INFORMATION OF THE DOCTORAL THESIS

Thesis title:

DEVELOPING EFFICIENT QUERY METHODS ON ENCRYPTED RELATIONAL DATABASES

Speciality: **Information Systems**

Code: **9.48.01.01**

PhD. Candidate: **Hoang Ngoc Canh**

Scientific Supervisors:

1. **Prof.Dr. Nguyen Hieu Minh**
2. **Dr. Ngo Duc Thien**

Training institution: **Posts and Telecommunications Institute of Technology**

NEW FINDINGS OF THE THESIS:

This thesis makes two primary contributions, proposing ***two corresponding SSE schemes*** that support ***efficient substring queries on character data*** and ***range queries on numerical data*** within encrypted relational databases. The consistent application of the DAS-PROXY model in the implementation of these two proposed schemes demonstrates high feasibility and potential for practical applications. Specifically, the contributions are as follows:

1) This thesis proposes *the construction of a DIQ-SSE scheme* based on blind indexes that support efficient substring queries (via the "$LIKE\ '\%\ substring\ \%'$" condition) on character data within encrypted relational databases. A key contribution of this work is *the development of a sequential query process across two blind indexes,* $Index1$ *and* $Index2$*, and the utilization of novel data structures in their construction*. Specifically, the search mechanism of $Index1$ relies on keywords, offering advantages in terms of fast execution speed, high filtering ratio, and strong security. Conversely, $Index2$ enables precise substring searches, also with good security, eliminates false positive results, and operates solely on the smaller reduced result set returned by the $Index1$ search process.

2) This thesis proposes *the construction of an ESIT-SSE scheme* based on blind indexes that support efficient range queries (via the "$BETWEEN\ l\ and\ h$" condition) on numerical data within encrypted relational databases. A key contribution of this work is *the development of a two-step blind index construction process: Step 1*. Building the NewBucketIndex with overlapping and order preservation mechanisms; *Step 2*. Transforming the NewBucketIndex into IHV hiding vectors that conceal the order information of the indexes. Subsequently, an IHV_B$^+$Tree data structure is built to support secure and high-performance range queries on the IHV vectors.

APPLICATIONS, PRACTICAL APPLICABILITY AND MATTES NEED FURTHER STUDIES

The SSE schemes based on blind indexing proposed in this thesis are suitable for enhancing the security of relational databases in cloud server environments. These schemes show particular potential when deploying Online Analytical Processing (OLAP) systems.

Besides the contributions, there are still several issues that need to be further addressed in the subsequent development direction of this thesis, such as: diversifying query commands, optimizing index storage costs, preventing access pattern leakage, key management, and query load balancing.

Confirmation of representative supervisors	**PhD candidate**
Prof.Dr. Nguyen Hieu Minh	**Hoang Ngoc Canh**