مجله "پدافند الکترونیکی و سایبری"، سال اول، شماره ۲، تابستان ۱۳۹۲، ص ۷۱-۸۳

تأمین محرمانگی و تمامیت دادهٔ برون‌سپرده، با استفاده از تسهیم راز آستانه‌ای

محمدرضا آذریون[۱]، مصطفی حق‌جو[۲]، مجید غیوری ثالث[۳*]

۱- دانشجوی کارشناسی ارشد دانشگاه امام حسین(ع)، ۲- استادیاردانشکدهٔ کامپیوتر دانشگاه علم و صنعت ایران، ۳- استادیار دانشگاه جامع امام حسین(ع)

(دریافت: ۹۱/۷/۵ ، پذیرش: ۹۱/۱۲/۲۱)

چکیده

در مدل برون‌سپاری داده‌ها، مالک داده، عملیات مربوط به مدیریت داده را به یک سرویس‌دهندهٔ خارجی می‌سپارد تا پرس‌وجوهای کاربران را دریافت کرده و به آن‌ها پاسخ دهد. داده‌ها برای مالکان بسیار با اهمیت است؛ حال آنکه ممکن است سرویس‌دهندهٔ خارجی قابل اعتماد نباشد. بنابراین، حفظ محرمانگی و همچنین تمامیت داده‌ها باید کاملاً مورد توجه قرار گیرد. حفظ محرمانگی داده‌ها به این معنا است که سرویس‌دهندهٔ خارجی از محتوای دادهٔ برون‌سپرده اطلاعی نیابد؛ و تمامیت نیز یعنی مجموع داده‌هایی که به عنوان جواب برای کاربر ارسال می‌گردد، دقیق و کامل باشد. روش‌های مختلفی برای تأمین این اهداف ارائه شده است که هر کدام دارای معایب و مزایایی می‌باشد. به عنوان مثال، می‌توان به استفاده از رمزنگاری، تسهیم داده‌ها و بازیابی محرمانهٔ اطلاعات اشاره کرد. در این مقاله، روشی بر مبنای رویکرد تسهیم داده‌ها ارائه شده است که کارایی بهتری نسبت به روش‌های قبلی دارد و برخی از مشکلات آنها را مرتفع می‌نماید. در روش پیشنهادی علاوه بر تأمین محرمانگی داده‌ها، تمامیت پرس و جوها نیز تأمین می‌گردد.

واژه‌های کلیدی :

محرمانگی و تمامیت داده، برون‌سپاری، پایگاه‌داده، تسهیم راز آستانه‌ای، توزیع داده

Privacy and Soundness of Outsourced Data, Based On Threshold Secret Sharing

Mohammad Reza Azariun, Mostafa Haghjoo and Majid Ghayoori

Abstract

In a data outsourcing model, the owner surrenders his data management operations to an external provider which receives users' queries replies and replies them. Besides, data may be of great importance to owners while the external provider may not be trustworthy. Thus, providing data privacy and integrity of user queries have to be considered, thoroughly. Here data privacy means that owner's data must not be revealed to service provider; and query integrity means that the result set returned to users must be sound, complete, and up-to-date. Different methods, having their own advantages and disadvantage, are proposed to achieve these goal. The methods include, data encryption, private information retrieval (PIR) and data distribution. In this article, a new approach to achieve both data privacy and integrity of user queries is proposed. It is shown that our proposed approach outperforms the existing ones and it supports both the data privacy and integrity of queries.

Keywords: **Privacy and Sundness of Data, Database, Outsourcing, Data Distribution, The Shad Secret Sharing**

* Corresponding Author Email:Ghayoori@ihu.ac.ir