Electronic Research Project Proposal Management System using Spring and Hibernate Framework

Preetham[1], **Manimozhi**[2]

[1]MVJ College of Engineering Bangalore, India

[2] Assistant Professor at MVJ College of Engineering Bangalore, India

Abstract: ***Researchers and scientist need a platform (framework) to reproduce there work to world, so in proposed system we designed a framework which is developed using spring, Hibernate , designed using HTML5, CSS3 with RSA, Digital signature to make the framework secure . PostgreSQL database was used as back end. The existing system has overcome the time consuming process of research proposal submission, scrutiny, review, obtaining required reports and certificates, monitoring etc. Architecture is integrated with the two frameworks which is suitable for enterprise web application. The architecture hands business logic of Webwork to Spring; utilize beans configuration to manage the related classes; manage objects' relation of between controller and data access object through Spring and make data persistence by Hibernate, from RSA and Digital signature we avoid man middle attack, eavesdropping. The verification shows, this system can achieve the standardization and paperless Research proposals. We can still provide the high security with implementing SSL and Deploying the framework in cloud.***

Keywords: Framework, SSL, Digital signature, RSA, eavesdropping, Research.

1. Introduction

With the development of education, the reform can reflect The progress, which is not only in educational philosophy but in educational technique and means. However, as an important link in the teaching process, the examination I always the one of major parts of consuming human and material resource in this process. As researchers got great attention by web application project over the years, these applications are developed which are valuable in terms of transparency, accuracy, efficiency and security but web applications are becoming complex day by day. The open source application platform Spring and hibernate based on J2EE, provide integrated framework and uses layered structure. The ePPMS developed has almost achieved the paperless of Proposal Submission, Evaluation, Technical and financial approval, transparency and security. The major Layers involved in the system development are:

JSP (Java server pages) is a technology that helps software developers create dynamically generated web pages based on HTML, XML, or other document types. Released in 1999 by Sun Microsystems, JSP is similar to PHP and ASP, but it uses the Java programming language.

Below is the architecture of how JSP works:

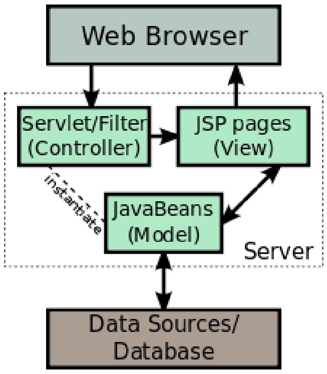


Figure 1: Java servlet pages.

HTML5 (Hypertext markup language) is a markup language used for structuring and presenting content on the World Wide Web. It is the fifth and current version of the HTML standard. The spring framework deals with the business logic. It is a Lightweight application development framework which uses MVC (Model-View-Controller) to separates business logic from the view and to separate the roles of handler objects and dispatcher, controllers and models objects, which makes them easier to be customized. Hibernate is a middleware providing database services, deal with the persistence layer which is helpful in reducing the difficulty of business logic. Hibernate is an Object/Relational Mapping (ORM) tool for Java Environment. ORM is used to map a java class with database tables and in data retrieval which can reduce development time

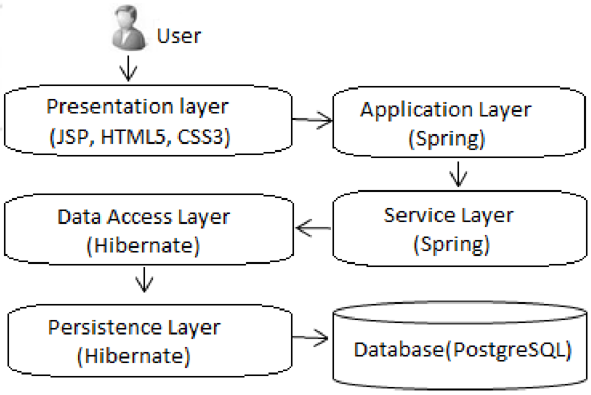

User
Presentation layer (JSP, HTML5, CSS3)
Application Layer (Spring)
Service Layer (Spring)
Data Access Layer (Hibernate)
Persistence Layer (Hibernate)
Database(PostgreSQL)

Figure 2: Layered approach

Comparing with the manual process of proposal submission the system has the various advantages like Flexibility in submission of proposal, easy, fast evaluation process and transparency in Proposal Processing, saves the physical space, email and SMS facility to know the status of proposal anytime, Maintain data integrity and security and provides role based access, responsive web design.

RSA:
RSA is one of the first practicable public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman.

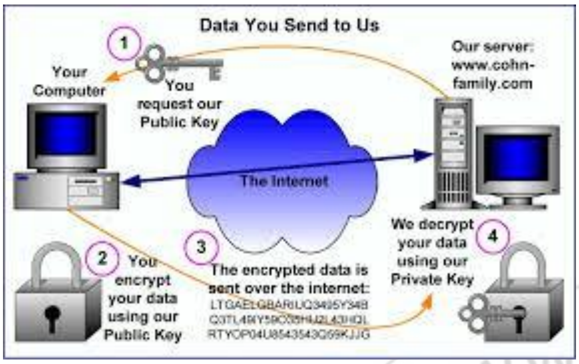

Data You Send to Us
1
Your Computer
You request our Public Key
Our server: www.cohn-family.com
The Internet
2
You encrypt your data using our Public Key
3
The encrypted data is sent over the internet:
LTGAELGBARILQ3495Y348
Q3TL49IY59CX5HIJ2L43HQL
RTYOP04U8543543G69KJJG
4
We decrypt your data using our Private Key

Figure 3: RSA

Digital Signature
DSA is a pair of large numbers that are computed according to the specified algorithm within parameters that enable the authentication of the signatory, and as a consequence, the integrity of the data attached. Digital signatures are generated through DSA, as well as verified. Signatures are generated in conjunction with the use of a private key; verification takes place in reference to a corresponding public key. Each signatory has their own paired public (assumed to be known to the general public) and private (known only to the user) keys. Because a signature can only be generated by an authorized person using their private key, the corresponding public key can be used by anyone to verify the signature.

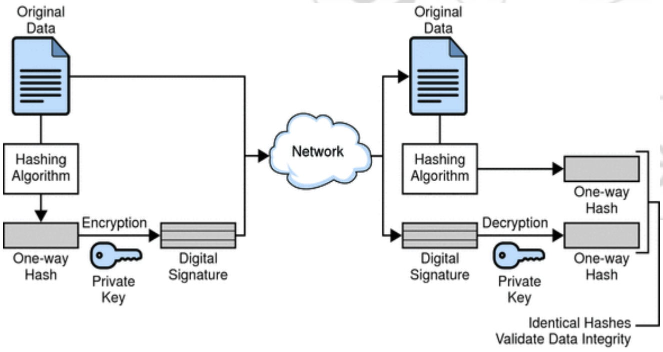


Figure 4: Digital Signature

The original data and the digital signature, which is basically a one-way hash (of the original data) that has been encrypted with the signer's private key. To validate the integrity of the data, the receiving software first uses the signer's public key to decrypt the hash. It then uses the same hashing algorithm that generated the original hash to generate a new one-way hash of the same data. (Information about the hashing algorithm used is sent with the digital signature, although this isn't shown in the figure.) Finally, the receiving software compares the new hash against the original hash. If the two hashes match, the data has not changed since it was signed. If they don't match, the data may have been tampered with since it was signed, or the signature may have been created with a private key that doesn't correspond to the public key presented by the signer.

Section II of this paper the existing system. Section III discusses the proposed system, Section IV discusses the conclusion and future enhancement.

2. Existing System

Manual Research proposal Submission:
The manual submission of research paper has following drawbacks.

- Time consumption for submitting a proposal reviewing a proposal report status, communication certificate
- No flexibility nor extendibility
- Unproven Security Model

Overcomes the time consuming process of research proposal submission, review, obtaining required reports, and certificates

Flexibility in submission of proposal, easy, fast evaluation process Transparency in proposal processing, saves the physical space, email facility to know the status of the proposal anytime. Maintain data integrity and security and provides role based access, responsive web design

3. Proposed System

3.1 Work mechanism of spring framework

Place the 7 basic modules of spring are AOP, ORM, DAO, Web MVC, Context package, Core package and Web package. Core packages provide Inversion of Control and dependency injection. The lengthy JDBC code is eliminated by JDBC abstraction layer provided by Data access object. Object relation mapping and Aspect oriented programming is provided by ORM and AOP packages respectively. A web application implementation is provided by MVC package.

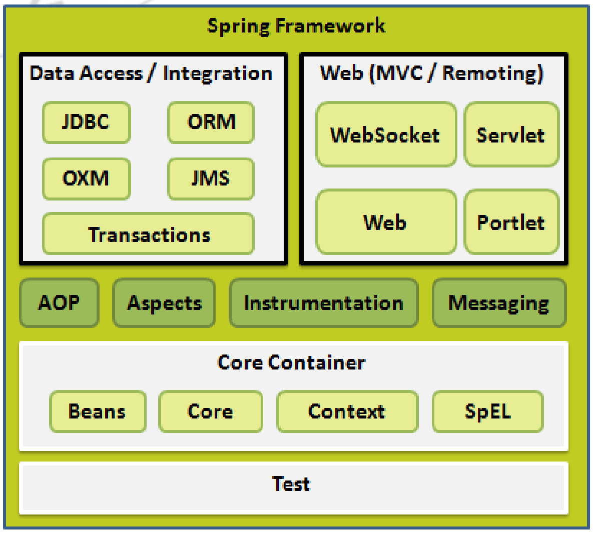


Figure 6: Basic modules of spring

The complete process is shown in figure II. The incoming request from the JSP is dispatched to handler which calls the appropriate controller. The dispatcher Servlet is declared in web.xml file as:

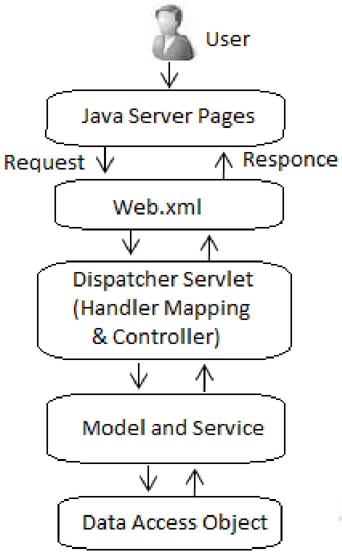


Figure 7: Work mechanism of spring

The Controller process the request using model class, service class and data access object, and returns the view name to dispatcher servlet which return the view back to user.

3.2 Work mechanism of hibernate

Hibernate separates business logic and data access by object relation mapping [1]. It uses object relation files and used as persistence layer which mainly consists of configuration files, persistence objects and mapping files as shown in figure III, the configuration files deals with the database connection information and mapping files provides mapping relationship between objects and database tables.

The session interface creates and destroys a session object [1]. Session buffers Hibernate automatically generated SQL statements and data to be reused in future. Hibernate uses Hibernate query language for query processing.

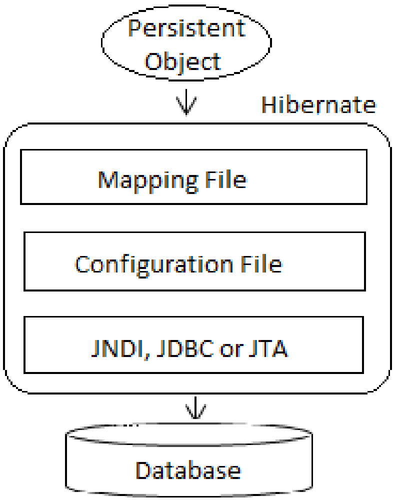


Figure 8: Work mechanism of Hibernate

3.3 System Architecture

In Architecture we have 5 roles principal investigator, member secretry ,Special invite ,programm advisory comitee and director. The job of principal investigator is the one who propose new papers.

Member secretery is the one who manages proposals, Referee evaluates the proposals ,Advisory comitte calls the person for meeting and decedes to accept the proposal or not and finally the director approves the financial formalities.

IMember secretery is the one who will manage the proposals

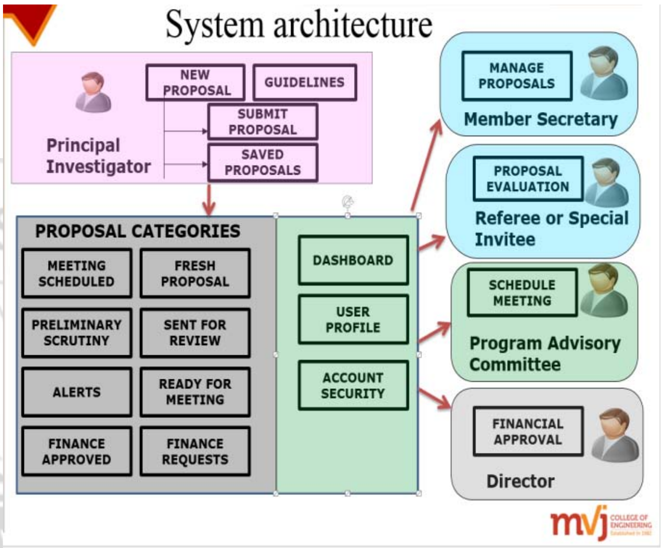


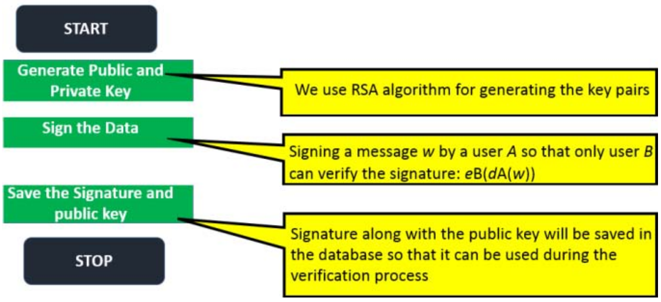
Figure 9: System Architecture

3.4 RSA and Digital Signature

To make the framework secure we have the RSA and Digital signature.

RSA works on presentation layer with asymmetric encryption, the admin will encrypt the data with a public key and the user can decrypt the data with private key.
Digital Signature works on two phases:

Generation of signature:


START
Generate Public and Private Key
Sign the Data
Save the Signature and public key
STOP

We use RSA algorithm for generating the key pairs

Signing a message *w* by a user *A* so that only user *B* can verify the signature: *eB*(*dA*(*w*))

Signature along with the public key will be saved in the database so that it can be used during the verification process

Figure 10: Signature generation

We use RSA algorithm with assymetric encryption for generating private key (key pairs are randomly generates by RSA), the Digital signature authority will sign the packet with a message, the message with public key will be saved in the database so that this can be used in verification purpose later.

Verifiying Signature

Public key used here will be mathematically related to the private key used in the signature generation algorithm.This verfying step is done while publishing paper to the principal

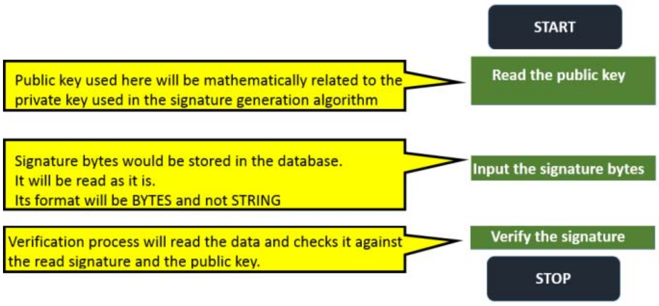

START
Read the public key
Public key used here will be mathematically related to the private key used in the signature generation algorithm
Input the signature bytes
Signature bytes would be stored in the database.
It will be read as it is.
Its format will be BYTES and not STRING
Verify the signature
Verification process will read the data and checks it against the read signature and the public key.
STOP

Figure 11: Signature verification

- Signature bytes would be stored in the database. It will be read as it is. Its format will be BYTES and not STRING
- Verification process will read the data and checks it against the read signature and the public key

4. System Implementation

Manual submission of proposal was a burden for researchers and coordinating personnel for obtaining the project proposals, scrutiny, send to Reviewers, obtaining progress reports and certificates, etc. Automation has speed up these activities

4.1 Registration of Roles

The director is the one who decides the roles and responsibilities of principal investigator, member secretary and program advisory committee.

4.2 Submission of research paper

Principal investigator logs in to website with his username and password. He adds his new ideas and submits the paper.

4.3 Evaluation paper

Special invite will review's the paper based on his knowledge and decides to approve or reject.

4.4 Schedule meeting

Program advisory committee verifies following points

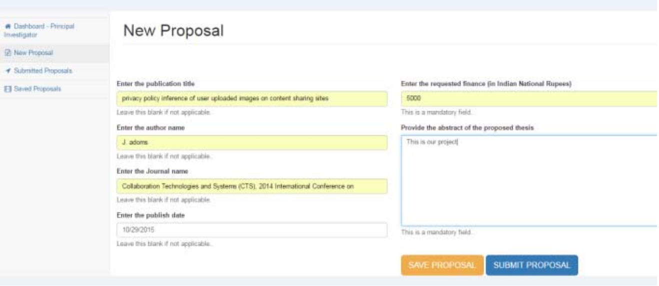
- No of proposals.
- Are proposals reviewed??
- Rejected or accepted??

If the proposals are accepted advisory committee calls the principal investigator for meeting.

4.5 Financial Approval

Finally director meets the principal investigator and completes the financial formalities.

5. Results



New Proposal

Enter the publication title
privacy policy inference of user uploaded images on content sharing sites
Leave this blank if not applicable.

Enter the author name
J. adoms
Leave this blank if not applicable.

Enter the Journal name
Collaboration Technologies and Systems (CTS), 2014 International Conference on
Leave this blank if not applicable.

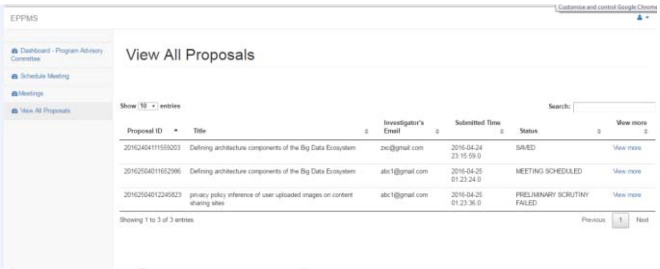
Enter the publish date
10/29/2015
Leave this blank if not applicable.

Enter the requested finance (in Indian National Rupees)
5000
This is a mandatory field.

Provide the abstract of the proposed thesis
This is our project
This is a mandatory field.

Figure 11: New proposals

Above figure shows addition new proposal by principal investigator.


EPPMS
Customise and control Google Chrome
Dashboard - Program Advisory Committee
Schedule Meeting
Meetings
View All Proposals
Previous
1
Next

View All Proposals

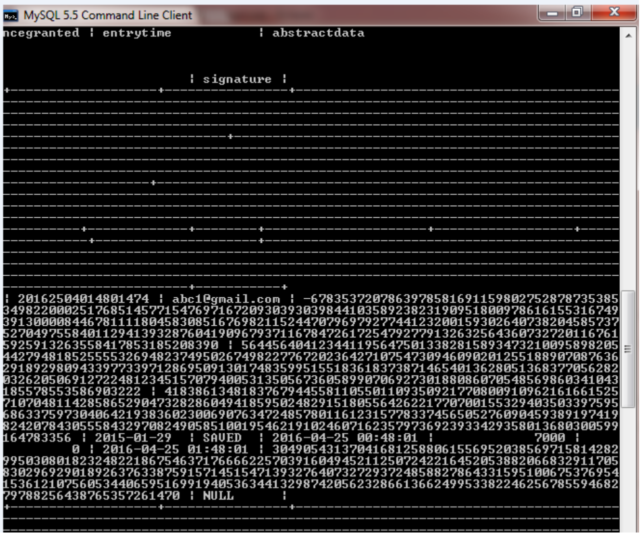
Show 10 entries Search:

Proposal ID	Title	Investigator's Email	Submitted Time	Status	View more
20162404111559203	Defining architecture components of the Big Data Ecosystem	zxc@gmail.com	2016-04-24 23:15:59.0	SAVED	View more
20162504011652986	Defining architecture components of the Big Data Ecosystem	abc1@gmail.com	2016-04-25 01:23:24.0	MEETING SCHEDULED	View more
20162504012245823	privacy policy inference of user uploaded images on content sharing sites	abc1@gmail.com	2016-04-25 01:23:36.0	PRELIMINARY SCRUTINY FAILED	View more

Showing 1 to 3 of 3 entries

Figure 12: Show proposals

Above figure shows the no of proposals.



```
ncegranted ¦ entrytime            ¦ abstractdata



                        ¦ signature ¦
+-------------------+----------------+------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
-----------------------------+--------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
-------------------+------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
----------+-------------+--------+---------------------+------------------+-----
-----------+---------------------+----------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
------------------------+-----------+-------------------------------------------
¦ 20162504014801474 ¦ abc1@gmail.com ¦ -6783537207863978581691159802752878735385
34982200025176851457715476971672093039303984410358923823190951800978616155316749
39130000844678111180458308516769821152447079697927744123200159302640738204585737
52704975584011294139328760419096793711678472617254792779132632564360732720116761
5925913263558417853185208390 ¦ 5644564041234411956475013382815893473210095898205
44279481852555532694823749502674982277672023642710754730946090201255188907087636
29189298094339773397128695091301748359951551836183738714654013628051368377056282
03262050691272224812345157079400531350567360589907069273018808607054856986034104 3
185578553586903222 ¦ 41838613481837679445581105501109350921770800910962161661525
71070481142858652904732828604941859502482915180556426221770700155329403503397595
68633759730406421938360230069076347248578011612315778337456505276090459389197419
82420784305558432970824905851001954621910246071623579736923933429358013680300599
164783356 ¦ 2015-01-29  ¦ SAVED  ¦ 2016-04-25 00:48:01 ¦               7000 ¦
        0 ¦ 2016-04-25 01:48:01 ¦ 304905431370416812588061556952038569715814282
99503080182324822186754637176666225703916049452112507242216452053882066832911705
83029692901892637633875915714515471393276407327293724858827864331595100675376954
15361210756053440659516991940536344132987420562328661366249953382246256785594682
79788256438765357261470 ¦ NULL      ¦
+-------------------+----------------+------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
```

Figure 13: Digital signature

6. Conclusion and future enhancement:

This paper is for Sciences and Engineering Research Board India. The system is highly reliable till now. Spring and Hibernate architecture is an effective lightweight J2EE application solution. RSA and digital signature gives the security to which was missing in any journals. In future we can provide more security with SSL.

7. Acknowledgement

Guledal preetham, thanks to Mrs. Manimozhi I, who is always encouraging and motivating me to do research

activities. I am also very thankful my families and friends

References

[1] Zhang Shengwen,Wang Xiangbing“An E-commerce System Structure Research Based on WSH(Webwork, Spring, Hibernate)”, II International Conference on Computer Science and Network Technolog.IEEE.

[2] Jiaqiaojie, Li juanli, Wang yuanyuan “Design and Implementation of Remote OnlineExamination System Based on Integration Framework”,IEEE.

[3] Nisha Sharma, P N Barwal “Electronic Project Proposal Management System for Research Projects Based on Integrated Framework of spring and Hibernate, IJSCE.

[4] RenYongchang, “Application Research for Integrated SSH Combination Framework to Achieve MVC Mode”, IEEE.

[5] Dawei LIU, “Design and Implementation of Highquality Course Scoring SystemBased on Struts and Spring and Hibernate Architecture”, International Conference of Information Technology, IEEE 2011.