اینترنت اشیا ناشی از مسائل عمومی (۱۳ محور فرعی با ۳۴ مؤلفه) بود. بُعد تهدیدات و حملات امنیتی با ۱۴ محور اصلی (دسترسی غیرمجاز، حملات فیزیکی، جعل هویت، استراق سمع و پایش، بدافزارها، تزریق، تحلیل رمز و یافتن کلید، مسیریابی، توان مصرفی، مهندسی اجتماعی، مهندسی معکوس، سرقت هویت، حملات بی‌سیم، وقفه و سیلابی) و ۴۸ مؤلفه در هر محور بود. بُعد مکانیسم در چارچوب امنیت اینترنت اشیا متشکل از ۱۲ محور اصلی (مکانیسم‌های رمزنگاری، توزیع و مدیریت کلید، طراحی امن و حفاظت فیزیکی از سخت‌افزار، مدیریت هویت دیجیتال، صرفه‌جویی در

توان مصرفی و انرژی، مدیریت اعتماد، مدیریت نگهداشت چرخه حیات سیستم، مخفی سازی داده‌ها و تصاویر، مسیریابی امن، تشخیص و

تحمل خطا و حفاظت از شبکه و بکارگیری پروتکل‌های امن برای انتقال داده) با ۸۰ مؤلفه بود

**نتیجه‌گیری:** انتظار می‌رود چارچوب ارائه شده در پژوهش حاضر به عنوان راهنمایی زمینه را برای برنامه ریزی و پیاده سازی سیستم امن

اینترنت اشیا در صنعت مراقبت سلامت فراهم نماید.

**کلید واژه‌ها:** اینترنت اشیا، چارچوب، امنیت، صنعت مراقبت سلامت