Implementation of XML based Digital Signature

Rosalina[1]

[1]Fakultas Komputer, Universitas Presiden
Jln. Ki Hajar Dewantara, Jababeka, Cikarang
[1]rosalina@president.ac.id

Abstract— **With the development of information technology, computer has played more and more important role in many regions and human's life. The number of computer and network users is increasing minutes by minutes which make this global network and its information expanding rapidly day by day. Meanwhile, the modern computerized information system has been developed rapidly and implemented in many regions, such as education regions, enterprise and provides an electronic means to access information and data. As the fast development of computerized system, the W3C group has developed a flexible language named XML. The W3C has deemed the Extensible Markup Language (XML) will form the important basis for the information interchange and accessing in the field of computer network. It will make the electronic exchange of documents and other exchangeable information much easier, convenient and less expensive. At the same time, the security requirement (e.g. integrity, authenticity of the information and/or data and/or signer authentication) of accessing and exchanging information and data in a modern computerized information system has increased rapidly, and now, as the development of XML function, a new efficient security technology is provided which is named XML digital signature (XMLDsig). The XML digital signature provides a more flexible secured technology to keep the integrity and authenticity of data and/or information.**

This paper aim to embed and implement XML based digital signatures to an existing Student Query System model in order to achieve the user authentication and integrity of accessing data and/or information from the system.

Keywords— XMLDsig, Student Query System

I. INTRODUCTION

The rapid development of global network and information technology, computer technology has played an important role in a wider regions. Meanwhile, more and more regions have entered to their e-era revolution which it can be call computer-based era. It provides people a more flexible way to store and access the data and information in an e-era environment. More and more entities build their own relevant computerized information system to record the data. These computerized information systems overcome time, attendance and travel difficulties. As widely and rapidly spreading of global and/or local network information, the proper security mechanism is required to protect the information's authentication and data integrity in the system.

Currently, there are many traditional different security technologies being used in the computerized information system to secure the data and/or information accessing, for example, user name and password. Otherwise, even though the system developer uses the password technology to secure the system, there are still many password-hackers to attack the system and steal the data and/or information. Besides these traditional security technologies, standards like SSL/TLS (Secure Socket

Layer/Transport Level Security) for point-to-point security already exist. S/MIME (Secure/Multipurpose Internet Mail Extensions) and PGP (Pretty Good Privacy) ensure that only a message's intended recipient can read that message—thereby achieving end-to-end security. It turns out that (fortunately) the World Wide Web Consortium (W3C) XML Encryption Working Group did have good reasons for XML digital signature. XML digital signature addresses two requirements that none of the above standards can satisfy together: end-to-end security and selective encryption; it take care of the specific properties of the signed data and documents.

Since most internal enterprise local computerized systems always focus on the means of setting password and user name, but always ignore the problem of user authentication and data integrity during accessing to the system. Hereby, most computerized information systems such as a simple existing Student Query System(SQS) model are lack of security during the data and/or information accessing requirement, especially for example, during the accessing and checking the student grade process where integrity and authentication play an importance role to the system.

This paper would like to analyze the methodology and embed XML based digital signature in an existing Student Query System (SQS) model to achieve the visual implementation of XML digital signature. XML stands for Extensible Markup Language, which is a markup language for documents containing structured information and the kernel for many other technologies. Besides researching the concept of XML digital signature, it would also implement XML based digital signature in an existing computerized system model called Student Query System (SQS) model to support this research.

II. THEORY

Digital Signatures have become an important aspect of electronic security because they can be used to ensure the integrity, authenticity and non-repudiation of data. In normal XML signature, the verifier does not need the signer's validation for verifying the signed document where this is harmful as the one who signed the document can deny the signing of document. With the help of undeniable signatures, the verifier requires the signer's verification for verification of the document[1].

XML signature standards are digital signatures designed for use in XML transactions. The standard defies a schema for capturing the result of a digital signature operation applied to arbitrary (but often XML) digital data. XML-based digital signatures add authentication, data integrity, and support for non-repudiation to the data and at the same time to take account for the advantage of network and XML. The signature object itself appears in XML syntax and makes used of a number of XML standards to define its precise XML format. The objectives of XML digital signature are:

- To ensure in-transit data are complete and accurate (for data integrity)
- To provide a mechanism to control and manage the data that is passed and presented

There are three basic types of XML Signatures[1],[3],[4],[2]: Enveloped Signature, Enveloping Signature and Detached Signature.

A fundamental feature of XML signature is the ability to sign only specific portions of the XML tree rather than the complete document. This will be relevant when a single XML document may have a long history in which the different components are authored at different times by different parties, each signing only those elements relevant to it. This flexibility will also be critical in situations where it is important to ensure the integrity of certain portions of an XML document, while leaving open the possibility for other portions of the documents to change. Consider, for example, a signed XML portion documents delivered to the system. If the signature were over the full XML form, any change by the user to the default form values would invalidate the original signature.

III. *METHODOLOGY*

3.1.1 XMLDsig based SQS model Analyzed Concept

Since the XMLDsig based Student Query System model focuses on the implementation of XML digital signature technology, one of principle outputs will be the XML digital signature (XMLDsig) generation and validation information. Meanwhile, this existing SQS model must also be able to show the student basic information, such as StudentID, StudentName, Gender, Major, Grade as so forth. Furthermore, it would also show the student grade information accordingly.

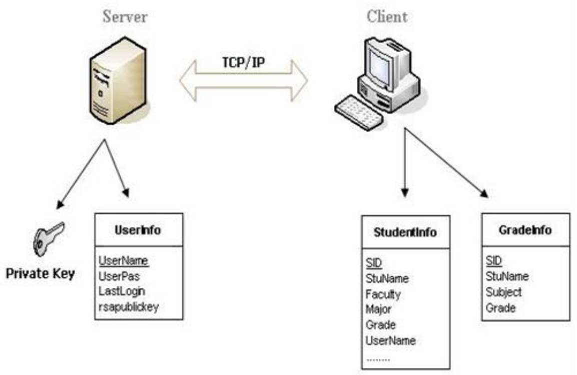


Figure 3.1 *XMLDsig based SQS basic design concept*

This paper is discussing the implementation of XMLDsig technology in an existing SQS model, the new aspects of system input design is embedding XMLDsig technology before the user can log-in and make query to access the system data. Before logging in the system, the user not only has to enter the traditional authorized information such as username and password, but also the user has to pass the XMLDsig authentication. In this case, the user will get a username, password and his/her own XMLDsig private key, which is used to encrypt the data and generated the XML digital signature, from the XML digital signature server, before logging-in the SQS, the user has to show his/her own private key and pass the XMLDsig verification. During the XMLDsig verification, the system will show the user himself the XMLDsig information and system log-in freely; otherwise, the system will deny the requirement. During the query process, before user can access the query, the system will send the query requirement together with the user XML digital signature, then the XMLDsig server will verify the user XML digital signature, if passed, the user can access the query successfully, vice versa.

This existing SQS model as a background platform of XMLDsig and the only precious main objective here is to show the visual implementation of the XMLDsig technology, according to this main objective, the existing SQS model would only require to collect the student information, user information and student's grade information to support the XMLDsig technology research without including complicated information system process.

For SQS model database support, it will use Microsoft SQL Server 2000 to store the basic user information, student information and so forth. Since Microsoft SQL Server 2000 is a full-featured relational database management system (RDBMS) that offers a variety of administrative tools to ease the burdens of database development, maintenance and administration, then this existing SQS model uses Microsoft SQL Server 2000 to be the database support.

3.2 XMLDsig based SQS in DFD Structure

Generally, the private key is used to keep secret, while the public key may be widely distributed. Both of private key and public key are related mathematically, but the private key cannot be practically derived from the public key. A message encrypted with the public key can be decrypted only with the corresponding private key. To send an encrypted message to someone, the sender uses the receiver's public key to encrypt the message; then in order to decrypt the message, the receiver uses the private key. Otherwise, in this XMLDsig based SQS project, the private key and public key are used in reverse. In XML digital signature, the private key is used to encrypt the digest and then generate the XML based digital signature; and the public key is used to decrypt the digest and finally verify the XML based digital, thereby proving that the sender signature and that the message has not been tampered with.

In the XMLDsig based SQS model, there are two main parts which are XMLDsig server and client mentioned above. The XMLDsig server create new username, password and generate the private key and public key. Before logging in SQS successfully, the client/user has to get his/her username, password and his/her own private key from the XMLDsig server, then the client/user uses his/her own username, password and unique private key to log in the system.

Since each client/user has his/her own unique private key, even though other persons know his/her username and password, they still cannot log in the system without that private key because he will be failed to pass the XMLDsig verification. It means that only the real user can enter the system and access the student data of the system. The data of system is only available for the user who shows his/her own private key. This process finally helps system client/user to achieve the data integrity and authentication.

In order to show a clear design and analysis concept of XMLDsig based SQS model, the following data flow diagram will show the details of XML digital signature theory in the SQS model. It includes two main parts: server side which belongs to server, and the client/user side. Meanwhile, inside these two main parts, XMLDsig based SQS model includes three main processes, first is "1.Create New User" which happens in the XMLDsig server side; second is "2. Log in" process and third is "3. Process Query (SQS)" in the client side. (see Figure 3.2) The XML digital signature will be embedded in the log-in process and query process.

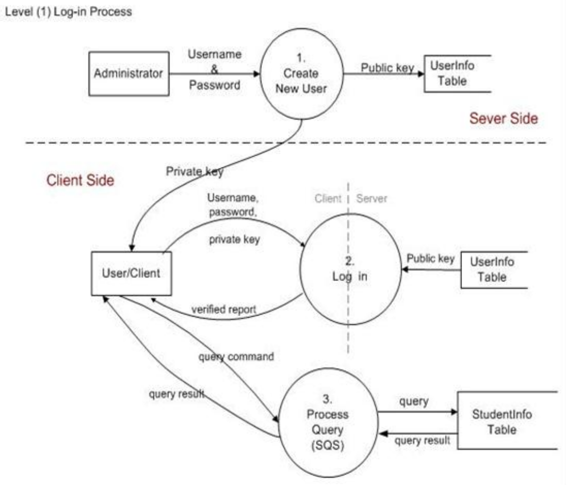


Figure 3.2. *XMLDsig based SQS level (1) Log-in Process*

During the log-in process, the user/client enters his/her own username, password and shows the private key, and then the system will create the XMLDsig based on the username, password and private key. After that, the user XML digital signature would be sent to the XMLDsig Server for verification. Meanwhile, the XMLDsig would decrypt and verify the XML digital signature using user public key and return a verified report to the user. If the current user passes the XMLDsig verification, it means that the current user is the purported user. This purported user has right to access to the data in the system; vice versa.

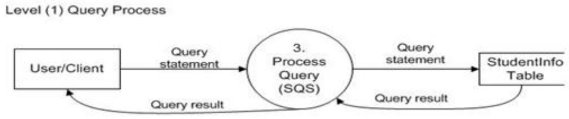


Figure 3.3. *Level (1) Query Process*

In this XMLDsig based SQS model, the second XML digital signature implementation example is in the "3. Process Query (SQS)". During query, the system would send the query requirement together with user XML digital signature to the XMLDsig server, then the server will decrypt and verify user XML digital signature before executing user query requirement. After verification, the XMLDsig server would send a verification reports to the user, if verification succeeded, the query will be executed, and otherwise, the query requirement will be denied.

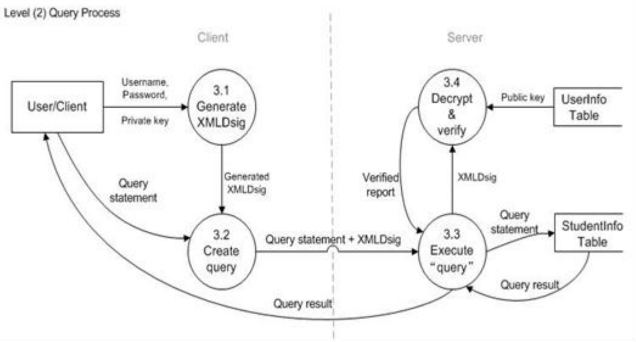


Figure 3.4. *Level (2) Query Process*

IV. RESULT AND DISCUSSION

4.1 The Main Functions of XMLDsig based SQS model

In the XML digital signature concept, the user must keep him self private key carefully since the user need to show his private key while logging in the system. During system logging in, the user must show his own private key, at the same time, the system generates an XML document based on the user information, and then create the user XML digital signature by encrypting this XML document using user private key, then send the encrypted data together with the original data to the XML digital signature server. Meanwhile, in order to make sure the user pass the XML digital signature authentication, at the XML digital signature Server, after received the data from client side, the system would divide the original data and the encrypted data, and then use the same algorithm to calculated the digest value D form original data; and get the digest value D' by fetching the user public key from database to decrypt the encrypted digest message. Finally, check whether D and D' is equal. After matching the D and D' digest value, it means that the user who wants to access to the system is the proper user but not faker, then the system will show the logging-in enable to the current proper user (see Figure 4.1).

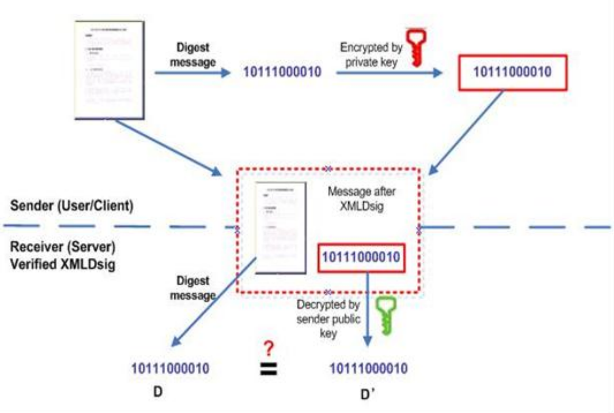
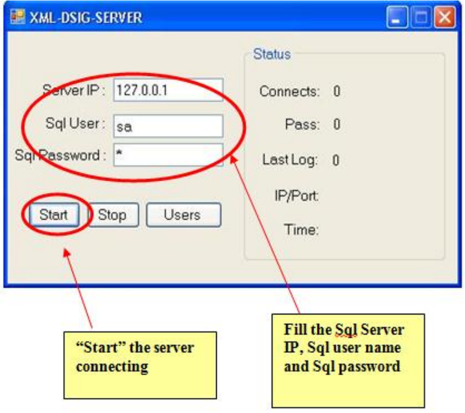


Figure 4.1. *XMLDsig Implementation Reference*

That is why, if someone else steal the username and password but without the user private key, the user cannot pass the XML digital signature testing, and then the system logging-in will be disable. Meanwhile, the user's private key cannot be duplicated easily since it is generated during creating new user in the XML digital signature server. As long as the user logs in the system by showing his or her correct private key, then all the manipulation or operation behaviors which happen in the system belong to current user. The current user cannot deny what he or she has done to the system because he or she can only log in by using his or her own username, password, private key and the XML digital signature testing.

4.2. The Main testing procedures of XMLDsig based SQS

The first design concept of this XMLDsig based SQS model includes two parts; one is XML digital signature server. Before running the whole SQS model, the administrator needs to start the XML digital signature server (see Figure 4.2). The XMLDsig Server requires administrator to fill the server IP, SQL user name and password in order to connect to the Microsoft SQL Server 2000. If XMLDsig based SQS model is tested in the same computer but not remote server, then the Server IP is "127.0.0.1", SQL user name is "sa" and password is "1". Otherwise, the server IP should be the remote server IP address, for example, "192.168.88.*".



Server IP: 127.0.0.1
Sql User: sa
Sql Password: *

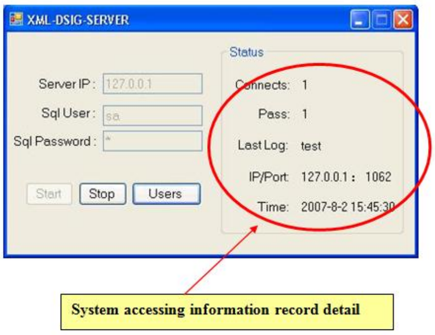
Status
Connects: 0
Pass: 0
Last Log: 0
IP/Port:
Time:

"Start" the server connecting

Fill the Sql Server IP, Sql user name and Sql password

Figure 4.2. *XMLDsig Server*

When "Start" the connecting of SQL server, the administrator can enter to "USERS" form to create and delete the user, or read the existed user information. In the "USERS" form, there is existed user list which keeps record of user's information. The administrator can create a new username, password by clicking "ADD"; meanwhile, the XMLDsig server would create the user private key and public key according to the new user information. The Private Key will be saved into a key file named *.key and the public key will be saved into the system database together with the user information. At the same time, the XMLDsig server would return a report for the private key generation. The administrator can take the generated user private key and give to the proper user together with user name and password. Then the user has the right to access to SQS model by entering the username, password, showing his/her private key to the system and passing the XML digital signature authentication. Meanwhile, at the XMLDsig server side, the server keeps running in order to monitor and record the client side system accessing information (see Figure 4.3).



Server IP : 127.0.0.1
Sql User : sa
Sql Password : *

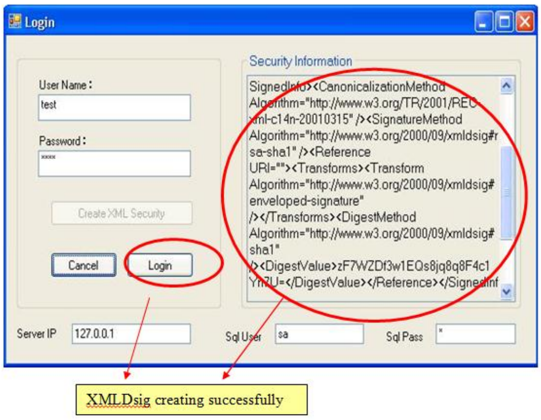
Connects: 1
Pass: 1
Last Log: test
IP/Port: 127.0.0.1 : 1062
Time: 2007-8-2 15:45:30

System accessing information record detail

Figure 4.3. *Record of system accessing I*

If there is more than one user logging-in behavior such as twice, in the XML digital signature server side, the "Connects" will be "2". Meanwhile, the "Pass" will show the logging-in information whether both two users pass the XML digital signature verification or not. "Last Log" shows the recent system log-in user and the "Time" shows the log-in time.

In the SQS model client side, the user must enter his/her own username, password and pass the XML digital signature verification if he/she wants to access to the system successfully . After filling user information, then click "Create XML Security", the client side will create XML digital signature based on the user logging-in information using current user private key. After succeeding in creating the XML digital signature security in client side, the system will envelop the user information together with the user-information-based XML digital signature and send to the XMLDsig server in order to verify the user XML digital signature. While creating the XML digital signature in client side, the system would read the user private key. If found the current user private key, the user XML digital signature would be created successfully (see Figure 4.4). At the same time, in the "Login" windows, it will show the XML digital signature generation in details. This "Security Information" includes the user log-in information and the detailed XML digital signature generation information.



User Name : test
Password : ****

SignedInfo><CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" /><SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" /><Reference URI=""><Transforms><Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" /></Transforms><DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" /><DigestValue>zF7WZDf3w1EQs8jq8q8F4c1Yn7U=</DigestValue></Reference></SignedInf

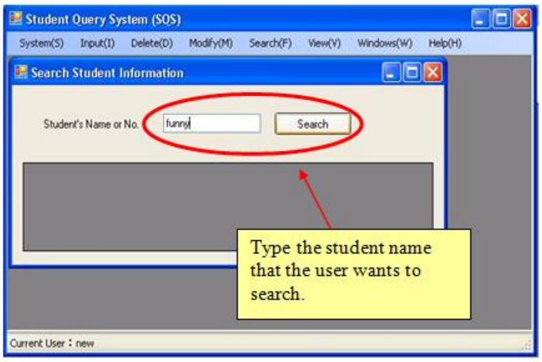
Server IP 127.0.0.1
Sql User sa
Sql Pass *

XMLDsig creating successfully

Figure 4.4. *Creating XML digital signature*

Then the "Login" is available if the user XML digital signature is created successfully. While user clicks "Login", the system will send the user XML digital signature to the XML digital signature server for verification. After XMLDsig server received the enveloped user XML digital signature data, it would read the user XML digital signature. Meanwhile, the server would access the user public key from the database, and decrypt the encrypted user information. If the user log-in information is match, the XMLDsig server would return a successful result to the user which is "Login OK". It means that the user is proper current system user and has the right to access to the system.

The second implementation of XML based digital signature is embedding in the "Process Query". During the "Process Query", for example, search student information, the user types the student name whose information the user would like to check, and then click "Search" button to send the query requirement (see Figure 4.5). Before getting the search result, the system will send the user's query statement to the XMLDsig server together with user's XML digital signature. In the XMLDsig server, the server will check the authenticity of user‘s XML digital signature.



Student's Name or No. funny

Type the student name that the user wants to search.

Current User : new

Figure 4.5. *Making Search Query*

After click "Search" button, the user must fill the "Query Verify" information, then click "Create XML Security" to generate the XML digital signature, and then click “Send” to send the generated user XML digital signature to the XMLDsig server for verificat). If verification ok, then the user would receive a result message from the system, then click ok.

4.3. Project Evaluation of XMLDsig based SQS

a) Succeed in embedding and implementing XMLDsig in an existing SQS model based on XML digital signature research

The main objective of this XMLDsig based SQS model is analyzing, researching and gaining the knowledge about XML digital signature through implementing the XML digital signature in an existing computerized system model. Finally, XML based digital signature has been embedded and implemented into the existing SQS model successfully. In a word, this XMLDsig based SQS model is almost achieve the objective of this XMLDsig based SQS project based on the XML digital signature knowledge.

In general, this XMLDsig project performs well and is easy to implement by the system users. Although this XMLDsig based SQS model is developed in a very short period (about 1 month), basically, it reflects almost the design concept discussed above in the paper and the objective of XMLDsig based SQS model. The system is built and developed around XML digital signature technology as the core new technology in a system authentication security. It applies a modern XML based digital signature technology and cryptography concept. It has performed successfully in the real computerized application and become an assuring new computerized system security technology. Moreover, the program is compatible with almost programs on Windows platform and requires very limited hardware.

b) New security function in an existing SQS model

The newest function of this XMLDsig based SQS model is: the XML digital signature based SQS model is safer than the general SQS model which is only secured by username and password. Even though other person got the username and password by accident, he/she doesn’t have the proper user private key, and then he/she will be rejected by the system. The system would return a caution report to tell non-proper user to show his/her private key, otherwise the system resource is forbidden to the non-proper user.

Possibly, the proper user forgets to show his/her private key, the system will return a reminding message to the user . Moreover, the private key cannot be duplicated easily and because of the characteristic of the algorithm of digest message, it can also make sure whether the original data has been modified or not. If the current user could not show the correct private key, no matter he or she is the non-proper user and proper user, both of them cannot access the system because the “Login” is disable. All the system resources are disabling for the user without showing correct private key. This new security concept of system user authentication makes sure the system data cannot be modified by the non-proper system user, thereby to keep the data integrity and user authentication. Finally, make the system resource safer and more secure.

Comparing to the original existing Student Query System, the XML digital signature based SQS model has many advantages dealing with the system security issue. For example, in the original existing SQS model which only has username and password, if the others steal the username and password, he/she can log in without any other security verification. Meanwhile, all the modification of data will be considered to the original user but not the faked user. It means that the faked user can modify any data and deny what he or she has done to the system without bearing any responsibility. Assume that the data in the SQS is very important, for example student grade; the faker can log in using stolen username and password and change his or her grade, even log-in to see other student private information. That is the security weakness of the original SQS model; otherwise, the XMLDsig based SQS model needn’t worry about this by embedding XML digital signature into the user logging-in process and query process.

c. Drawback in XMLDsig based SQS model

Although this XMLDsig based SQS model has its own security advantage compared to the general modern computerized system. However, XMLDsig based SQS model also has its weakness due to the fresh of technology and network hacker development. For example, the key calculating algorithm is limited which can be implemented easily. If the hacker really wanted to steal the important system resource, and if he or she knew the key algorithm that the XML digital signature uses, it can run the algorithm to get the private key and public key.

V. CONLCUSIONS

This XMLDsig based SQS model, compared with the traditional digital signature, XML digital signature has its own advantages, which support and provide the digital signature and authentication to a different specific portion data. This can decrease the traffic of data, and increase the flexibility of data transmitted. Furthermore, XML digital signature can be able to analyze the XML file preciously, at the same time, keep structured of XML file well. Besides, private key information provided by XML digital signature is easy to understand. It is more convenient to authenticate the digital signature in the computerized system and achieve the data integrity.

REFERENCES

[1] Bertino, E., Carminati, B. and Ferrari, E. (2001) 'XML Security',Elsevier Science Ltd. Information Security Technical Report, Vol. 6, No. 2, pp. 44 –58.

[2] Sun, L. and Li, Y, “XML Undeniable Signatures”,In Proceedings of InternationalConferenceof Computational Intelligence for Modeling, Control and Automation and International Conference on Intelligent Agents, Web Technologies and Internet Commerce. 2005.

[3] Han, W. Y., Park, C. S. and Lim, S. Y. (2011) 'An XML Digital Signature for Internet e-business Applications', In Proceedings of International Conference in Info-tech and Info-net, pp. 23 –29.

[4] Nordbotten, N. A. (2009)'XML and Web Services Security Standards', IEEE Communications Survey and Tutorials, Vol. 11, No. 3,pp. 4 –21

Data Sharing Application with SMS Notification

[1] **Bernardus Satrio Palapessy**, [2]**Nur Hadisukmana**
[1,2] President University, Jl. Ki Hajar Dewantara, Cikarang Baru, Bekasi
[1,2] Fakultas Komputer
e-mail: [1]palapessy.rio@gmail.com,[2]anursu2002@yahoo.com

Abstract— **The result of the research is the application that allow user to retrieve information through News and Event Agenda Feature. This application also allows the member to keep in touch with their stuff with SMS notification. The application is easy to control by an administrator through a message system and capabilities of administrator of any file, also by a user hierarchy system.**

Keywords—**data sharing, sms notification**

I. INTRODUCTION

Good communication in an organization will make the working condition more conducive. Data sharing among members of the organization is one form of communication. There are many ways for people to share data with others. Today, there are many applications or web sites that allow the user to upload and download any data. In many organizations, the accesses to web sites that have this functionality are often blocked because the company sees them as a threat that can harm work productivity of the worker.

The number of websites that provide this functionality has been increased from time to time. This fact shows that the number of users of that web site is also increased. Youtube.com as one of the largest data sharing site has their daily data transfer equal to 75 billion text email. It means many people need to share something to others. This communication can lead to a better relationship in a community. This kind of communication can be brought into office environment. Data sharing among the members can lead to a better communication of the member.

In most organization, file sharing is an inseparable part of daily activities. Easy and smooth sharing of data and files leads to work efficiency. Data sharing tool can also act as a news centre for the organization. Therefore, the need to have a reliable file sharing system is crucial. Unfortunately, many organizations do not equip themselves with this tool.

The beneficial of data sharing application will be reduced when there is no enough controlling by an administrator. Enough control is needed to enhance the beneficial of data sharing. And also the sense of belonging from data that been shared is highly needed as a sense of responsibility when sharing a data.

The application created in this research isdivided into three main parts. The first part is “News” part. This part will show any news that written by administrator and moderator. The entire member can read the news and also give a comment on it. Whenever a member writes a comment to News there will be a SMS notification to the writer of the particular News.

The second part is “Event”. In this part, the administrator and the moderator can write down an event that will be shown in the format like calendar. The event can be shown in daily, weekly, and monthly. Just like in News part, whenever a member writes a comment to an Event there will be an SMS notification to the writer of the particular Event.

The last part is “File” part. In this part, the entire user can do uploading and downloading data. The entire file that has been uploaded will be checked to determine the type of the file. In the download section, there will be a list that shows the entire file that already uploaded before. The file will be arranged in its name order or its uploaded date order. There is also a search feature that will make file browsing become easier. In the downloaded section, member also can put a comment in every file, SMS notification also sent to the owner of the file.

The application can be access through a local area network. This application works like a digital library with more variety of content. This application will develop using PHP technology with additional java script and using NowSMS application to send SMS Notification.

II. THEORY

A. Data Sharing

Data sharing is the practice of making data used for scholarly research available to other investigators. Many funding agencies, institutions, and publication venues have policies regarding data sharing because transparency and openness are considered by many to be part of the scientific method. A number of funding agencies and science journals require authors of peer-reviewed papers to share any supplemental information (raw data, statistical methods or source code) necessary to audit or reproduce published research. A great deal of scientific research is not subject to data sharing requirements, and many of these policies have liberal exceptions. In the absence of any binding requirement, data sharing is at the discretion of the scientists themselves. In addition, in certain situations agencies and institutions prohibit or severely limit data sharing to protect proprietary interests, national security, and patient/victim confidentiality. Data sharing (especially photographs and graphic descriptions of animal research) may also be restricted to protect institutions and scientists from misuse of data for political purposes by animal rights extremists.

Data and methods may be requested from an author years after publication. In order to encourage data sharing and prevent the loss or corruption of data, a number of funding agencies and journals established policies on data archiving. Access to publicly archived data is a recent development in the history of science made possible by technological advances in communications and information technology.

Despite policies on data sharing and archiving, data withholding still happens. Authors may fail to archive data or they only archive a portion of the data. Failure to archive data alone is not data withholding. When a researcher requests additional information, an author sometimes refuses to provide it. When authors withhold data like this, they run the risk of losing the trust of the science community.

B. Digital Library

A digital library is much more than just the collection of material in its repositories. It provides a variety of services to all of its users (both humans and machines, and producers, managers, and consumers of information). There are a large and varied set of such services, including services to support management of collections, services to provide replicated and reliable storage, services to aid in query formulation and execution, services to assist in name resolution and location, etc. The basis for a digital library, however, must be the information objects that provide the content. A basic characteristic of the digital library is that the information objects are found in collections with associated management and support functions.

The goal of the digital library is to assist users by satisfying their needs and requirements for management, access, storage, and manipulation of the variety of information stored in the collection of material that represents the "holdings" of the library. Users may be humans or they may be automated processes acting on behalf of or in support of human needs. Users also vary and include those who are "end" users (those not involved in the management and operation of the library but rather are the customers), library operators, and information "producers" who want their material available through the library.

The key to effective collections management is to implement simple structural organizations and be able to present those organizations in a way that library users find useful and can understand easily. In traditional libraries, books are primarily stored by subject, title, author, and date, and accessed by following signs to the appropriate floor, room, bookcase, shelf, and spine-labeled book. The size and relative celebration of each portion of the collection gives patrons information about the collection and can reveal the library's collection management objectives as well.

A library is created to serve a community of users. Users who participate in the digital library should be aware of its design and be able collectively to refine that design to better serve their own information needs. Therefore, the ongoing human usability of a digital library depends on the clear and unobtrusive exposure of the library's design, its near-term goals, and its overall objectives.

Furthermore, digital libraries should continue the ongoing tradition of coupling utility with aesthetics in the organization and presentation of materials.

C. Existing Application

4shared.com

4shared.com is a Ukrainian file sharing service based in Kiev. This application allows user to upload and download file to their account. 4shared.com start operating in 2005. 4shared.com is a free online file sharing service.

Megaupload

Megaupload is a Hong Kong based company that allow user to do file sharing. Every user that done the uploading process will have a unique URL as a address to download. Every file that has not been downloaded for 21 days will expires.

Table 2.1. *Comparisons*

Point of View	**Your One Way**	**4shared.com**	**Megaupload**
Upload	OK	OK	OK
Download	OK	OK	OK
Searching	OK	OK	Not OK
News	OK	Not OK	Not OK
Event Agenda	OK	Not OK	Not OK
Advertising	Not OK	OK	Not OK
Large Size File Sharing	Not OK	Not OK	OK
File Preview	Not OK	OK	Not OK

III. METHODOLOGY

Your one way application is made by a methodology called Rapid Application Development. Rapid Application Development (RAD) is a methodology for compressing the analysis, design, build, and test phases into a series of short, iterative development cycles. This has a number of distinct advantages over the traditional sequential development model. Rapid application development promotes fast, efficient, accurate program and/or system development and delivery. Compared to other methodologies, RAD generally improves user/designer communication, user cooperation, and user commitment, and promotes better documentation. The author use RAD system due to a fast system that RAD shows to give the author more time to do preparation and post production.

IV. RESULT AND DISCUSSION

Data sharing system is about the communication among the user and transferring the data itself. The main components of a data sharing software are the administrator, the user client, and the system manager. The sequence diagram of Upload File, Add Member, Add News and Add Event is shown in Figure 4.1.

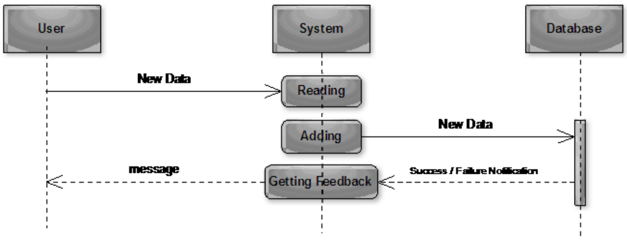


Figure 4.1 *Upload File, Add Member, Add News and Add Event Sequence Diagram*

In order to download file, user will send a request to the system about the ID of the desire file that he/she want to download. Then the system will make a query to database to get the data about the file and also send the message box about the file and the download process. The user will validate that he/she want to download, then the system will do the process download from database to user computer. The system also sent a SMS notification to the owner of the file and the dowload sequence diagram is shown in Figure 4.2.

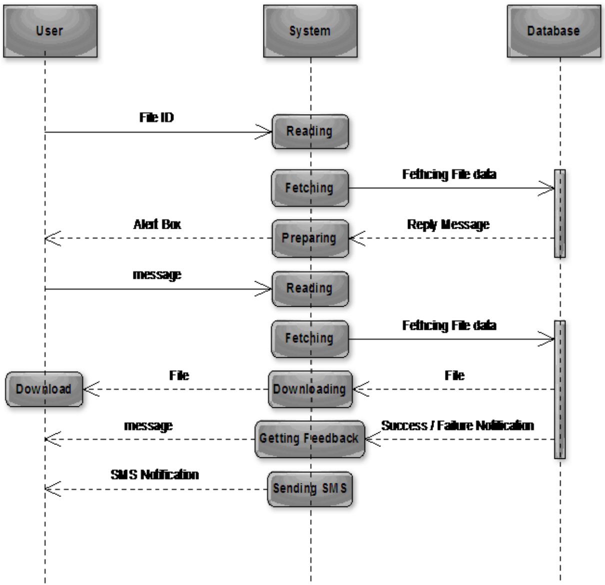


Figure 4.2. *Download Sequence Diagram*

Searching features is used to make the Member easier to browse the file inside the database. The search system also makes the member faster to found their wanted file.

Member will fill the search form, then the system will process it end send a relevant query to database to get the expected result.

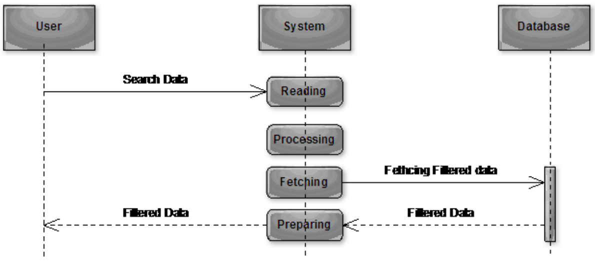


Figure 4.3. *Searching Sequence Diagram*

To send the SMS notification, the author use NowSMS software. This is an SMS gateway that easy to use and have a user friendly interface and the Intranet schema is shown in Figure 4.4.

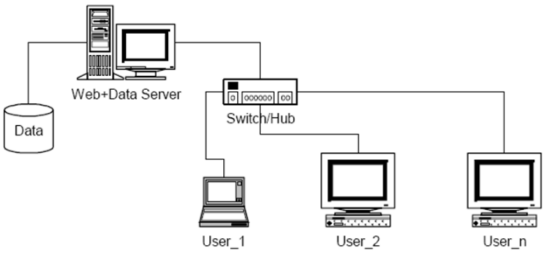


Figure 4.4. *Intranet Schema*

The ERD shows how all the database entities relate each other. There are 9 tables in the database to store the information regarding to each class

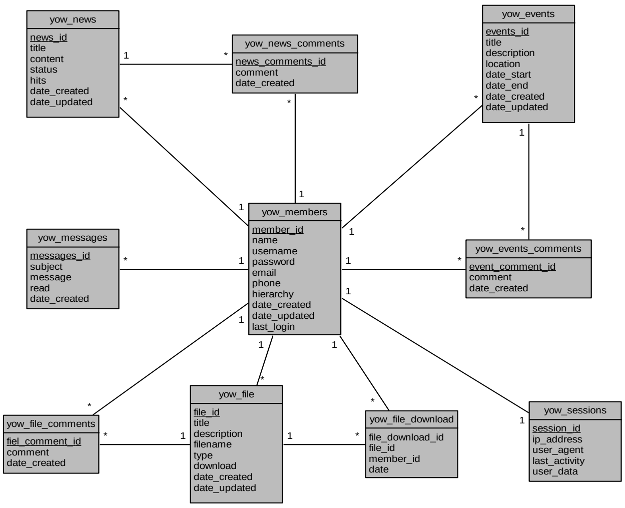
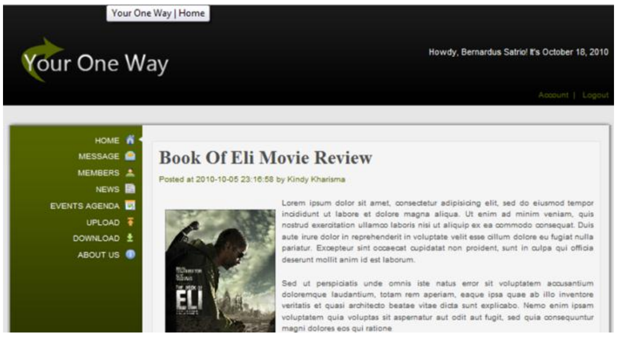


Figure 4.5 *ER Digram*

The interface of this application will adopt a common pattern of any application with menu in the left side.



Book Of Eli Movie Review

Posted at 2010-10-05 23:16:58 by Kindy Kharisma

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam, eaque ipsa quae ab illo inventore veritatis et quasi architecto beatae vitae dicta sunt explicabo. Nemo enim ipsam voluptatem quia voluptas sit aspernatur aut odit aut fugit, sed quia consequuntur magni dolores eos qui ratione

Figure 4.6 *Interface*

V. CONCLUSION

The author has developed an application that can be used to do data sharing in an organization. The data sharing application also has several additional functions beside data sharing that can enhance the quality of communication along the member of the company. The additional functions are “News” and “Event”. This application tries to provide information to the user with the latest activities that happen in the organization. This kind of information can enhance the sense of belonging of the member in the organization. This application also can add the awareness of the member of an organization. This application used PHP technology with Rapid Application Design.

REFERENCES

[1] Alexandrou, Marios. Rapid Application Development (RAD) Methodology. Retrieved February 2, 2010 from mariosalexan

[2] Deitel, P., & Deitel, H. (2009). Internet & World Wide Web, How To Program. New Jersey: Pearson Education, Inc.

[3] Duffy, S. (2003). How To Do Everything With Javascript. McGraw-Hill/Osborne.

[4] Fulghum, E. (2009). Learning PHP: The What's and the Why's. Retrieved February 2, 2009, from Developer.com

[5] From: http://www.developer.com/lang/php/article.php/900521

[6] Kahn, R. E., and Cerf, V. G, “An Open Architecture for a Digital Library System and a Plan for Its Development”, the Digital Library Project Volume I: The World of Knowbots, 2003

[7] M. Leyner. Barry, “The scope of digital Library”, DLib Working Group on Digital Library Metrics, 1998

INFORMATION FOR AUTHORS

Articles are accepted from President University faculty members and from outside President University, in the area of Information Technology, submission of the paper is assumed that it has never been published elsewhere. Articles are written in Indonesian or English. Papers will be reviewed through a refereeing system and acceptance for publication will be based on originality and scientific validity.

The format of the paper is follows:

Sample IEEE Paper for A4 Page Size

First Author[#1], Second Author[*2], Third Author[#3]

[#]*First-Third Department, First-Third University*
Address Including Country Name
[1]first.author@first-third.edu
[3]third.author@first-third.edu

[*]*Second Company*
Address Including Country Name
[2]second.author@second.com

Abstract— **This document gives formatting instructions for authors preparing papers for publication in the JOURNAL IT FOR SOCIETY. The authors must follow the instructions given in the document for the papers to be published. You can use this document as both an instruction set and as a template into which you can type your own text.**

Keywords— **Include at least 5 keywords or phrases**

I. Introduction

This document is a template. For questions on paper guidelines, please contact the publications committee secretariat@president.ac.id.

II. Page Layout

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

D. Page Layout

Your paper must use a page size corresponding to A4 which is 210mm (8.27") wide and 297mm (11.69") long. The margins must be set as follows:

- Top = 19mm (0.75")
- Bottom = 43mm (1.69")
- Left = Right = 14.32mm (0.56")

Your paper must be in two column format with a space of 4.22mm (0.17") between columns.

III. Page Style

All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified.

E. Text Font of Entire Document

The entire document should be in Times New Roman or Times font. Type 3 fonts must not be used. Other font types may be used if needed for special purposes.

Recommended font sizes are shown in Table 1.

F. Title and Author Details

Title must be in 24 pt Regular font. Author name must be in 11 pt Regular font. Author affiliation must be in 10 pt Italic. Email address must be in 9 pt Courier Regular font.

TABLE I
Font Sizes for Papers

Font Size	**Appearance (in Time New Roman or Times)**		
	Regular	**Bold**	**Italic**
8	table caption (in		reference item

	Small Caps), figure caption, reference item		(partial)
9	author email address (in Courier), cell in a table	abstract body	abstract heading (also in Bold)
10	level-1 heading (in Small Caps), paragraph		level-2 heading, level-3 heading, author affiliation
11	author name		
24	title		

All title and author details must be in single-column format and must be centered.

Every word in a title must be capitalized except for short minor words such as “a”, “an”, “and”, “as”, “at”, “by”, “for”, “from”, “if”, “in”, “into”, “on”, “or”, “of”, “the”, “to”, “with”.

Author details must not show any professional title (e.g. Managing Director), any academic title (e.g. Dr.) or any membership of any professional organization (e.g. Senior Member IEEE).

To avoid confusion, the family name must be written as the last part of each author name (e.g. John A.K. Smith).

Each affiliation must include, at the very least, the name of the company and the name of the country where the author is based (e.g. Causal Productions Pty Ltd, Australia).

Email address is compulsory for the corresponding author.

G. Section Headings

No more than 3 levels of headings should be used. All headings must be in 10pt font. Every word in a heading must be capitalized except for short minor words as listed in Section III-B.

1) Level-1 Heading: A level-1 heading must be in Small Caps, centered and numbered using uppercase Roman numerals. For example, see heading “III. Page Style” of this document. The two level-1 headings which must not be numbered are “Acknowledgment” and “References”.

2) Level-2 Heading: A level-2 heading must be in Italic, left-justified and numbered using an uppercase alphabetic letter followed by a period. For example, see heading “C. Section Headings” above.

3) *Level-3 Heading:* A level-3 heading must be indented, in Italic and numbered with an Arabic numeral followed by a right parenthesis. The level-3 heading must end with a colon. The body of the level-3 section immediately follows the level-3 heading in the same paragraph. For example, this paragraph begins with a level-3 heading.

H. Figures and Tables

Figures and tables must be centered in the column. Large figures and tables may span across both columns. Any table or figure that takes up more than 1 column width must be positioned either at the top or at the bottom of the page.

Graphics may be full color. All colors will be retained on the CDROM. Graphics must not use stipple fill patterns because they may not be reproduced properly. Please use only *SOLID FILL* colors which contrast well both on screen and on a black-and-white hardcopy, as shown in Fig. 1.

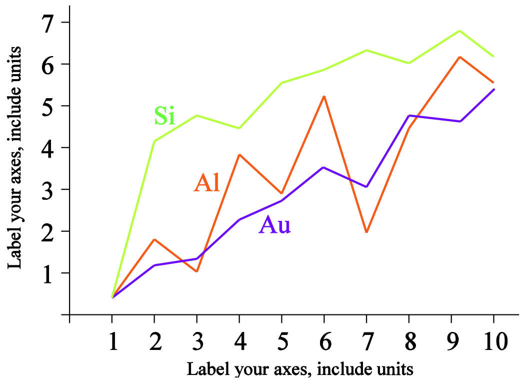


Fig. 1 A sample line graph using colors which contrast well both on screen and on a black-and-white hardcopy

Fig. 2 shows an example of a low-resolution image which would not be acceptable, whereas Fig. 3 shows an example of an image with adequate resolution. Check that the resolution is adequate to reveal the important detail in the figure.

Please check all figures in your paper both on screen and on a black-and-white hardcopy. When you check your paper on a black-and-white hardcopy, please ensure that:

- the colors used in each figure contrast well,
- the image used in each figure is clear,
- all text labels in each figure are legible.

I. Figure Captions

Figures must be numbered using Arabic numerals. Figure captions must be in 8 pt Regular font. Captions of a single line (e.g. Fig. 2) must be centered whereas multi-line captions must be justified (e.g. Fig. 1). Captions with figure numbers must be placed after their associated figures, as shown in Fig. 1.

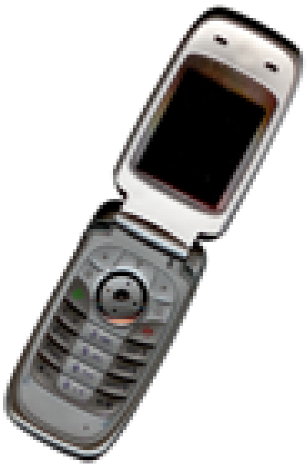


Fig. 2 Example of an unacceptable low-resolution image

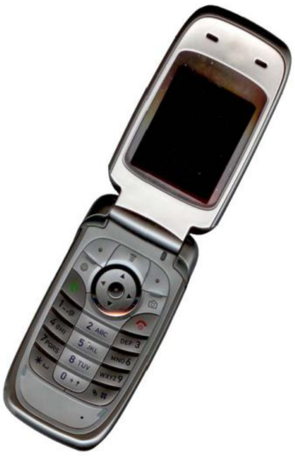


Fig. 3 Example of an image with acceptable resolution

J. Table Captions

Tables must be numbered using uppercase Roman numerals. Table captions must be centred and in 8 pt Regular font with Small Caps. Every word in a table caption must be capitalized except for short minor words as listed in Section III-B. Captions with table numbers must be placed before their associated tables, as shown in Table 1.

K. Page Numbers, Headers and Footers

Page numbers, headers and footers must not be used.

L. Links and Bookmarks

All hypertext links and section bookmarks will be removed from papers during the processing of papers for publication. If you need to refer to an Internet email address or URL in your paper, you must type out the address or URL fully in Regular font.

M. References

The heading of the References section must not be numbered. All reference items must be in 8 pt font. Please use Regular and Italic styles to distinguish different fields as shown in the References section. Number the reference items consecutively in square brackets (e.g. [1]).

When referring to a reference item, please simply use the reference number, as in [2]. Do not use “Ref. [3]” or “Reference [3]” except at the beginning of a sentence, e.g. “Reference [3] shows …”. Multiple references are each numbered with separate brackets (e.g. [2], [3], [4]–[6]).

Examples of reference items of different categories shown in the References section include:

- example of a book in [1]
- example of a book in a series in [2]
- example of a journal article in [3]
- example of a conference paper in [4]
- example of a patent in [5]
- example of a website in [6]
- example of a web page in [7]
- example of a databook as a manual in [8]
- example of a datasheet in [9]
- example of a master’s thesis in [10]
- example of a technical report in [11]
- example of a standard in [12]

IV. Conclusions

The version of this template is V2. Most of the formatting instructions in this document have been compiled by Causal Productions from the IEEE LaTeX style files. Causal Productions offers both A4 templates and US Letter templates for LaTeX and Microsoft Word. The LaTeX templates depend on the official IEEEtran.cls and IEEEtran.bst files, whereas the Microsoft Word templates are self-contained. Causal Productions has used its best efforts to ensure that the templates have the same appearance.

Causal Productions permits the distribution and revision of these templates on the condition that Causal Productions is credited in the revised template as follows: “original version of this template was provided by courtesy of Causal Productions (www.causalproductions.com)”.

Acknowledgment

The heading of the Acknowledgment section and the References section must not be numbered.

Causal Productions wishes to acknowledge Michael Shell and other contributors for developing and maintaining the IEEE LaTeX style files which have been used in the preparation of this template. To see the list of contributors, please refer to the top of file IEEETran.cls in the IEEE LaTeX distribution.

References

[8] S. M. Metev and V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

[9] J. Breckling, Ed., *The Analysis of Directional Time Series: Applications to Wind Speed and Direction*, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.

[10] S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," *IEEE Electron Device Lett.*, vol. 20, pp. 569–571, Nov. 1999.

[11] M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in *Proc. ECOC'00*, 2000, paper 11.3.4, p. 109.

[12] R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, "High-speed digital-to-RF converter," U.S. Patent 5 668 842, Sept. 16, 1997.

[13] (2002) The IEEE website. [Online]. Available: http://www.ieee.org/

[14] M. Shell. (2002) IEEEtran homepage on CTAN. [Online]. Available: http://www.ctan.org/tex-archive/macros/latex/contrib/supported/IEEEtran/

[15] *FLEXChip Signal Processor (MC68175/D)*, Motorola, 1996.

[16] "PDCA12-70 data sheet," Opto Speed SA, Mezzovico, Switzerland.

[17] A. Karnik, "Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP," M. Eng. thesis, Indian Institute of Science, Bangalore, India, Jan. 1999.

[18] J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.

[19] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11, 1997.