به نام خدا

فرم خلاصه مقاله خوانده شده

نام و نام خانوادگی: رضا آدینه پور　　شماره دانشجویی: ۴۰۲۱۳۱۰۵۵

پس از مطالعه مقاله مورد نظر، بخش‌های زیر را پاسخ دهید، در صورتی که فضای پاسخ کافی نمی باشد، پاسخ خود را در انتهای این مستند بطور تکمیل تر ذکر نمایید.

الف) بخش تجزیه و تحلیل مقاله		
۱.	نام رویداد مربوطه، سال برگزاری و محل آن	۵۴th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Brisbane, Australia ۲۰۲۴
۲.	نوع مقاله (short, poster, regular, panel)	Regular
۳.	عنوان مقاله	PagPassGPT: Pattern Guided Password Guessing via Generative Pretrained Transformer
٤.	نام نویسندگان	Xingyu Su, Xiaojie Zhu, Yang Li, Yong Li, Chi Chen, and Paulo Esteves-Verissimo
٥.	دانشگاه نویسندگان	School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China King Abdullah University of Science and Technology, Thuwal, Kingdom of Saudi Arabia
٦.	ایمیل نویسندگان	{suxingyu, liyang۸۱۱۹, liyong, chenchi}@iie.ac.cn {xiaojie.zhu, paulo.verissimo}@kaust.edu.sa
۷.	نویسنده اول مقاله	Xingyu Su
۸.	تعداد صفحات مقاله	۱۴
۹.	سال انتشار مقاله	۲۰۲۴
۱۰.	دلیل اهمیت موضوع کلی عنوان مقاله (چرا تحقیق در زمینه عنوان مقاله مفید بوده است؟ چه توجیهی برای انجام این مقاله بوده است)	۱) افزایش خطرات ناشی از حملات حدس رمز عبور: در دنیای دیجیتال امروز، استفاده گسترده از رمزهای عبور موجب شده که تهدیداتی مانند حملات حدس رمز به یک نگرانی عمومی تبدیل شود. کاربران معمولاً رمزهایی با الگوهای قابل حدس انتخاب می‌کنند، که این امر آنها را در برابر حملات آسیب‌پذیر می‌سازد. تحقیق در این حوزه می‌تواند به شناسایی الگوها و تقویت امنیت کاربران کمک کند. ۲) مشکلات مدل‌های موجود: مدل‌های حدس رمز عبور موجود، حتی آنهایی که از یادگیری عمیق استفاده می‌کنند، با چالش‌هایی مانند تولید رمزهای تکراری و عدم پشتیبانی مناسب از الگوهای ساختاری مواجه هستند. مدل PagPassGPT تلاش می‌کند این کاستی‌ها را برطرف کند و عملکرد بهتری نسبت به مدل‌های پیشین ارائه دهد. ۳) اهمیت حملات گسترده (Trawling Attacks): این نوع حملات به جای هدف قرار دادن افراد خاص، تلاش می‌کند تعداد زیادی از رمزهای عبور کاربران را کشف کند. با توجه به گسترش استفاده از داده‌های درز کرده و اهمیت افزایش نرخ موفقیت این حملات، توسعه مدلی که بتواند رمزهای عبور با کیفیت و غیرتکراری تولید کند، ضرورت دارد. ۴) کاربردهای پژوهشی و عملی: این تحقیق با استفاده از تکنیک‌های پیشرفته، الگوریتم‌هایی ارائه می‌دهد که می‌توانند به‌طور مستقیم برای تحلیل امنیتی رمزهای عبور، توسعه سیستم‌های امنیتی بهتر، و حتی ارزیابی نقاط ضعف کاربران در انتخاب رمزهای عبور استفاده شوند. ۵) نوآوری در مدل‌های یادگیری عمیق: مقاله نشان می‌دهد که مدل

		PagPassGPT با استفاده از الگوریتم‌های جدید مانند D&C-GEN و روش‌های پیشرفته مانند استفاده از اطلاعات الگو، در افزایش نرخ موفقیت و کاهش تکرار رمزهای تولید شده موفق‌تر از مدل‌های قبلی عمل کرده است.
۱۱.	موضوع ذکر شده چه مشکل پژوهشی و تحقیقاتی داشته است که ادامه کار در این زمینه را توجیه کرده است؟	در مقاله، مشکلات پژوهشی و تحقیقاتی که ادامه کار در این زمینه را توجیه کرده‌اند به‌وضوح بیان شده است. این مشکلات به شرح زیر هستند: ۱) کیفیت پایین رمزهای عبور تولید شده توسط مدل‌های موجود: * بسیاری از مدل‌های موجود، به‌ویژه مدل‌های مبتنی بر یادگیری عمیق، در تولید رمزهای عبور که از نظر ساختاری متنوع و واقع‌گرایانه باشند، با مشکل مواجه‌اند. * این مدل‌ها معمولاً نمی‌توانند رمزهایی تولید کنند که الگوهای رایج کاربران را به‌طور مؤثری شبیه‌سازی کنند. ۲) تکرار بالای رمزهای تولید شده: * یکی از مشکلات جدی در مدل‌های موجود، نرخ بالای تولید رمزهای تکراری است. این موضوع باعث کاهش کارایی مدل در حملات گسترده (Trawling Attacks) می‌شود. * به‌عنوان مثال، در مدل‌های پیشین مانند PassGAN و PassGPT، نرخ رمزهای تکراری تولید شده بسیار بالاست (در حدود ۳۴٪ برای PassGPT). ۳) عدم پشتیبانی مناسب از الگوهای رمز عبور: * مدل‌های موجود عموماً توانایی انجام حدس الگوهای ساختاری رمزهای عبور (Pattern Guided Guessing) را ندارند. * حتی مدل‌های پیشرفته مانند PassGPT تنها می‌توانند الگوها را با محدودیت‌های زیادی اجرا کنند و در بسیاری موارد، الگوی تولید شده با پیش‌بینی مدل مطابقت ندارد که این مسئله باعث کاهش نرخ موفقیت می‌شود. ۴) محدودیت در توانایی تعمیم به مجموعه‌های داده جدید: * مدل‌های موجود، به دلیل وابستگی زیاد به داده‌های آموزشی، توانایی تعمیم مناسبی برای مجموعه‌های داده جدید یا شرایط متغیر ندارند. * این محدودیت در حملات میان‌سایتی (Cross-Site Attacks) مشهود است، جایی که مدل‌های قدیمی در حدس زدن رمزهای عبور از منابع مختلف عملکرد ضعیفی دارند. ۵) چالش در تعادل بین دقت و سرعت حدس: * در حملات گسترده، مدل‌های موجود نمی‌توانند تعادل مناسبی میان دقت حدس و سرعت تولید رمزها برقرار کنند. * تولید رمزهای با کیفیت بالا معمولاً مستلزم صرف زمان بیشتری است، که این امر در شرایط عملی کارایی مدل را محدود می‌کند.
۱۲.	دیگران (کارهای گذشته) در این زمینه چه کرده اند؟ در صورت وجود چه محاسن و چه معایبی داشته اند؟	پژوهش‌های پیشین را می‌توان به سه دسته اصلی تقسیم کرد: ۱) مدل‌های مبتنی بر قوانین (Rule-Based Models) محاسن: ۱.۱) سرعت بالا در تولید رمزهای عبور. ۱.۲) استفاده از قوانین ساده و قابل فهم برای استخراج رمزهای جدید از مجموعه‌های موجود (مانند ابزارهای Hashcat و John the Ripper). معایب: ۱.۱) وابستگی زیاد به دانش پیش‌زمینه و قوانین ثابت.

		۱.۲) عدم توانایی در تولید رمزهای متنوع و جدید که در داده‌های آموزشی وجود ندارند. ۲) مدل‌های مبتنی بر احتمالات (Probability-Based Models) محاسن: ۲.۱) توانایی مدل‌سازی الگوهای رایج در رمزهای عبور (مانند مدل‌های Markov و PCFG). ۲.۲) کارایی نسبتاً خوب در حدس الگوهای ساختاری رایج. معایب: ۲.۱) محدودیت در واژگان ثابت و ناتوانی در تولید کلمات خارج از واژگان. ۲.۲) مشکل در تقسیم دقیق رمزهای عبور به بخش‌های مناسب. ۳) مدل‌های مبتنی بر یادگیری عمیق (Deep Learning-Based Models) محاسن: ۳.۱) توانایی یادگیری الگوهای پیچیده و استخراج اطلاعات غنی از داده‌ها. ۳.۲) مدل‌هایی مانند PassGAN، VAEPass و PassGPT موفقیت‌های قابل توجهی در حدس رمزهای عبور با استفاده از شبکه‌های عصبی داشته‌اند. ۳.۳) PassGPT با استفاده از مدل‌های GPT توانایی تولید رمزهای عبور با دقت بالا را نشان داده است. معایب: ۳.۱) نرخ بالای تکرار رمزهای عبور تولید شده، به‌ویژه در مدل‌هایی مانند PassGAN (تا ۶۶٪) و PassGPT (تا ۳۴٪). ۳.۲) عدم پشتیبانی مؤثر از حدس الگوهای ساختاری رمز عبور (Pattern Guided Guessing). ۳.۳) محدودیت در تعمیم به داده‌های جدید یا شرایط نامتعارف (ضعف در حملات میان‌سایتی). ۳.۴) افزایش پیچیدگی محاسباتی و نیاز به منابع سخت‌افزاری بیشتر.
۱۳.	تفاوت این مقاله با روشهایی که در گذشته ارایه شده است در چیست؟ (بدون این تفاوت مقاله فاقد ارزش است.)	۱) پشتیبانی پیشرفته از الگوهای ساختاری (Pattern Guided Guessing): برخلاف مدل‌های گذشته، PagPassGPT الگوهای رمز عبور را به عنوان دانش پیش‌زمینه در فرآیند حدس رمز استفاده می‌کند و تطابق بهتری بین الگو و پیش‌بینی مدل دارد. ۲) کاهش نرخ تکرار رمزهای تولیدی: استفاده از الگوریتم D&C-GEN برای تقسیم وظایف و جلوگیری از تولید رمزهای تکراری، که نرخ تکرار را تا ۹.۲۸٪ کاهش داده است (در مقابل ۳۴٪ برای PassGPT). ۳) تولید رمزهای با کیفیت بالاتر: رمزهای تولید شده توسط PagPassGPT از نظر طول و الگوی ساختاری نزدیک‌تر به داده‌های واقعی هستند. ۴) بهبود تعمیم‌پذیری: عملکرد بهتر در حملات میان‌سایتی (Cross-Site Attacks) نسبت به مدل‌های قبلی.
۱٤.	توضیح کلی مقاله و روش ارایه شده برای حل مشکل یاد شده	این مقاله به بررسی چالش‌های موجود در حدس رمزهای عبور می‌پردازد، از جمله کیفیت پایین رمزهای تولید شده، نرخ بالای تکرار رمزها و عدم پشتیبانی مناسب از الگوهای ساختاری رمز عبور. برای حل این مشکلات، مدل جدیدی به نام PagPassGPT و الگوریتم D&C-GEN ارائه شده است. روش ارائه شده: ۱) مدل PagPassGPT: * ساختار: این مدل مبتنی بر معماری -۲GPT است و از مکانیزم خودبازگشتی (Auto-Regressive) برای تولید رمز عبور استفاده می‌کند.

		* ویژگی کلیدی: الگوهای ساختاری رمز عبور (مانند ترکیب حروف، اعداد و کاراکترهای خاص) به عنوان ورودی اولیه در فرآیند تولید رمز استفاده می‌شوند. این ویژگی به مدل اجازه می‌دهد رمزهایی تولید کند که به الگوهای واقعی نزدیک‌تر باشند. * نتیجه: نرخ موفقیت (Hit Rate) تا ۱۲٪ بالاتر از مدل PassGPT است. ۲) الگوریتم D&C-GEN: * هدف: کاهش نرخ تکرار رمزهای تولید شده. * روش: این الگوریتم از رویکرد "تقسیم و غلبه" (Divide-and-Conquer) استفاده می‌کند. وظیفه اصلی حدس رمز به زیروظایف کوچک‌تر با الگوها و پیشوندهای غیر همپوشان تقسیم می‌شود. * نتیجه: نرخ تکرار رمزها به کمتر از ۱۰٪ کاهش یافته (در مقایسه با ۳۴٪ برای PassGPT).
۱۵.	نتایج نهایی مقاله	۱) بهبود نرخ موفقیت (Hit Rate): مدل PagPassGPT نرخ موفقیت در حدس رمز عبور را در حملات گسترده (Trawling Attacks) تا ۱۲٪ بیشتر از مدل PassGPT افزایش داده است (۵۳.۶۳٪ در مقابل ۴۱.۹۳٪ برای 10^9 حدس). ۲) کاهش نرخ تکرار رمزها (Repeat Rate): با استفاده از الگوریتم D&C-GEN، نرخ تکرار رمزها به ۹.۲۸٪ کاهش یافته است، در حالی که این مقدار برای PassGPT برابر با ۳۴٪ بوده است. ۳) بهبود در حدس الگوهای ساختاری (Pattern Guided Guessing): مدل PagPassGPT در تولید رمزهای مبتنی بر الگوهای پیچیده عملکرد بهتری داشته و نرخ موفقیت برای الگوهای چندبخشی (بیش از ۵ بخش) به طور چشمگیری افزایش یافته است. ۴) تعادل در کیفیت و تنوع رمزها: رمزهای تولیدی از نظر طول و توزیع الگو به داده‌های واقعی نزدیک‌تر بوده و تنوع بیشتری نسبت به مدل‌های قبلی دارند. ۵) عملکرد بهتر در حملات میان‌سایتی (Cross-Site Attacks): PagPassGPT با ۱۱٪ تا ۱۶٪ نرخ موفقیت بالاتر نسبت به PassGPT در حملات میان‌سایتی (Cross-Site Attacks) عملکرد بهتری نشان داده است.
۱۶.	حسن عمده این روش با توجه به نتایج بدست آمده چیست؟	حسن عمده روش PagPassGPT با توجه به نتایج، ترکیب بهینه دقت، کیفیت، و تنوع در تولید رمزهای عبور است. این روش: ۱) افزایش موفقیت در حدس رمز (Hit Rate): عملکرد بهتر در حدس رمزهای واقعی، با بهبود ۱۲٪ نرخ موفقیت در حملات گسترده و میان‌سایتی. ۲) کاهش نرخ تکرار رمزها: تولید رمزهایی با تنوع بیشتر و کاهش تکرار به ۹.۲۸٪ (در مقایسه با ۳۴٪ در روش‌های پیشین)، که تنوع و کارایی حملات را افزایش می‌دهد. ۳) پشتیبانی پیشرفته از الگوهای ساختاری رمز: توانایی تولید رمزهایی که به الگوهای واقعی نزدیک‌تر هستند، حتی در الگوهای پیچیده و چندبخشی. ۴) تعادل میان دقت و کارایی: رویکرد "تقسیم و غلبه" در الگوریتم D&C-GEN ضمن حفظ سرعت حدس، از هدر رفتن منابع جلوگیری کرده است. ۵) تعمیم‌پذیری بالا: موفقیت در حملات میان‌سایتی نشان‌دهنده قابلیت تعمیم این روش به مجموعه داده‌های مختلف است.
۱۷.	ضعف این روش با توجه به نتایج بدست آمده چیست؟	۱) زمان و منابع محاسباتی بالا:

		* استفاده از مدل‌های مبتنی بر -۲GPT و الگوریتم D&C-GEN ممکن است نیاز به منابع محاسباتی زیادی داشته باشد (مثلاً نیاز به GPUهای قدرتمند و زمان پردازش طولانی برای آموزش و تولید رمزها). * این امر ممکن است محدودیت‌هایی برای استفاده عملی از مدل در مقیاس‌های بزرگ ایجاد کند. ۲) محدودیت در تولید رمزهای طولانی‌تر: * PagPassGPT به‌طور خاص برای تولید رمزهای عبور با طول حداکثر ۱۲ کاراکتر طراحی شده است و ممکن است برای تولید رمزهای طولانی‌تر یا پیچیده‌تر عملکرد بهینه نداشته باشد. * برای رمزهای با طول بیشتر، باید مدل دوباره آموزش داده شود که می‌تواند زمان‌بر باشد. ۳) محدودیت در نوع و پیچیدگی الگوها: هرچند مدل قادر به تولید رمزهایی با الگوهای متداول است، اما ممکن است برای برخی الگوهای پیچیده و نادرتر که در داده‌های آموزشی موجود نباشند، دقت کمتری داشته باشد. ۴) وابستگی به داده‌های آموزشی: مدل‌های یادگیری عمیق مانند PagPassGPT نیاز به داده‌های آموزشی بزرگ و متنوع دارند تا بتوانند به خوبی عمل کنند. در غیر این صورت، ممکن است در تعمیم به داده‌های جدید و ناشناخته ضعف نشان دهند.
۱۸.	برای کارهای آتی در این زمینه چه راههایی پیشنهاد شده است؟	۱) افزایش تنوع و پشتیبانی از الگوهای پیچیده‌تر: * طراحی مدل‌هایی که قادر به تولید رمزهای عبور با الگوهای نادر و پیچیده‌تر باشند، مانند رمزهای چندبخشی با ترکیب‌های غیرمعمول. * توسعه روشی برای شناسایی و یادگیری الگوهای جدید و ناشناخته از داده‌های درز کرده. ۲) گسترش طول رمزهای عبور: * بهبود مدل برای پشتیبانی از رمزهای عبور با طول بیشتر از ۱۲ کاراکتر. * استفاده از تکنیک‌های بهینه‌سازی حافظه و پردازش برای کاهش هزینه محاسباتی تولید رمزهای طولانی‌تر. ۳) کاهش وابستگی به داده‌های آموزشی: * طراحی مدل‌هایی که نیاز کمتری به داده‌های بزرگ و متنوع داشته باشند و بتوانند با داده‌های محدود نیز تعمیم‌پذیری خوبی ارائه دهند. * استفاده از روش‌های یادگیری انتقالی (Transfer Learning) برای تعمیم بهتر به دامنه‌های جدید. ۴) بهبود سرعت و کارایی محاسباتی: * بهینه‌سازی الگوریتم D&C-GEN برای کاهش زمان پردازش و بهره‌برداری بهتر از منابع محاسباتی. * استفاده از تکنیک‌های موازی‌سازی بهتر برای افزایش کارایی در محیط‌های محاسباتی با مقیاس بالا. ۵) توسعه الگوریتم‌های پیشرفته‌تر برای کاهش نرخ تکرار: * ارائه روش‌های جدید برای کاهش بیشتر نرخ تکرار رمزها بدون کاهش کیفیت و تنوع آنها. * ترکیب الگوریتم D&C-GEN با روش‌های دیگر مانند یادگیری تقویتی برای بهبود خروجی. ۶) مطالعه رفتار کاربران در انتخاب رمز عبور: * انجام تحقیقات بیشتر روی نحوه انتخاب رمز عبور توسط کاربران در فرهنگ‌ها و مناطق مختلف و ادغام این دانش در مدل.

		* شناسایی الگوهای روانشناختی و معنایی که می‌توانند به تولید رمزهای واقعی‌تر کمک کنند. ۷) افزایش امنیت و کاربردهای دفاعی: * استفاده از این مدل‌ها برای توسعه ابزارهای امنیتی که بتوانند به کاربران در انتخاب رمزهای قوی‌تر کمک کنند. * شبیه‌سازی حملات برای ارزیابی مقاومت سیستم‌های امنیتی در برابر تهدیدات جدید.
۱۹.	چه کارهایی به ذهن شما می‌رسد که می‌توان ادامه داد؟	برای ادامه تحقیقات در این زمینه، چندین ایده و جهت‌گیری وجود دارد که می‌توانند به گسترش و بهبود مدل‌های حدس رمز عبور کمک کنند: ۱) استفاده از مدل‌های چندمنظوره برای تحلیل رمزهای عبور: می‌توان مدل‌های جدیدی را طراحی کرد که نه‌تنها رمزهای عبور را تولید کنند، بلکه تحلیل رفتار کاربر را نیز انجام دهند. به عبارت دیگر، مدل‌هایی که ترکیبی از یادگیری عمیق و تحلیل‌های روان‌شناختی برای پیش‌بینی رمزهای عبور بر اساس ویژگی‌های فردی کاربر (مانند رفتار، تاریخچه انتخاب رمز، یا داده‌های شخصی) باشند. ۲) افزایش دقت مدل‌های یادگیری عمیق با داده‌های متنوع: * تحقیق در زمینه گسترش مجموعه داده‌های آموزشی با داده‌های رمز عبور از منابع مختلف و شبیه‌سازی حملات می‌تواند به مدل کمک کند تا بهتر قادر به تعمیم‌پذیری به مجموعه‌های داده مختلف باشد. * همچنین، استفاده از داده‌های رمز عبور مربوط به مناطق جغرافیایی مختلف یا زبان‌های مختلف می‌تواند به بهبود دقت مدل در پیش‌بینی رمزهای عبور متنوع کمک کند. ۳) پیاده‌سازی مدل‌های امنیتی برای جلوگیری از حملات سایبری: * توسعه مدل‌های حدس رمز عبور می‌تواند به ابزاری برای ارزیابی مقاومت سیستم‌ها در برابر حملات brute-force تبدیل شود. به عبارت دیگر، استفاده از مدل‌ها برای آزمون امنیتی سیستم‌های رمزنگاری و پیش‌بینی آسیب‌پذیری می‌تواند به تیم‌های امنیتی کمک کند. * همچنین، می‌توان از این مدل‌ها برای گسترش سیستم‌های احراز هویت دو مرحله‌ای (FA۲) استفاده کرد. ۴) گسترش در زمینه تولید رمزهای عبور با ویژگی‌های خاص: یکی دیگر از کارهایی که می‌توان ادامه داد، تولید رمزهای عبور با ویژگی‌های خاص مانند رمزهای عبور بیومتریک یا مبتنی بر یادگیری ماشین است. مدل‌هایی که قادر به تولید رمزهایی با معیارهای خاص امنیتی (مثلاً مقاومت در برابر حملات خاص) یا حتی تولید پاسفرازها (password phrases) با ترکیب‌های معنایی جدید می‌باشند. ۵) ۵. کاربرد در زمینه‌های واقعی (Real-World Applications): * گسترش استفاده از این مدل‌ها در سیستم‌های واقعی مانند مدیریت پسوردها و امنیت موبایل می‌تواند به کاهش خطرات امنیتی در محیط‌های عملی کمک کند. * همچنین، مدل‌ها می‌توانند برای پیش‌بینی رمزهای عبور در حملات اجتماعی (social engineering attacks) یا استفاده در سیستم‌های امنیتی داخلی سازمان‌ها مورد استفاده قرار گیرند. ۶) تحلیل و شبیه‌سازی حملات اجتماعی (Social Engineering Attacks): بررسی رفتار کاربران در انتخاب رمز عبور و شبیه‌سازی نحوه نفوذ مهاجمین به کمک حملات اجتماعی و پیش‌بینی کلمات و عبارات احتمالی که کاربران بر

		اساس ویژگی‌های اجتماعی خود انتخاب می‌کنند، می‌تواند به طراحی مدل‌های مقاوم در برابر چنین تهدیداتی کمک کند. ۷) پژوهش در زمینه دفاع فعال در برابر حملات حدس رمز عبور: طراحی سیستم‌های دفاعی هوشمند که به صورت فعال از روش‌های یادگیری ماشین برای شناسایی و مقابله با حملات حدس رمز عبور (Trawling Attacks) استفاده کنند. این سیستم‌ها می‌توانند بر اساس رفتار حمله، روش‌های مقابله‌ای مناسب را اتخاذ کنند.
۲۰.	شما به نوبه خود چه انتقادی به این مقاله دارید؟ (نوشتاری، نگارشی، ساختاری، ترسیم شکل، علمی، بهبودی و مانند آن)	با توجه به محتوای مقاله و بررسی آن، چند نکته و انتقاد به جنبه‌های مختلف مقاله قابل ذکر است که می‌تواند برای بهبود آن مفید باشد: ۱) ساختار و شفافیت مقاله: * پیچیدگی در ارائه مفاهیم: در برخی بخش‌ها، توضیحات به‌ویژه در بخش‌های فنی و ریاضیاتی (مانند فرمول‌ها و نحوه کارکرد مدل‌ها) ممکن است برای خوانندگان غیرمتخصص کمی پیچیده باشد. توضیحات بیشتری در مورد مفاهیم اصلی مدل (مثل D&C-GEN و نحوه تقسیم و غلبه) می‌تواند کمک‌کننده باشد. * لایه‌بندی بهتر بخش‌ها: برخی از بخش‌ها ممکن است بیش از حد فنی و بدون زمینه‌سازی مناسب برای خواننده غیرمتخصص نوشته شده باشد. اضافه کردن بخش‌هایی برای توضیح بیشتر قبل از وارد شدن به جزئیات پیچیده می‌تواند مقاله را برای یک دامنه وسیع‌تری از خوانندگان قابل فهم‌تر کند. ۲) ترسیم اشکال و نمودارها: * کیفیت تصاویر و نمودارها: برخی از نمودارها و اشکال، به‌ویژه در بخش‌های تجربی، ممکن است برای نمایش داده‌ها و مقایسه مدل‌ها مفید باشند، اما می‌توانند کیفیت و وضوح بالاتری داشته باشند تا خواننده راحت‌تر بتواند اطلاعات را تجزیه و تحلیل کند. * عنوان و توضیحات شکل‌ها: در برخی موارد، توضیحات همراه با شکل‌ها و نمودارها ممکن است کوتاه و کلی باشد. افزودن توضیحات دقیق‌تر و کاربردی‌تر برای هر شکل می‌تواند کمک کند تا خواننده بهتر متوجه ارتباط داده‌ها با نتایج مقاله شود. ۳) نگارش و وضوح زبان: * زبان پیچیده: در برخی قسمت‌های مقاله، زبان ممکن است کمی پیچیده باشد و درک مفاهیم را برای برخی خوانندگان دشوار کند. استفاده از زبان ساده‌تر و واضح‌تر در قسمت‌های توضیحی می‌تواند کمک‌کننده باشد. * استفاده بیشتر از مثال‌های عملی: در بخش‌های توضیحی، استفاده از مثال‌های عملی و کاربردی‌تر می‌تواند کمک کند تا مفاهیم بهتر در ذهن خواننده جا بیفتد. این امر به‌ویژه در بخش‌های مربوط به الگوریتم‌ها و مدل‌ها مفید است. ۴) نقد علمی و پیشنهادات بهبود: * آزمون مدل بر روی مجموعه داده‌های بیشتر: با وجود اینکه مقاله آزمایش‌ها و مقایسه‌های خوبی با مدل‌های قبلی انجام داده، گسترش آزمایش‌ها به مجموعه داده‌های متنوع‌تر و یا داده‌های ناشناخته (cross-domain) می‌تواند اعتبار و قابلیت تعمیم مدل را بهتر نشان دهد. * مقایسه بیشتر با مدل‌های جدیدتر: در مقاله به مقایسه با مدل‌های پیشین پرداخته شده است، اما شاید بررسی و مقایسه بیشتر با مدل‌های جدیدتر مانند

		PassBERT یا مدل‌های مبتنی بر Transformerهای جدیدتر می‌توانست نتایج بهتری را در مورد قدرت و کارایی مدل در مقابل جدیدترین پیشرفت‌ها ارائه دهد. * بررسی چالش‌های عملی: اگرچه مقاله به طور مفصل به مدل پرداخته است، ولی چالش‌های عملی در استفاده از مدل (مثلاً مسائل مربوط به پردازش موازی، هزینه‌های محاسباتی، و محدودیت‌ها در دنیای واقعی) می‌تواند بیشتر بررسی شود. ۵) نگارش بهبود یافته برای مخاطب عمومی‌تر: * گرفتن نتیجه‌گیری بیشتر از داده‌ها: برخی از نتایج به‌ویژه در بخش‌های تجربی نیاز به جمع‌بندی و نتیجه‌گیری بیشتر دارند. به‌طور مثال، با ارائه شواهد بیشتر در قالب جدول‌ها یا مقایسه‌های دقیق‌تر می‌توان بهتر نشان داد که چرا این مدل جدید برتری‌های قابل توجهی در مقایسه با مدل‌های قبلی دارد.
ب) بخش‌های اطلاعاتی و مفید قابل استخراج از مقاله		
۱.	چکیده فهم شما از مقاله در یک پاراگراف چیست؟	این مقاله مدل جدیدی به نام PagPassGPT ارائه می‌دهد که بر پایه معماری GPT-۲ طراحی شده و هدف آن بهبود فرآیند حدس رمزهای عبور است. این مدل با استفاده از الگوهای ساختاری رمزهای عبور (Pattern Guided Guessing) و ترکیب آنها با پیش‌بینی مدل، توانسته است رمزهایی با دقت و کیفیت بالاتر تولید کند. علاوه بر این، الگوریتم D&C-GEN برای کاهش نرخ تکرار رمزهای تولیدی به کار گرفته شده که از رویکرد "تقسیم و غلبه" برای تقسیم وظایف حدس رمز استفاده می‌کند. نتایج نشان می‌دهد که این مدل در حملات گسترده و میان‌سایتی عملکرد بهتری نسبت به مدل‌های پیشین داشته و نرخ موفقیت و تنوع رمزهای تولیدی را به میزان قابل توجهی افزایش داده است، در حالی که نرخ تکرار رمزها کاهش یافته است. این رویکرد نوآورانه، چالش‌های مدل‌های پیشین مانند نرخ تکرار بالا، ضعف در تعمیم‌پذیری، و عدم پشتیبانی از الگوهای پیچیده را به طور موثری حل کرده است.
۲.	نوع ارزیابی چگونه بوده است؟ تجری/تحلیلی/هردو	هر دو
۳.	بستر آزمایشات چیست؟ و محیط بدست آوری نتایج چگونه بوده است؟	۱) بستر سخت‌افزاری: * آزمایش‌ها روی سیستمی با چهار کارت گرافیک GeForce RTX ۳۰۸۰ انجام شده است. * سیستم عامل استفاده شده لینوکس بوده که برای اجرای مدل‌ها و الگوریتم‌های پردازشی سنگین مناسب است. ۲) بستر نرم‌افزاری: * مدل PagPassGPT با استفاده از کتابخانه GPT-۲ توسعه داده شده است. * برای بهینه‌سازی مدل، از AdamW Optimizer با نرخ یادگیری اولیه ۵×۱۰^{-۵} استفاده شده است. ۳) پارامترهای تنظیم شده برای مدل: * تعداد Epochها: ۳۰ * Batch Size: ۵۱۲ * تعداد توکن‌های ورودی: حداکثر ۳۲ توکن. * Embedding Size: ۲۵۶ * تعداد لایه‌های مخفی: ۱۲ لایه. * Attention Heads: ۸

		۴) مجموعه داده‌های مورد استفاده: * از پنج مجموعه داده رمزهای عبور واقعی شامل RockYou، LinkedIn، phpBB، MySpace و Yahoo استفاده شده است. ۵) روش انجام آزمایشات: * مدل‌ها بر اساس داده‌های آموزشی آموزش داده شده‌اند و روی داده‌های آزمایشی مستقل ارزیابی شده‌اند. * آزمایش‌ها شامل مقایسه نرخ موفقیت، نرخ تکرار رمزها، و توزیع طول و الگوهای رمزهای تولیدی بوده است. * از حملات میان‌سایتی (Cross-Site Attacks) نیز برای ارزیابی تعمیم‌پذیری مدل استفاده شده است. آموزش مدل PagPassGPT در این محیط بیش از ۲۵ ساعت طول کشیده است.
٤.	نام ابزارها، شبیه‌سازها، تجهیزات بکار رفته به همراه مرجع	۱) تجهیزات سخت‌افزاری: * چهار کارت گرافیک GeForce RTX ۳۰۸۰ برای تسریع پردازش‌های یادگیری عمیق و اجرای مدل PagPassGPT. * سیستم عامل لینوکس برای مدیریت محیط آزمایش و استفاده از ابزارهای پیشرفته یادگیری عمیق. ۲) ابزارهای نرم‌افزاری: * کتابخانه GPT-۲: مرجع [OpenAI[Radford et al., ۲۰۱۹ * AdamW Optimizer: مرجع Kingma & Ba, ۲۰۱٤ ۳) مجموعه داده‌های مورد استفاده: * RockYou: مرجع: [RockYou Leak Dataset]. * LinkedIn: مرجع: [LinkedIn Data Breach]. * phpBB: مرجع: [phpBB Password Dataset]. * MySpace: مرجع: [MySpace Password Dataset]. * Yahoo!: مرجع: [Yahoo! Password Dataset].
٥.	بارهای کاری استفاده شده در این مقاله چیست؟	در این مقاله، بارهای کاری شامل آموزش مدل PagPassGPT با استفاده از مجموعه داده‌های رمزهای عبور واقعی (مانند RockYou و LinkedIn) بوده که پس از پردازش، به بخش‌های آموزشی، اعتبارسنجی و آزمایشی تقسیم شده‌اند. مدل با تولید تا 10^9 رمز عبور برای ارزیابی در حملات گسترده و میان‌سایتی آزمایش شده است. نرخ موفقیت (Hit Rate) و نرخ تکرار (Repeat Rate) رمزهای تولیدی محاسبه شده و با مدل‌های قبلی مانند PassGAN، PassFlow، VAEPass و PassGPT مقایسه شده است. علاوه بر این، آزمایش‌هایی برای بررسی توانایی مدل در تولید رمزهای عبور بر اساس الگوهای ساختاری (Pattern Guided Guessing) و تحلیل توزیع این الگوها انجام شده است. نتایج نشان‌دهنده بهبود در دقت، تنوع و تعمیم‌پذیری مدل بوده است.
٦.	نگارش مراجع استاندارد و یکنواخت است؟	بلی
۷.	تعداد مراجع؟	۶۸	درصد (٪۱۰۰)
۸.	تعداد مراجع ژورنالی؟ (Journal/Transactions)	۴۵	٪ ۶۶
۹.	تعداد مراجع کنفرانسی؟ (Conference/Symposium)	۲۸	٪ ۴۱
۱۰.	تعداد مراجع کارگاهی؟ (Workshop)	۴	٪ ۵
۱۱.	تعداد مراجع کتاب؟	۰	٪ ۰
۱۲.	تعداد مراجع گزارش علمی؟ (Technical Report)	۰	٪ ۰
۱۳.	تعداد مراجع تزهای فوق لیسانس یا دکتری؟	۰	٪ ۰
۱٤.	تعداد مراجع که HTML هستند؟	۱۶	٪ ۲۳

۱۵.	تعدا مراجع حداکثر تا ۵ سال قبل از سال انتشار مقاله؟	۲۲	٪ ۳۲
۱۶.	تعداد مراجع حداکثر تا ۱۰ سال قبل از سال انتشار مقاله؟	۳۸	٪ ۵۵
۱۷.	دلیل انتخاب این مقاله توسط شما چه بوده است؟	علاقه مندی به حوزه شبکه های عصبی و نزدیک بودن موضوع مقاله (صرفا مدل ترنسفرمر) به موضوع پایان نامه بنده	