Chapter 8

Locus Standi of the Work

In the present Chapter we tried to find out where does the present research work stand, in the space populated by current academic as well as commercial solutions for office automation. Since, office automation is an active field of research for a long time, a number of work are available. The work related to document production workflow only are discussed here.

8.1 OMAIL

The Office Mail System (OMAIL) [8], developed at Indian Institute of Technology, Kanpur, addresses some of the issues of MPMSD. The system is based on client-server model. In this system server is trusted. By making the server trusted, the responsibility of ensuring integrity, protection and failures can be handled by them. Content integrity of MPMSD is ensured by the server. The server computes a signature of the MPMSD using its secret key whenever a document is given out to reviewers and stores this signature along with the length of the document on which it is computed on, in a per user record. Later on, when the reviewer, after reviewing and adding comments on the
original document, resubmits the document to the server to forward it to another reviewer, this stored signature is used to ensure content integrity of the document by recomputing a signature on the same length of the submitted document and comparing with the stored one. In this system, the document flows from one reviewer to the other via the trusted server, which acts as the arbiter. The reviewer is allowed to append his / her signed comment to the original MPMSD passed to him / her. This implies he/she is allowed to edit the document. But any modification to a previous parts, even by the creator of the parts, are detected by the server when the document is resubmitted to the server by comparing signatures as mentioned above. Similarly, order of parts and dropping of any part can obviously been detected. But the issue of reuse of parts in not addressed in this system. The loophole, in the system lies in allowing the reviewer to add comments directly to the original document and resubmitting it to the server. Moreover, with every review of the document, generation and verification of the signatures on the entire document up to the point of review, overloads the server and thereby slows down the performance. This can be avoided as shown in our schemes. Moreover, the context component is altogether absent in the discussion.

8.2 POLITeam

The decision of the German parliament to move the capital from Bonn to Berlin, increased the demand for a computer and telecommunication based support of ministerial process within and between dislocated government departments. In this context, four projects have been launched by the German research ministry in the framework of POLIKOM. One of the four projects is the POLITeam. The objective of the POLITeam project is the development
of an adequate electronic support for workflows and the coordinated docu-
ment and task processing in a ministry. A scenario of preparing a speech for
a minister is presented in [27]. The request for a speech from a minister is
issued by the minister's office to the manager of the department responsible
for the speech topic. The request along with the background information
are send to the manager in a circulation folder. The managers at the depart-
mental, sub-departmental level acknowledge the receipt of the folder and
additionally provides comments or advises. Then it goes to the unit level
where the speech is prepared in a cooperative process between different peo-
ple of the same unit or of different units. After creation of the draft version,
it is sequentially processed by the managers of the unit, sub-department and
department. Each manager reviews the speech and additionally annotates
the document with her own comments. During the process we get the multi-
ple versions of the document. Only the final version will be presented to the
minister. Since the result of a ministerial procedure will have long lasting
political consequences, the reconstruction of the document history and the
authentication of the reviewer of the concerned version are the fundamental
requirements of the system. We observe that the multi-version workflow doc-
ument in this speech preparation process is a specific case of our more general
MPMSD framework, where each part is a version of the speech. However, the
security issues are not properly spelled out and addressed in the POLITeam
solutions [27] as done in the present work.

8.3 Lotus Notes

Lotus Notes/Domino suite is a popular and commercially successful group-
ware product. The workflow component of the suite is basically the document
production workflow. The production of MPMSD can be implemented in this software by designing a form with multiple sections. Each section of the form contains a comment of a reviewer. But the workflow is rigid in nature. It does not support flexibility in rerouting a document under review. That means, the channel of the review is determined a priori and a form with multiple sections is designed accordingly. A reviewer cannot reroute a particular case of a workflow during review unless the form is modified first in this effect. But flexible routing is a common phenomena in document production workflow in an office. For example, in the scenario discussed in Chapter 1, if the Director feels that before taking a final decision of the travel plan, the comment of the registrar on the matter may be better to be taken for a particular case. Therefore, the registrar may be included as a reviewer in a certain DPW, but for some special cases only and not for all cases. Moreover, the Director may sent back the case to previous reviewer, that means to the finance officer, for further comment. Therefore, a priori fixed form-based solution may be suitable for routine industrial production workflow but it becomes a bottleneck to implement a flexible and dynamic document production workflow in an office. Our solution is naturally flexible. The context component is also not incorporated in Lotus Notes till date.

Lotus Notes implemented RSA crypto method for document security and for transport security it adopted standard web security like Secured Socket Layer (SSL). The protocols based on signed session key, discussed in Chapter 4 are more efficient than, the Lotus Notes protocols, because public-key schemes, like RSA, are much slower than simple symmetric key schemes. Moreover, security model of Lotus Notes has multi-level access control. The access levels are server, database, document, section and field levels. Conventional ACLs are attached to the objects at each level. Therefore, dynamic
authorization is not directly implemented. Currently these authorization
costs have to be implemented as ad hoc application code [5].

8.4 Signcryption

To enhance confidentiality, the current standard approach is to sign a mes­
sage and then to encrypt it with a randomly chosen encryption key. The
encryption key would then be encrypted using a recipient’s public key. This
two step approach is called signature-then-encryption [42] and is popularly
known as a digital envelope. The best example for this is Privacy Enhanced
Mail (PEM), a standard for secure e-mail on the Internet. Signature genera­
tion and encryption consumes machine cycles, and also introduce ‘expanded’
bits to an original message. Hence the cost of a cryptographic operation
on a message is typically measured in the message expansion rate and the
computational time invested by both the sender and the recipient. In the
signature-then-encryption, the cost for delivering a message in a secure and
authentic way is essentially the sum of the cost for the digital signature and
that for the encryption. Whether is it possible to transfer a message of ar­
bitrary length in a secure and authentic way with an expense less than that
required by signature-then-encryption. To answer this question Zheng has
discovered a new cryptographic primitive termed as 'signcryption', which si­
multaneously fulfills both the functions of digital signature and public-key
encryption in a logical single step, and that with a cost significantly smaller
than that required by signature-then-encryption [42, 43]. The signcryption
protocol have certain limitations on verifiability, Only the recipient can ver­
ify the signature. A third party cannot verify the origin of a signcrypted
message independently. In a situation, like the one discussed in the present
work, where one of the two parties involved in the communication is trusted, the digital signature based on signed session key, discussed in Chapter 4 is more efficient than Signcryption. Moreover, there there no limitation on varifiability by a third party.

8.5 Semi-Structured Data

Research on semistructured data was in a primary stage, when the present work was started. By now, semi-structured data has been studied from the database perspective in different works. Prominent among them are the Lore project at Stanford University (http://www-db.stanford.edu/lore), and Sengupta's work, DocBase [35]. Both works try to build formalisms to deal with data which are structured with some form of markups, but the structure is irregular and incomplete, in contrast to relational databases. With the advent of XML as a powerful markup language, Lore project is implementing its Lore data base and its corresponding query language lorel in XML. Lorel uses path expressions as the key feature [31].

Docbase, a database environment for a structured document, structured with SGML is a major work for semi-structured data [35]. The work provides an in depth study on the formalisms for representing a SGML document as a database, where the DTD is the schema of the database. It also provides formal query languages to query SGML encoded data using simple path expressions. Even though this work deals with SGML document database, without any loss of generality it can be extended to XML databases as well. Both Lore and DocBase tries to find out a data element contained in a SGML document using some formalism similar to data retrieval, from a relation. Our work looks into a different aspect of document production and storage.
As a result, in our work, the object of retrieval is a page not an element in a page. The content of a page, in the present work, may be unstructured ASCII strings, or may be structured with, say XML. If we consider the content of a page is marked up with XML, our work may be complementary to these two works. For designing query languages for Page Cube, we derived some concepts from both the works.

8.6 Workflow Authorization

Workflow authorization is discussed in brief in Chapter 6. Role-Based Access Control (RBAC) is a standard tool for enforcing authorizations in security policies, but separation of duty constraint is not addressed by RBAC. Bertino el. al. [9] proposed separation of duty and proposed a language to express both the static and dynamic authorization constraints and also mechanisms to check constraint consistency. Atluri et.al. [5] proposed a model, Workflow Authorization Model (WAM), which provides synchronization of authorization flow with workflow. WAM also supports roles and separation of duty constraints. Enforcement of workflow authorization constraints using triggers and rules in active databases is studied in [13, 12]. In the present work, it is shown that how a simple extension to the page cube model takes care of basic authorization requirements for a DPW. Of course all the authorization constraints discussed in the literature are not taken care of in the page cube model. It remains as a future work.
8.7 Discussion

In the present chapter, some of the currently available solutions for office solutions are reviewed. But these solutions are not complete in nature. Our findings in the present work are not alternatives but complements the existing solutions. The output of the present work may be input to the future solutions for paper-less office. Even the future versions of the existing solutions, like Lotus Notes, Cabinet NG (www.cabinetng.com etc. may include the results of the present work.