



فعالیت‌های انجام شده کاربران در اپراتورهای تلفن همراه در قالب لاگ‌های مختلف ذخیره میشوند. از آنجا که این لاگ‌ها در شناسایی انواع حملات سایبری، کشف دسترس‌های احراز اصالت نشده و همچنین یافتن الگوهای رفتاری کاربران شبکه قابل استفاده هستند، نیاز به تحلیل و بررسی آنها بیش از پیش احساس میشود. در شبکه تلفن همراه یکی از پرکاربردترین این لاگ‌ها، رکوردهای جزئیات تماس است که دارای اطلاعات فراوانی همانند شماره‌های مبدا و مقصد مشترکین، مدت زمان مکالمه، منطقه فعالیت، نوع تماس (پیامک یا تماس) و برجسبهای زمانی هستند، که این گوناگونی چالش اساسی را در تحلیل آنها مطرح می‌سازد. با استفاده از تشخیص ناهنجاری میتوان کاهش یا افزایش غیر عادی میزان ترافیک شبکه یا تماس‌های یک شخص خاص را مشخص نمود. مساله مهم برای تشخیص ناهنجاری، این است که بتوان آن را در همان زمان وقوع و یا قبل از وقوع تشخیص داد که لازمه آن، داشتن اطلاعات از پیشینه رفتار شبکه و پیشینی آنها است. تشخیص ناهنجاری برای شناسایی حملات سایبری، پاسخ به حوادث امنیتی، تشخیص خرابی سامانه‌ها و جرم‌شناسی در شبکه استفاده میشود.

هدف اصلی در این پژوهش مطالعه رفتار کاربران، پیشینی تعداد تماسها با استفاده از رکوردهای جزئیات تماس و تشخیص ناهنجاری در ترافیک شبکه تلفن همراه است. در این پژوهش، از روشهای تشخیص ناهنجاری مختلفی بر روی داده‌های تلفن همراه برای مشخص کردن داده‌های پرت استفاده و تحلیل‌هایی روی علت بروز این ناهنجاریها انجام شده است.

رکوردهای جزئیات تماس، تشخیص ناهنجاری و سری های زمانی

Call Detail Record, Anomaly Detection and Time Series

کلمات کلیدی

کلمات کلیدی انگلیسی