

عنوان مقاله:

تحلیلی بر انواع معماری های رهگیری و ثبت رفتار نرم افزارها و ارائه یک معماری جدید

محل انتشار:

اولین همایش منطقه ای شبکه های کامپیوتری (سال: 1392)

تعداد صفحات اصل مقاله: 9

نویسندگان:

جواد مرادی دهنوی - دانشجوی ارشد ، گروه مهندسی کامپیوتر و فناوری اطلاعات دانشگاه پیام نور (شهر ری)

علی رضوی ابراهیمی - استادیار گروه مهندسی کامپیوتر و فناوری اطلاعات ، دانشگاه پیام نور (تهران)

حمیدرضا ناجی - استادیار، گروه مهندسی برق و کامپیوتر، دانشگاه تحصیلات تکمیلی صنعتی و فناوری پیشرفته کرمان (کرمان)

خلاصه مقاله:

روش های رهگیری رفتار نرم افزار به دو دسته رهگیری بصورت ایستا و رهگیری بصورت پویا، تقسیم بندی می شوند. در روش رهگیری ایستا بدون اجرای کد برنامه و تنها با بررسی ساختار کد نرم افزار، رفتار آن شناسایی می گردد. اما در روش رهگیری پویا با اجرای واقعی بدافزار، رفتار آن بصورت پویا ثبت می گردد. رهگیری پویا به دو روش رهگیری در سطح هسته و رهگیری در سطح کاربر انجام می گیرد. روش رهگیری سطح هسته بسیار سریع تر است. اما در روش رهگیری سطح کاربر تعداد بیشتری فراخوانی سیستمی می توان رهگیری کرد. در این مقاله قصد داریم به بررسی انواع روش های رهگیری رفتار نرم افزار و مزایا و معایب هریک بپردازیم. در نهایت یک معماری جدید جهت رهگیری و ثبت رفتار نرم افزار ارائه خواهد شد و این معماری مورد ارزیابی قرار خواهند گرفت.

کلمات کلیدی:

معماری، رهگیری، بدافزار، رفتار، پویا

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/250263>

