

بسمه تعالی



طرح پیشنهادی جهت دریافت پایان نامه کارشناسی ارشد

دانشکده علوم ریاضی، گروه علوم کامپیوتر

عنوان:

حفظ حریم خصوصی مبتنی بر رمزگذاری همومورفیک چند کلیدی در یادگیری فدرالی

Privacy-preserving based on Multi-key Homomorphic Encryption in Federated Learning

مشخصات دانشجو:

نام و نام خانوادگی: نام فامیل

شماره دانشجویی: ۴۰۳۱۹۰۳۰۰۰

رشته تحصیلی: علوم کامپیوتر، گرایش محاسبات علمی

مشخصات استاد راهنما:

نام و نام خانوادگی	تخصص	مرتبه دانشگاهی	محل کار
دکتر نام فامیل	علوم کامپیوتر	استادیار	دانشکده علوم ریاضی، دانشگاه شهرکرد

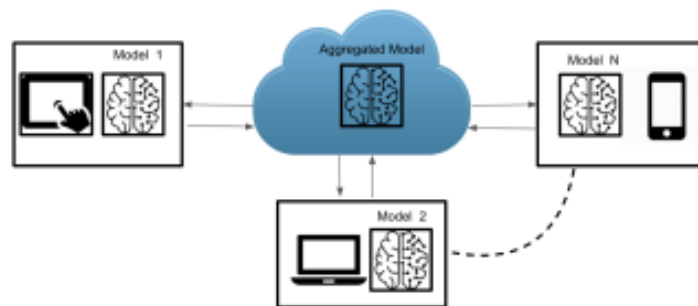
مشخصات استاد مشاور:

نام و نام خانوادگی	تخصص	مرتبه دانشگاهی	محل کار
دکتر نام فامیل	علوم کامپیوتر	استادیار	دانشکده علوم ریاضی، دانشگاه شهرکرد

۱ مقدمه و بیان مساله

یادگیری ماشین (ML)^۱ یکی از زیر مجموعه‌های هوش مصنوعی است که به سیستم‌ها این امکان را می‌دهد که به صورت خودکار، یادگیری و پیشرفت داشته باشند؛ بدون اینکه برنامه‌نویسی صریحی برای آن داشته باشند. الگوریتم‌های یادگیری ماشینی، یک مدل ریاضی را بر اساس داده‌های نمونه یا داده‌های آموزش، به منظور پیش‌بینی یا تصمیم‌گیری بدون برنامه‌ریزی آشکار، ایجاد می‌کنند. با محبوبیت بسیاری از دستگاه‌ها و گسترش اینترنت اشیا (IOT)^۲، میزان داده‌های توزیع شده به طور چشم‌گیری افزایش یافته است که توسعه شدید یادگیری ماشینی را در بسیاری از حوزه‌ها، مانند، مراقبت‌های بهداشتی هوشمند، خانه‌های هوشمند، یا تشخیص تصادفات ترافیکی ارتقا می‌دهد [۱، ۲، ۳].

در حالی که مزیت یادگیری ماشین غیر قابل انکار است، جمع‌آوری حجم زیادی از داده‌ها در سرورهای مرکزی به منظور تجزیه و تحلیل، به علت نقض حریم خصوصی^۳ شرکت کنندگان، غیر ممکن است.



شکل ۱.۱: یادگیری فدرالی

۲ اهداف اصلی

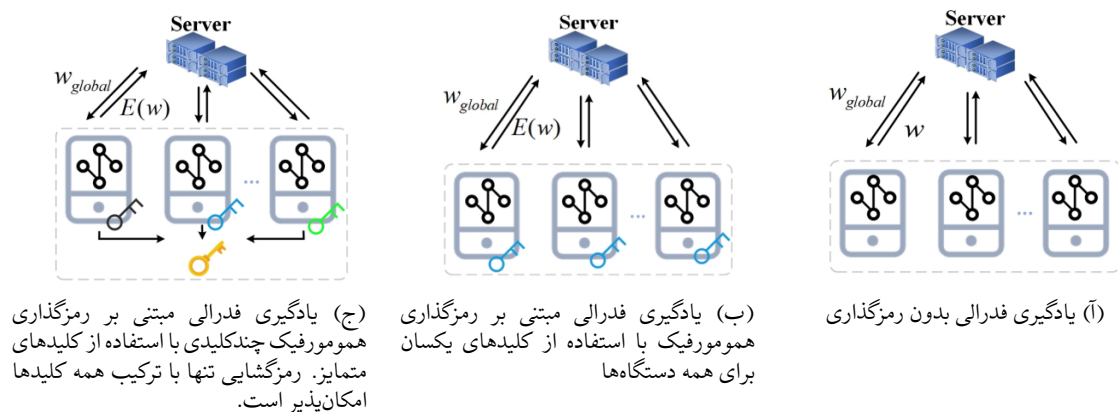
هدف از پیشنهادیه این پایان‌نامه این است که XMK-CKKS را به عنوان یک نسخه بهبود یافته از پروتکل رمزگذاری همومورفیک چندکلیدی MK-CKKS [۴] برای افزایش حریم خصوصی بررسی کنیم. با توجه به اینکه از طریق مدل‌های آموزش دیده، امکان فاش شدن اطلاعات حساس برای مهاجم‌های خارجی و شرکت کنندگان کنجکاو داخلی وجود دارد، این نیاز وجود دارد که این مدل‌های محلی از طریق یک کلید عمومی رمزگذاری شوند و این کلید باید به گونه‌ای باشد که برای رمزگشایی، همکاری بین همه‌ی دستگاه‌های شرکت کننده لازم باشد. این طرح از نشت حریم خصوصی به روزرسانی‌های مدل‌های محلی جلوگیری می‌کند و در برابر تبانی $K < N - 1$ دستگاه شرکت کننده و سرور مقاوم است. ارزیابی‌ها نشان می‌دهد که این طرح با حفظ دقت مدل، در ارتباطات و هزینه‌های محاسباتی نیز بهتر عمل می‌کند.

1. machine learning
2. internet of things
3. privacy

۳ پیشینه پژوهش

بسیاری از طرح‌های یادگیری فدرالی ایمن مبتنی بر فناوری‌های رمزنگاری در سال‌های گذشته پیشنهاد شده است، اما این راه‌حل‌ها مستقیماً برای سناریوهای توزیع شده، قابل اجرا نیستند و یا از دست دادن عملکرد اجتناب‌ناپذیری دارند. یادگیری فدرالی مبتنی بر محاسبات چندجانبه (MPC)^۱ به افراد اجازه می‌دهد تا با استفاده از داده‌های ترکیبی خود، محاسباتی را انجام دهند، بدون اینکه ورودی فردی و خصوصی خود را آشکار کنند؛ اما با این حال، امکان نقض حریم خصوصی^۲ توسط مهاجم درونی و بیرونی وجود دارد. برای رفع این مشکل، یادگیری فدرالی مبتنی بر محاسبات چندجانبه ایمن (SMPC)^۳ را مطرح کردند. این پروتکل نیازمند دوره‌های زیادی از تعامل بین شرکت‌کنندگان برای دستیابی به تجمیع ایمن است، که برای سناریوهای توزیع شده، بسیار عملی نیست [۵، ۶، ۷، ۸].

در شکل ۱۰.۳ نشان داده شده است که



شکل ۱۰.۳: مقایسه انواع پروتکل‌های یادگیری فدرالی

قضیه ۱۰.۳. این قضیه بیان می‌کند

حل. برهان این قضیه

■

1. multi-party computation
2. privacy violation
3. secure multi-party computation

- [1] S. Kianoush, M. Raja, S. Savazzi, S. Sigg, A cloud-iot platform for passive radio sensing: Challenges and application case studies, *IEEE Internet of Things Journal* 5 (5) (2018) 3624–3636.
- [2] J. Li, J. Jin, D. Yuan, M. Palaniswami, K. Moessner, Ehopes: Data-centered fog platform for smart living, in: *2015 International Telecommunication Networks and Applications Conference (ITNAC)*, IEEE, 2015, pp. 308–313.
- [3] J. Li, J. Jin, D. Yuan, H. Zhang, Virtual fog: A virtualization enabled fog computing framework for internet of things, *IEEE Internet of Things Journal* 5 (1) (2017) 121–131.
- [4] H. Chen, W. Dai, M. Kim, Y. Song, Efficient multi-key homomorphic encryption with packed ciphertexts with application to oblivious neural network inference, in: *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, 2019, pp. 395–412.
- [5] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, K. Seth, Practical secure aggregation for federated learning on user-held data, *arXiv preprint arXiv:1611.04482* (2016).
- [6] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, K. Seth, Practical secure aggregation for privacy-preserving machine learning, in: *proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 1175–1191.
- [7] Y. Li, Y. Zhou, A. Jolfaei, D. Yu, G. Xu, X. Zheng, Privacy-preserving federated learning framework based on chained secure multiparty computing, *IEEE Internet of Things Journal* 8 (8) (2020) 6178–6186.
- [8] G. Xu, H. Li, S. Liu, K. Yang, X. Lin, Verifynet: Secure and verifiable federated learning, *IEEE Transactions on Information Forensics and Security* 15 (2019) 911–926.

تاییده دانشجو، اساتید راهنما و مشاور

هزینه انجام پایان نامه های کارشناسی ارشد در هر سال توسط شورای تحصیلات تکمیلی دانشگاه تعیین و توسط دانشکده ها قابل پرداخت خواهد بود. در صورتی که بخشی از هزینه انجام پایان نامه از محل های دیگر تامین شود، ذکر نام سازمان، مبلغ و مشخصه ای از قرارداد همراه با موافقت سازمان مربوطه الزامی است.

زمان پیشنهادی برای تاریخ دفاع: شهریور ۱۴۰۵
در ضمن، تمدید این زمان منوط به موافقت شورای تحصیلات تکمیلی دانشکده بر حسب مقررات دانشگاه است.

نام و نام خانوادگی دانشجو: نام فامیل

امضاء

نام و نام خانوادگی استاد راهنما: دکتر نام فامیل

امضاء

نام و نام خانوادگی استاد مشاور: دکتر نام فامیل

امضاء

موضوع طرح پیشنهادی پایان نامه در جلسه شورای گروه در تاریخ مورد بررسی قرار گرفت و به تصویب رسید.

نام و نام خانوادگی مدیر گروه:

امضاء

موضوع این پایان نامه در جلسه شورای پژوهشی و تحصیلات تکمیلی دانشکده علوم ریاضی مورخ مورد بررسی قرار گرفت و به تصویب رسید.

معاون پژوهشی و تحصیلات تکمیلی دانشکده علوم ریاضی

امضاء

موضوع طرح پیشنهادی پایان نامه در شورای تحصیلات تکمیلی دانشگاه در تاریخ مورد بررسی قرار گرفت و به تصویب رسید.

مدیر تحصیلات تکمیلی دانشگاه

امضاء