سیویلیکا - ناشر تخصصی مقالات کنفرانس ها و ژورنال ها
گواهی ثبت مقاله در سیویلیکا
CIVILICA.com

عنوان مقاله:
رویکرد بهینه احراز اصالت گواهی X.509 سامانه های توری با استفاده از الگوریتم مشبکه- مبنا

محل انتشار:
نخستین کنفرانس ملی محاسبات نرم (سال: 1394)

تعداد صفحات اصل مقاله: 7

نویسندگان:
پریسا وارسته نوبیجار - *گروه مهندسی کامپیوتر، دانشکده فنی، دانشگاه گیلان، رشت*

رضا ابراهیمی آتانی - *گروه مهندسی کامپیوتر، دانشکده فنی، دانشگاه گیلان، رشت*

خلاصه مقاله:
ارتباطات توری به عنوان ششمین جایگاه در صنعت حرفه ای فناوری اطلاعات با کارایی وسیع در مباح ث محاسباتی به منظور تامین امنیت ارتباطات نیازمند بکارگیری طرح هایی امن برای تبادل داده در بستر خود می باشد. از آنجا که گواهی های اعتبارسنجی دیجیتال به عنوان یکی از پرکاربردترین و مطمین ترین روش ها در ساختار توری شناخته می شوند. توجه به ساختار درونی، روش های امضا و الگوریتم های مورد استفاده در آنها یکی از موارد چالش برانگیز در حوزه امنیت اطلاعات توری بشمار می رود. در این مقاله ضمن شناسایی ابعاد مختلف ناامنی در ساختار رمزنگاری فعلی، راهکار پیشنهاد ی سیستم رمزنگاری NTRU Lattice مطرح، از جنبه های امنیت و توان مقاومتی در برابر تهدیدات بررسی و سرعت اعتبارسنجی آن به صورت تحلیلی محاسبه می گردد.

کلمات کلیدی:
امنیت ارتباطات توری، گواهی اعتبارسنجی، الگوریتم رمزنگاری، رمزنگاری مشبکه- مبنا

لینک ثابت مقاله در پایگاه سیویلیکا:
https://civilica.com/doc/656572