Swammis: Sinhgads'wide Area Multiuser and Multitasking Intranet System (Educational ERP)

Mangesh Powar, Tejas Vichare, Rashmi Udeg,Yojana Namdas, Swati Joshi

Abstract—Ineducational system at different departments, all the administrative jobs are being carried out manually. It not only consumes a lot of time but also reduces output efficiency. For every single job, faculties need to manually approach colleagues, carry out sumptuous hand written documentation, attendances, leave applications etc. If such jobs are automated by an Intranet application and a common communication platform, by making use of different technologies such as remote installation, VOIP with video conferencing, PDF data extraction in LAN etc. This paper begins by explaining the background to education ERP systems and goes on to discuss specific systems and their capabilities. Enterprise Resource Planning (ERP) Systems are powerful software packages that enable educational system to integrate a variety of disparate functions.

Keywords- ERP, video conferencing, RTMFP, VOIP, PDFand data extraction.

I. INTRODUCTION

Today, ERP systems integrate internal and externalman-agement information across an entire organization, embracing, customer relationship management. ERP systems automate this activity with an integrated software application. The purpose of ERP is to facilitate the flow of informationbetween all functions inside the boundaries of the educational organization and manage the connections between internal modules. ERP systems can run on a variety of computer hardware and network configurations, typically employing a database as a repository for information.

The traditional educational system which is seen generally in most of the educational institutes, these days, makes for an excessive utilization of resources which can be avoided easily.The traditional system has been the same for generations and has not been changed or varied despite a massive change in the other fields of education. ERP makes way for reduced efforts, reduced time utilization for task completion and minimal usage of resources.On similar ideology, ERP systems can also be brought onto educational domain. A highly efficient system for any educational institute considerably reduces the efforts and tedious nature of work structure of the members and faculties.

Another advantage of using ERP in educational institutes isthe reduced efforts of everyone related to the institute which would include the Head of Department to start with, Staff Members and also the Students.

Manuscript received April. 2013.

Mangesh Powar, Department of Computer Engineering, Sinhgad College of Engineering, University of Pune, India.

Tejas Vichare, Department of Computer Engineering, Sinhgad College of Engineering, University of Pune, India.

Rashmi Udeg, Department of Computer Engineering, Sinhgad College of Engineering, University of Pune, India.

Yojana Namdas, Department of Computer Engineering, Sinhgad College of Engineering, University of Pune, India.

Swati Joshi, (ME. ELEX-COMP), Department of Computer Engineering, Sinhgad College of Engineering, University of Pune, India.

Ease of keeping up with performances/detailed records of fellow colleagues/subordinates are also an added advantage over traditional institutes. Broadly, the system can be utilized in the following manner, keeping in mind the end user's perspective:

Head of Department:
HOD can use the system for performing various Management functions including task, event, and Calendar management.

Faculties:
Faculties can use the system for informationsharing such as the discussion board, issuealerts/notices and interactive contact methods.
Communication module for handling Videoconferencing, PC to PC voice calls, mobile and SMSgateway integration etc. Day-wise, real timeattendance collection via mobile.

For Students:
Students can also use this system for tasks such as Project group management, academic notifications, data sharing, news and alerts etc.

II. FUNCTIONAL REQUIREMENTS

The system when deployed onto an educational institute would automate its various processes. Primary functional requirements of the system include:

1. Allocation and Management of the available resources.
2. Correct utilization of the scarce resources.
3. Executing escape strategy to deal with unavailable resources.
4. Centralized administration for easy monitoring and executing higher order functions.

An architectural overview of the proposed system is mentioned in Figure 1.

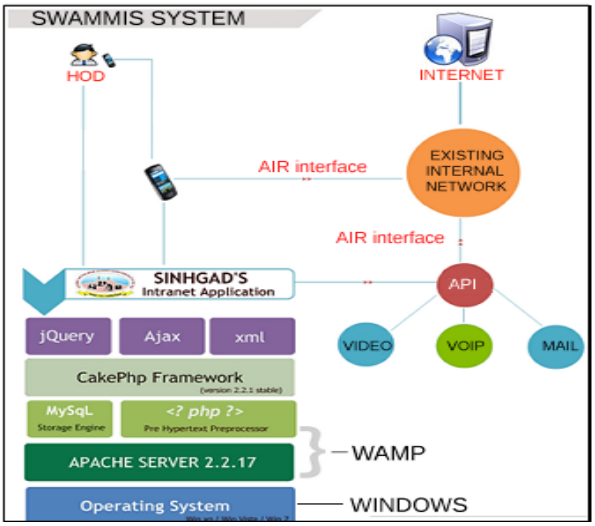

Figure 1. Architectural Structure of Proposed ERP

III. LIST OF MODULES AND RELATED PROTOCOLS

The basic modules of this project are listed below:

1. Communication Module
2. Management Module
3. Project Management Module
4. Examination Module
5. Attendance Module

For the implementation of all this modules different technologies are has been discussed in this paper.
Such as:

1. Communication Module:

VoIP calls over network, video conferencing comes under this module.For Communication Module, RTMP(Real Time Media flow Protocol) – a proprietary protocol of ADOBE systems [1]will be used to develop video conferencing and calling.

2. Management Module:

This module includes all the Management functions in the system developed [1]. This would include:

2.1 Student Management:

In Student Management every student will have a separate unique identification. With this unique identification the student can log onto the system and check for all his data. Detailed listing of all the students is maintained here. Students are distinguished by their year, batch or other details. Provision for search/add/update/delete student is provided.

2.1 Staff Management:

In Staff Management every staff member will have a separate unique identification. With this identification the staff member can log on to the system and perform required functions. Internal communication between the staff members would be provided via internal email/sms/chat. Similar provision for adding/deleting/updating staff is available.

2.2 Attendance Management:

Subject wise detailed attendance of every student would be maintained daily/ weekly/monthly. Provision for SMS based attendance would also be provided.

2.3 Task Management:

This module assigns task for staff and generates respective alerts for staff and students. It also does the functionality of creating and deleting poll.

3. Project Management Module:

This module will take care of efficient management and execution of Project committees as well as project group formations among students, project acceptance/rejections, domain allocations and its associated functions. A project committee manager will be the prime administrator of this module.

4. Examination Module:

It's concerned with conduction of various examinations in the institute, student marks management, reports generation etc. An Exam coordinator will be the highest priority user for this module.

5. Attendance Module:

Allow faculty to carry out attendance procedure from mobile, maintain dailyattendance for each student,attendance calculations, Android Interface, Simple phone interface, access point setup in department to check attendance of anystudent and automatic reports generation.

IV. RESEARCHED MODULES

Part I: PDF Data Extraction in LAN& Results

Restrictedaccess/subscription to IEEEconference papers in many engineering institutions is primarily becoming the main concern amongst most of the educational institutes across the country. There is lack of central repository which can act as a whole and sole provider of the required papers. Even though there is limited access, considerable number of papers isdownloaded; the lack of provision of saving these downloaded papers or not maintaining their backup can give rise to inconvenience. If all the downloaded papers are saved or maintained in a repository, it would help other students searching for the similar material. Major problem with current system is that no search string operations can be performed on multiple PDF files and every time,
PDF data extraction conversion enables us to find a specific string, be it author name, abstract or any other data from thousands of papers and help in saving this textual data which is much smaller in size. Each page in a PDF file is defined by a content stream(s) containing a series of commands. These commands change the current color, draw filled polygons, change the current font, draw text, and so on. Text can be (and usually is) broken into small chunks for purposes of kerning. To display "Text can be...", a PDF file might draw "T", then move back a little to the left, then draw "ext can be...". A PDF text extractor must reassemble this into the proper sequence of characters.[9]
xPDF open source library released by Glyph and Cogwhich runs on just about any platform that has a C++ compiler can be used in this context for reading and parsing PDF files. It uses Windows DLL libraries and runs on a single host machine. The idea is to make this library run in a network and make mass data extraction from PDF possible. This can be used to allow users to upload the PDF IEEE papers to a central server where the xPDF library will be running on every single PDF file that is uploaded in a specific directory. All the uploaded papers will reside into this directory which will be continuously checked by our application for new unprocessed files at the frequency of one minute.[9]
The "**shell_exec()**" function of PHP allows execution of .exe files from the PHP code to the shell layer. The output of converted file is stored into a text file which is further read by our application and its related textual data is stored in the database.Paper Search operations on the basis of Author name, ISBN Number, publication date, conference name etc will be handled by our application.
Tthe architectural working of the data extraction concept in LAN is shown in Figure 2.

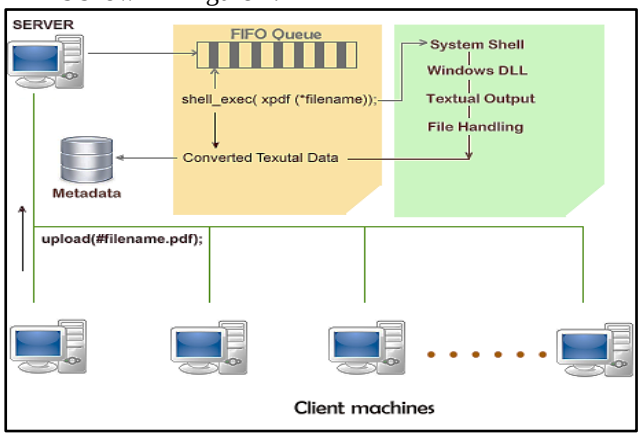

Figure2PDF Data Extraction in LAN

V. PRACTICAL EXPERIMENTAL RESULTS

PDF data extraction process is carried out in a one-file-at-a-time fashion by the xPDF plugin and hence different size file testing was performed to calculate expected time of execution and data generation.

Table 1: Results of PDF to text conversion locally

File Size	After Conversion	Processing Time
27,492,352 bytes	1,994,752 bytes	00:00:06:52
13,256,000 bytes	9,42,321 bytes	00:00:03:25

Part II:Video Conferencing and VoIP

The need for inclusion of VoIP and Video conferencing in educational ERP is to allow the stakeholders of institute to communicate vocally via their service desktops in real time (or close to real time). Voice over IP (VOIP) uses the InternetProtocol (IP) [1][2][3][8] to transmit voice as packets over an IP network.So VOIP can be achieved on any datanetwork that uses IP, like Internet, Intranets andLocal Area Networks (LAN). Here the voice signalis digitized, compressed and converted to IPpackets and then transmitted over the IP network.

VI. RTMFP (REAL TIME MEDIA FLOW PROTOCOL)

VoIP is a traditional method to initiate Voice communications using IP Packets. For the purpose of adding an enhanced security to the streaming packets, a newly launched RTMFP protocol can be adequately channelized with VoIP packets. The Secure Real-Time Media Flow Protocol (RTMFP) is a proprietary protocol suite developed by Adobe Systems for encrypted, efficient multimedia delivery through both client-server and peer-to-peer models over the Internet.[1][4][6] By using RTMFP, applications that rely on live, real-time communications will be able to deliver higher quality communication solutions. RTMFP enables end-users to connect and communicate directly with each other using their computer's microphone and webcam. This solution enhances the current functionality in the Flash Player by creating a higher quality solution that will perform better regardless of variations in the network. RTMFP is a peer-to-peer system, but is only designed for direct end user to end user communication for real-time communication, not for file sharing between multiple peers using segmented downloading.[5][6]

RTMFP can be used for developing real-time collaboration applications, Codename Cirrus (previously codename Stratus) enables peer assisted networking using the Real Time Media Flow Protocol (RTMFP) within the Adobe Flash® Platform.[8] RTMFP is the evolution of media delivery and real time communication over the Internet enabling peers on the network to assist in delivery. Cirrus was first introduced in 2008 as a rendezvous-only service that allowed clients to send data from client to client without passing through a server. Adobe Flash Player 10, which debuted peer assisted networking, has been adopted today by over 90% of all internet connected PCs.

Adobe has made various changes in the RTMFP protocol over the period of time and the mechanism of streaming in Unicast model and Multicast model as shown in Figure 3.

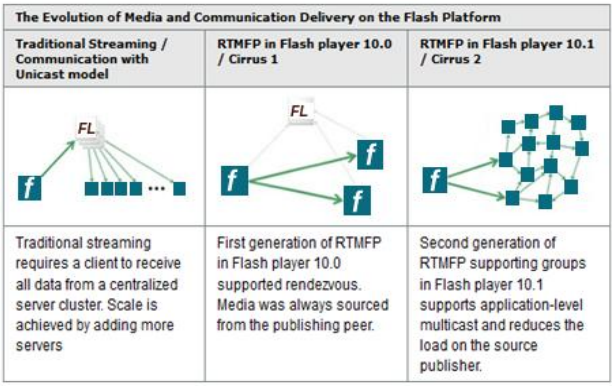

Figure3 Flash Data Streaming Platform Comparison

Parameters in RTMFPImplementation Session

An RTMFP session is an end-to-end bi-directional pipe between two UDP transport addresses. A transport address contains an IP address and port number, e.g., "192.1.2.3:1935". A session can have one or more flows where a flow is a logical path from one entity to another via zero or more intermediate entities. UDP packets containing encrypted RTMFP data are exchanged in a session. A packet contains one or more messages. A packet is always encrypted using AES with 128-bit keys.

In the protocol description below, all numbers are in network byte order (big-endian). The | operator indicates concatenation of data. The numbers are assumed to be unsigned unless mentioned explicitly[1].

Scrambled Session ID

The packet format is as follows. Each packet has the first 32 bits of scrambled session-id followed by encrypted part. The scrambled (instead of raw) session-id makes it difficult if not impossible to mangle packets by middle boxes such as NATs and layer-4 packet inspectors. The bit-wise XOR operator is used to scramble the first 32-bit number with subsequent two 32-bit numbers. The XOR operator makes it possible to easily unscramble.

packet := scrambled-session-id | encrypted-part

To scramble a session-id,

scrambled-session-id = a^b^c

where ^ is the bit-wise XOR operator, a is session-id, and b and c are two 32-bit numbers from the first 8 bytes of the encrypted-part.

To unscramble,

session-id = x^y^z

where z is the scrambled-session-id, and b and c are two 32-bit numbers from the first 8 bytes of the encrypted-part.

The session-id determines which session keys are used for encryption and decryption of the encrypted part. There is one exception for the fourth message in the handshake which contains the non-zero session-id but the handshake (symmetric) session keys are used for encryption/decryption. For the handshake messages, a symmetric AES (advanced encryption standard) with 128-bit (16 bytes) key of "Adobe Systems 02" (without quotes) is used. For subsequent in-session messages the established asymmetric session keys are used as described later.

Encryption

Assuming that the AES keys are known, the encryption and decryption of the encrypted-part is done as follows.

For decryption, an initialization vector of all zeros (0's) is used for every decryption operation. For encryption, the raw-part is assumed to be padded as described later, and an initialization vector of all zeros (0's) is used for every encryption operation. The decryption operation does not add additional padding, and the byte-size of the encrypted-part and the raw-part must be same[1].

Checksum

The 16-bit checksum number is calculated as follows. The concatenation of network-layer-data and padding is treated as a sequence of 16-bit numbers. If the size in bytes is not an even number, i.e., not divisible by 2, then the last 16-bit number used in the checksum calculation has that last byte in the least-significant position (weird!). All the 16-bit numbers are added in to a 32-bit number. The first 16-bit and last 16-bit numbers are again added, and the resulting number's first 16 bits are added to itself. Only the least-significant 16 bit part of the resulting sum is used as the checksum [1].

Network Layer Data

The network-layer data contains flags, optional timestamp, optional timestamp echo and one or more chunks [1].

network-layer-data = flags | timestamp | timestamp-echo | chunks ...

TimeStamp

The timestamp is a 16-bit number that represents the time with 4 millisecond clock. The wall clock time can be used for generation of this timestamp value. For example if the current time in seconds is tm = 1319571285.9947701 then timestamp is calculated as follows:

int(time * 1000/4) & 0xffff = 46586

i.e., assuming 4-millisecond clock, calculate the clock units and use the least significant 16-bits.

The timestamp-echo is just the timestamp value that was received in the incoming request and is being echo'ed back. The timestamp and its echo allow the system to calculate the round-trip-time (RTT) and keep it up-to-date [1].

Message Flow

There are three types of session messages: session setup, control and flows. The session setup is part of the four-way handshake whereas control and flows are in-session messages. The session setup contains initiator hello, responder hello, initiator initial keying, responder initial keyingand responder hello cookie change and responder redirect.

The control messages are ping, ping reply, re-keying initiate, re-keying response, close, close acknowledge, forwarded initiator hello. The flow messages are user data, next user data, buffer probe, user data ACK (bitmap), user data ACK (ranges) and flow exception report.

A new session starts with an handshake of the session setup. Under normal client-server case, the message flow is as follows:

Table 2: Message Flow In Initial Handshaking

Initiator (client)	Target (server)
-----Initiator Hello---------->	
<-----Responder Hell------>	

The handshake messages for session-setup use the symmetric AES key "Adobe Systems 02" (without the quotes), whereas in-session messages use the established asymmetric AES keys. Intuitively, the session setup is sent over pre-established AES cryptosystem, and it creates new asymmetric AES cryptosystem for the new session. Note that a session-id is established for the new session during the initial keying process, hence the first three messages (initiator-hello, responder-hello and initiator-initial-keying) use session-id of 0, and the last responder-initial-keying uses the session-id sent by the initiator in the previous message[1].

Message Types

The 8-bit type values and their meaning are shown in Tab. 3.

Table 3: 8 Bit Values With Meaning.

Type	Meaning
\x30	Initiator hello
\x70	Responder hello
\x38	Initiator initial keying
\x78	Responder initial keying
\x0f	Forwarded initiator hello

Table 3: 8 Bit Values With Meaning.

\x71	Forwarded hello response
\x10	Normal user data
\x11	Next user data
\x0c	Session failed on client side
\x4c	Session died
\x01	Causes response
\x41	Reset times keep alive
	\x5e Negative ACK
\x51	Some ACK

RTMFP Connection and Security

Illustration of showing two clients that have connected to Flash Media Server and to each other via RTMFP is shown in Figure 4.

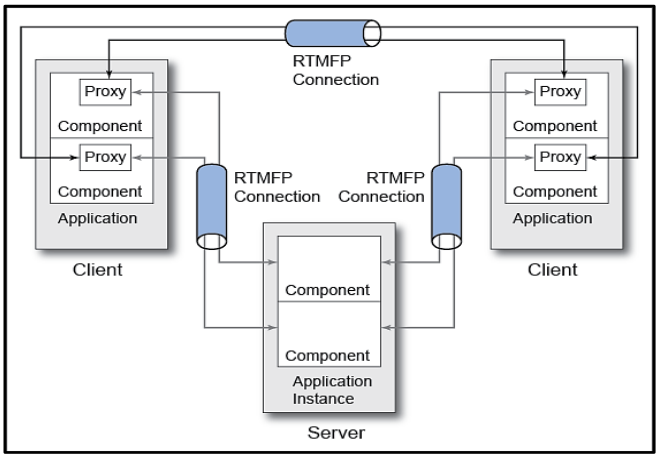

Figure 4.Clients Connected via RTMFP

Many clients may connect to the server but may not always pass information directly between each other. If the clients have formed P2P mesh information may be passed from client-to-client-to-client. In this sort of arrangement there may not be a server-side component at all or there may be cases where client-side components only communicate with server-side components.[5][6]

The illustration shows the case where client-side components communicate with both a server-side component and directly with each other via P2P. Hence we can conclude that RTMFP not only saves a lot of network bandwidth but also provides a considerable amount of application level security to the video stream.

VII. CONCLUSIONS AND FUTURE WORK

Therefore, we have presented a highly efficient architectural overview of an ERP that can be utilized by educational institutes. We have also discussed newly introduced RTMFP protocol and its technical details of how it can be implemented in practical application development which can be used to provide video streaming and content delivery to stakes holders of the educational institute or any profit based commercial organization.

The proposed educational ERP is still in its early stages. Current study focuses on the front end processes that are a vital part of any educational institute. The maintenance department that undertakes all types of setup and installation jobs is unable to monitor and manage remote software installations. Hence, for future scope of this project, a network based remote software deployment and management can be well considered as an add-on module.

VIII. ACKNOWLEDGMENTS

This Research Paper cannot be considered complete without mentioning Prof. P.R. Futane, Head of Department, Computer Engineering for their valuable support and co-operation.We wish to express true sense of gratitude towards their valuable contribution. We are grateful to them for their constant encouragement and guidance in the fulfillment of our project activity.

REFERENCES

[1] "Understanding RTMFP Handshake" byKundan Singh, [Online] Available at URLhttp://p2p-sip.blogspot.in/2011/12/understanding-rtmfp-handshake.html

[2] "RTCF – Real Time Component Framework" by Brian Lesser, [Online] Available at URLhttp://broadcast.oreilly.com/2011/08/real-time-component framework.html

[3] "Understanding Voice over Internet Protocol (VoIP)", Matthew Desantis, US-CERT

[4] "Voice Over Internet Protocol (VoIP)" , Invited Paper, Bur Goode, SENIOR MEMBER, IEEE

[5] "Application Middleware for convergence of IP Multimedia system and Web Services", Ivan Budiselic, Ivan Zuzak, Ivan Benc, MIPRO, 2010 Proceedings of the 33rd International Convention.

[6] "Dynamic code selection Algorithm for Voip" by Maja Sulovic, Mesud Hadzialic, Darijo Raca, Nasuf Hadziahmetovic, The Sixth International Conference on Digital Telecommunications, ICDT 2011

[7] "Application Middleware for convergence of IP Multimedia system and Web Services", Ivan Budiselic, Ivan Zuzak, Ivan Benc.

[8] Real Time Media Flow Protocol by Adobe Systems, [WWW] Available online at URLhttp://labs.adobe.com/technologies/cirrus

[9] "XPDF and Open Source" by Glyph and Cog, [WWW] Available online at URL http://www.glyphandcog.com/Xpdf.html