آنالیز انواع حملات DDOS و چگونگی تشخیص آن در رایانش ابری

فرهنگ پدیداران مقدم[1*]، عابد فلاحتی[2]، شادی منفردی[3]

۱- استادیار،گروه کامپیوتر، موسسه آموزش عالی اشراق *Padidaran@eshragh. ac. ir*

۲- دانشجوی کارشناسی ارشد، موسسه آموزش عالی اشراق بجنورد، *Mail4abed@gmail. com*

۳- کارشناسی ارشد، موسسه آموزش عالی اشراق بجنورد، *shadi. monfaredi@yahoo. com*

چکیده

امروزه رایانش ابر از موضوعات تحقیقاتی مهم به شمار می‌رود. ماهیتاً هدف آن تحکیم کاربری تجاری از طریق توسعه تکاملی بسیاری از رویکردهای موجود و فناوری‌های محاسباتی است، از جمله خدمات توزیع شده، برنامه‌ها و زیرساخت‌های اطلاعاتی متشکل از منابع اشتراکی کامپیوتر، شبکه و منابع ذخیره‌سازی. اما جنبه‌های بی همتایی از این محاسبات باعث تشدید مشکلات امنیتی شده است. یکی از مسایل امنیتی که در محیط ابر با ان مواجه هستیم، بروز حملات DDOS از طرف مهاجمان به سرورهای ابر میباشند. در این مقاله انواع حملات DDOS بررسی، تشخیص ودر نتیجه به بررسی اقدامات متقابل در برابر این حملات می‌پردازیم.

واژگان کلیدی: رایانش ابری، محیط ابر، امنیت، حملات DDOS

مقدمه

حملات ممانعت از سرویس، حملات صریحی می‌باشند که برای جلوگیری از استفاده مشروع از یک سرویس هستند. که این حملات یکی از تهدیدات اصلی علیه در دسترس بودن اینترنت است عاملین حملات DDOS به طور معمول سایت‌های مختلفی را مورد حمله قرار می‌دهد که تاثیر آنها در هر حمله متفاوت است و ناراحتی جزئی را در کاربران به همراه دارد و یا در برخی موارد ممکن است زیان‌های مالی جدی را برای شرکت هایی که به صورت آنلاین به کسب و کار می‌پردازد به بار آورد. که از بالاترین سرورها می‌توان به وب سرویس بانک ها، دروازه پرداخت کارت‌های اعتباری سرورهای روت، موتورهای معروف جستجو google و yahoo، وب سرویس های دولتی سرورهای اخبار رادیو و تلویزیون، سرویس‌های تجاری مانند Ebay و Amazon، سایت‌های اجتماعی مانند twitter، Face book، سرورهای زیر ساخت حیاتی و غیره اشاره کرد. که به احتمال زیاد ممکن است همه اینها به خطر بیفتد[۱].

حملات DDOS را می توان به دو دسته infurstraucture level Attacks and application buy level اشاره کرد [۲،۳]. در حملات Application level Attacks، مهاجم یک منبع محاسباتی غیر قابل دسترس با تغییر پیکربندی سیستم را ارائه می کند و یا با بارکاری نرم افزار را به حد سر ریز می‌رساند و یا یک یا چند بسته دقیق را جهت هدف آسیب‌پذیری آن نرم‌افزار می‌فرستد.

یک مثال کلاسیک از این نوع حملات می توان به حمله ping of dealth اشاره کرد که در آن مهاجم یک بسته ping بزرگ را حداکثر اندازه بسته Ip ورژن ۴ می‌فرستد که در حدود ۶۵۵۳۵ بایت است. از لحاظ تاریخی بسیاری از سیستم عامل‌ها به چنین