

9-1997

# A Bibliography and Index of Our Works on Belief Data: Concept of Error and Multilevel Security

Shashi K. Gadia

Iowa State University, [gadia@iastate.edu](mailto:gadia@iastate.edu)

Follow this and additional works at: [http://lib.dr.iastate.edu/cs\\_techreports](http://lib.dr.iastate.edu/cs_techreports)

 Part of the [Databases and Information Systems Commons](#), [Information Security Commons](#), and the [Systems Architecture Commons](#)

---

## Recommended Citation

Gadia, Shashi K., "A Bibliography and Index of Our Works on Belief Data: Concept of Error and Multilevel Security" (1997).

*Computer Science Technical Reports*. 87.

[http://lib.dr.iastate.edu/cs\\_techreports/87](http://lib.dr.iastate.edu/cs_techreports/87)

This Article is brought to you for free and open access by the Computer Science at Iowa State University Digital Repository. It has been accepted for inclusion in Computer Science Technical Reports by an authorized administrator of Iowa State University Digital Repository. For more information, please contact [digirep@iastate.edu](mailto:digirep@iastate.edu).

---

# A Bibliography and Index of Our Works on Belief Data: Concept of Error and Multilevel Security

## **Abstract**

In 1988 we initiated our work on belief data. The work proceeded in two phases: in the first phase we formalized the concept of error in everyday record keeping, and in the second phase we considered multilevel security. The purpose of this report is to create an awareness about our works on belief data and to serve as a guide for the following manuscripts. The first two manuscripts are on the concept of errors, and the latter three are on multilevel security. Except [TR97-17], all manuscripts are in their original form.

## **Disciplines**

Databases and Information Systems | Information Security | Systems Architecture

# A bibliography and index of our works on belief data: concept of error and multilevel security

Shashi K. Gadia

Department of Computer Science

Iowa State University

Ames, IA 50011

gadia@cs.iastate.edu

September 1997

In 1988 we initiated our work on belief data. The work proceeded in two phases: in the first phase we formalized the concept of error in everyday record keeping, and in the second phase we considered multilevel security. The purpose of this report is to create an awareness about our works on belief data and to serve as a guide for the following manuscripts.<sup>1</sup> The first two manuscripts are on the concept of errors, and the latter three are on multilevel security. Except [TR97-17], all manuscripts are in their original form.

- [TR97-14] Gadia, Shashi K. and Gautam Bhargava. **A formal treatment of errors and updates in a relational database.** 1988-89. [45 scanned pages; the file size is about 3.4 MBytes]
- [TR97-15] Bhargava, Gautam and Shashi K. Gadia. **The concept of error in a database: An application of temporal databases.** 1989-90. [16 scanned pages; the file size is about 1.0 MBytes.]
- [TR97-16] Tsz Shing Cheng and Shashi K. Gadia. **An algebra for belief persistence in multilevel security.** 1995. [20 pages; 105 KBytes]
- [TR97-17] Gadia, Shashi K. **Applicability of temporal data models to query multilevel security databases: a case study.** 1995-97. [20 pages; 85 KBytes]
- [TR97-18] Tsz Shing Cheng and Shashi K. Gadia. **An algebra for belief persistence in multilevel security.** A revised version of [TR97-16] incorporating some findings from [TR97-16]. 1996. [20 pages; 95 KBytes]

## 1. Concept of error in a database [TR97-14,TR97-15]

The purpose of an update operation is to alter a value, e.g., the salary of an employee, in a database. The need to alter a value arises in two different contexts: first, when a value changes in the real world (e.g., when an employee gets a salary raise); and second, when it is learned that the knowledge (belief) about the salary was incorrectly recorded in the database. [TR97-14,TR97-15] present a model to elevate this problem. This model gives a formal definition and query language for the concept of error in a database. It turns out that this is a non-trivial exercise:

---

1. [TR97-14] and [TR97-15] were a part of the work that Gautam Bhargava and I did toward Gautam's Ph.D. dissertation. The thesis was also published as a technical report TR89-24 by our department. [TR97-15] appeared in 1990 COMAD International Conference on Management of Data. The proceedings of that conference were published in the book **Data Management: Current Trends**, edited by Naveen Prakash, published by Tata McGraw-Hill Publishing Company, New Delhi. A brief treatment also appeared in the book **Temporal Databases: Theory, Design, and Implementation**, edited by Tansel et. al., Benjamin-Cummings, 1993. [TR97-17] is expected to appear in a forthcoming book.

- The concept of error must allow for transition: a value believed to be correct today may be considered in error tomorrow, and yet the after tomorrow the original value may again be believed to be correct.
- Correct and incorrect values reside in the same database. When algebraic operations are performed, incorrect values can assume the role of identity and corrupt information.
- Even key values (e.g., name of an employee) may need correcting, yet the value based identity of an object must persist beyond corrections.

The model in [TR97-14,TR97-15] introduces the concept of anchor. An anchor is the correct value under a given belief. The entire database is anchored before it is queried. An anchor is read-only, that is, it cannot be deleted by the user. The anchoring is done automatically by the system; the anchor cannot be destroyed by the algebraic operators, and it keeps the information meaningful during query evaluation.

## 2. Multilevel security [TR97-16,TR97-17,TR97-18]

Multilevel security is a hierarchical system for beliefs. In a hierarchy of users, the upper users own information not available to lower users. In a multilevel security database, a multiplicity of varying beliefs about a real world object exists at the same time.

### 2.1. The problem of covert channel

In the multilevel security literature it has been pointed out that the classical model is not capable of handling multilevel security data. As an example, suppose that an upper user has some information about an employee named John. By hypothesis, in multilevel security neither this information nor its existence is known to a lower user. Now suppose the lower user learns some information about some other employee, also named John, and tries to add a tuple containing that information to the database. Then the system will reject the insertion complaining that John's tuple already exists in the database. From this message, the lower employee might conclude that some upper user knows John. This is violation of security, in fact a very serious one. It can be shown that this has the potential of setting up a **covert channel** between the two users by which the upper user can leak information (an arbitrary sequences of bits 0 and 1) to the lower user.

### 2.2. Solution: polyinstantiation

It should be clear now that one must be able to maintain multiple instantiations (termed **polyinstantiation**) of a value in a multilevel security database. In current multilevel security literature, polyinstantiation is typically incorporated by adding a USER column to a relation. Thus, in an employee relation the two attributes NAME USER form the key instead of the single attribute USER. This security problem is thereby eliminated.

Polyinstantiation is not new to database. In temporal and spatial databases, the concept of time or space is incorporated either by adding a time or a space column at the tuple level or incorporated at the attribute level. For example, starting with a temporal database model and rewording the term "instant" to "user level" one immediately obtains the core of a model for multilevel security. Therefore, in a mathematical sense, polyinstantiation exists a priori in all temporal and spatial data models. It turns out that there is no hand-waving in this argument, [TR97-17] deals specifically with this point and it makes a detailed comparison between a model in multilevel security and a multilevel security model tailored from a temporal model.

### 2.3. Polyinstantiation and key attributes

All models in multilevel security literature seem to be conceived under the assumption that the key attributes of an object do not vary from one level to another. This is a very strong assumption; yet, it is also important to subject even key attributes in multilevel security to variations in beliefs. In other words, just as nonkey attributes are polyinstantiated, so should be key attributes as well. Belief-based model for errors in [TR97-14,TR97-15] introduced the concept of polyinstantiation for key attributes. The manuscripts [TR97-16] and [TR97-18] achieved polyinstantiation of key attributes in multilevel security databases.

### 3. Reading guide

The manuscripts offer an argument against 1nf modeling of belief data. Although the framework may at first seem overwhelming, the light at the end of the tunnel may well be a user-friendly, reliable query language. Here are some useful hints:

- If the reader is only interested in the concept of errors, he/she should read [TR97-15] before reading [TR97-14]. [TR97-14], which is written in a very formal style, goes over and beyond [TR97-15].
- If the reader has a casual curiosity about the relationship between temporal and multilevel security databases, it is enough to read [TR97-17].
- If the reader is interested in reading about errors as well as about multilevel security, the best starting point is Section 3 in [TR97-18]. For a reasonable appreciation of errors and multilevel security, read [TR97-18] followed by [TR97-15]. For the most detailed understanding of these works all five manuscripts should be read in the following sequence: [TR97-17], [TR97-18], [TR97-16], [TR97-15] and [TR97-14].

Comments about these manuscripts are appreciated. We are aware of a partial error in our definition of the projection operator in [TR97-14,TR97-15]. If a reader discovers any additional errors, the authors will be grateful to be informed about them.