IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Crime Investigation using Advanced Cybernetic Protectors

[1]Dr. Abhay Shukla, [2]Mohd Ahmad, [3]Shweta Gond, [4]Shreya Tiwari

[1]Associate Professor, [2-4]Student

[1-4]Compter Science and Engineering Department,

[1-4]Axis Institute of Technology and Management, Kanpur, India

Abstract: The main objective of Cybernetic Protectors is to provide a secure way of communication and transferring evidences in Secret Intelligence Agency of defence system which has always uses undercover agents to solve complex cases and dismantle criminal organizations.

We are conceptualizing this software as a solution so that Secret Intelligence Agencies and their agents can communicate through this Software for the exchange of evidences in a secure way. And maintain the details of the Defence Minister.

Index Terms **- Secret intelligence agency (SIA), Security.**

I. INTRODUCTION

1.1Existing System

- This existing system is not providing secure registration and profile management of all the users properly.
- This manual system gives us very less security for saving data and some data may be lost due to mismanagement.
- The system is giving only less memory usage for the users.
- The system doesn't provide facility to track all the activities of Agency-Chief and under working Agents.
- The system doesn't provide any facility to maintain any tips & suggestion for Citizen.
- The system doesn't provide any functionality to upload evidences in encrypted format.
- This system doesn't provide recruitment of agents through online.
- The system doesn't provide any functionality to Defence Minister/Secrete Agency-Chief/Agents for online chatting.

1.2 Proposed System

The development of this new system contains the following activities, which try to automate the entire process keeping in the view of database integration approach.

- This system maintains user's personal, address, and contact details.
- User friendliness is provided in the application with various controls provided by system rich user interface.
- This system makes the overall project management much easier and flexible.
- Various classes have been used for maintain the details of all the users and catalog.
- Authentication is provided for this application only registered users can access.
- Report generation features is provided using to generate different kind of reports.
- The system provides facilities to track the all activities of Agency-Chief and Agents.
- System also tracks the tips and suggestion online.
- System provides facility to recruit Agents in online.

- System also provides facility to upload evidences in encrypted format and view cases, related resources.
- This system is providing more memory for the users to maintain data.
- This system is providing accessibility control to data with respect to users.
- This system provides citizens to view success Stories.
- This system provides the functionality to Defence Minister/Secrete Agency-Chief/Agents for online chatting.

II. PROPOSED ALGORITHM OF PROJECT

2.1 RSA Algorithm

The RSA algorithm was publicly described in 1977 by Ron Rivest, Adi Shamir, and Leonard AdlemanThe RSA algorithm involves three steps:

2.1.1 Key generation-

RSA involves a **public key** and a private key**.** The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q.
   - For security purposes, the integers p and q should be chosen at random, and should be of similar bit-length.
2. Compute $n = pq$.
   - n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
3. Compute $\varphi(n) = (p-1)(q-1)$, where φ is Euler's totient function.
4. Choose an integer e such that $1 < e < \varphi(n)$ and greatest common divisor $\gcd(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are coprime.
   - e is released as the public key exponent.
   - e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $2^{16} + 1 = 65{,}537$. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.
5. Determine d as $d \equiv e^{-1} \pmod{\varphi(n)}$, i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$).
   - This is more clearly stated as solve for d given $de \equiv 1 \pmod{\varphi(n)}$
   - This is often computed using the extended Euclidean algorithm.
   - d is kept as the private key exponent.

By construction, $d \cdot e \equiv 1 \pmod{\varphi(n)}$.

The **public key** consists of the modulus n and the public (or encryption) exponent e. The **private key** consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and $\varphi(n)$ must also be kept secret because they can be used to calculate d.

- An alternative, used by PKCS#1, is to choose d matching $de \equiv 1 \pmod{\lambda}$ with $\lambda = \operatorname{lcm}(p-1, q-1)$, where lcm is the least common multiple. Using λ instead of $\varphi(n)$ allows more choices for d. λ can also be defined using the Carmichael function, $\lambda(n)$.
- The ANSI X9.31 standard prescribes, IEEE 1363 describes, and PKCS#1 allows, that p and q match additional requirements: being strong primes, and being different enough that Fermat factorization fails.

2.1.2 Encryption –

Alice transmits her public key (n, e) to Bob and keeps the private key secret. Bob then wishes to send message M to Alice.

He first turns M into an integer m, such that $0 \leq m < n$ by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext c corresponding to

$$c \equiv m^e \pmod{n}.$$

This can be done quickly using the method of exponentiation by squaring. Bob then transmits c to Alice.

2.1.3 Decryption –

Alice can recover *m* from *c* by using her private key exponent *d* via computing

$$m \equiv c^d \pmod{n}.$$

Given *m*, she can recover the original message *M* by reversing the padding scheme. (In practice, there are more efficient methods of calculating c^d using the precomputed values below.)

III. OVERVIEW OF THE PROPOSED PROJECT

3.1 Modules

3.1.1 Citizen:-

a. Ability to see Success Stories.
b. Ability to view for a job in Secret Intelligence Agency.
c. Ability to give tips & suggestion.

3.1.2 Under Agent:-

a. Able to view case details.
b. Should be able to encrypt & upload evidence or data to Data Base.
c. Able to view resources from ministry or chief.
d. Generate Report.

3.1.3 Defense Ministry:-

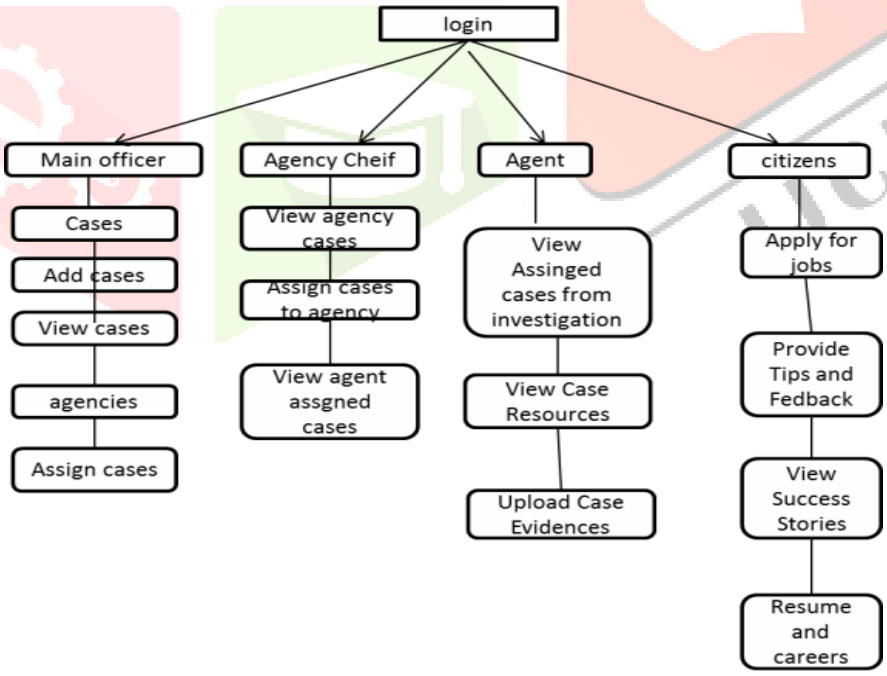
a. Should be able to send resources to Secret Agency.
b. Receive reports
c. Ability to assign cases to the Agency.

3.1.4 Secret Intelligence Agency's chief:-

a. Chief should be able to create/edit/view Agent's profile
b. Appointing of Agent to a particular case.
c. Secure retrieval of evidences received from Agent.
d. Access to Data Base logs.
e. Generate Reports
f. Ability to store data with history (archive cases).

3.1.5 Security and Authentication Module:-

The user details should be verified against the details in the user tables and if it is valid user, they should be entered into the system. Once entered, based on the user type access to the different modules to be enabled / disabled and individual user can change their default password or old password.



IV. SYSTEM REQUIREMENT

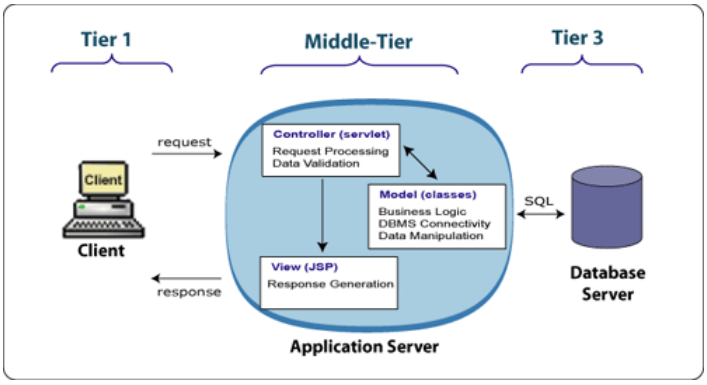
4.1 Software Requirements

Operating System	:	Windows XP/07 or Linux
User Interface	:	HTML, CSS
Client-side Scripting	:	JavaScript
Programming Language	:	Java
Web Applications	:	JDBC, Servlets, JSP
IDE/Workbench	:	My Eclipse 8.6
Database	:	Oracle 10g/11g
Server Deployment	:	Tomcat 6.x/7.x

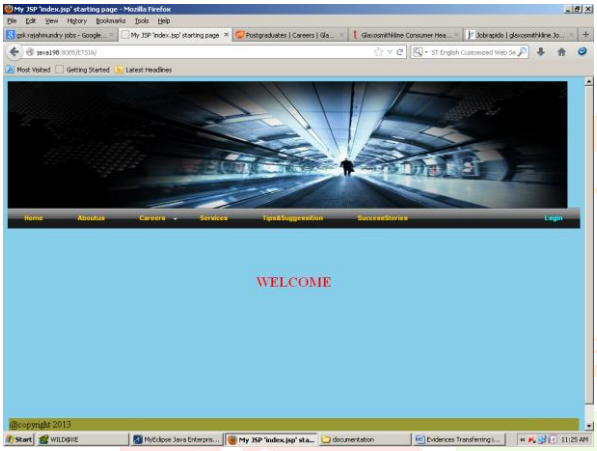
4.2 Hardware Requirements

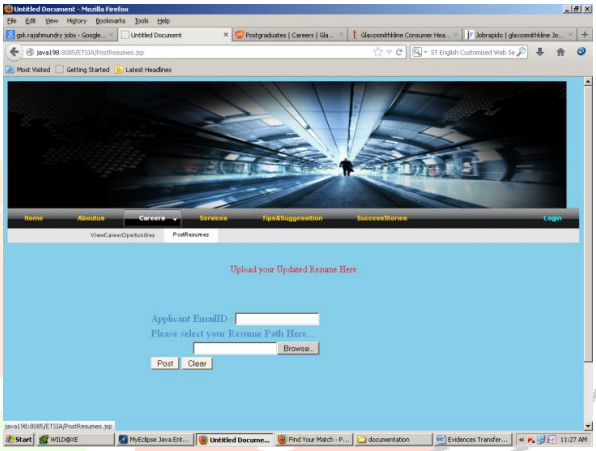
Processor	:	Core 2 duo
Hard Disk	:	160GB
RAM	:	1GB or more

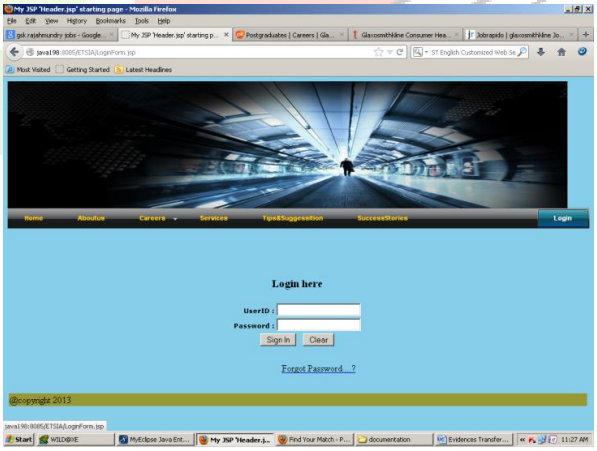
V. ARCHITECTURE DIAGRAM

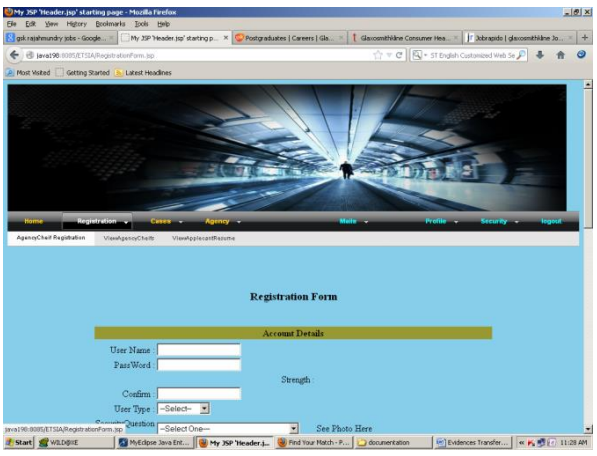


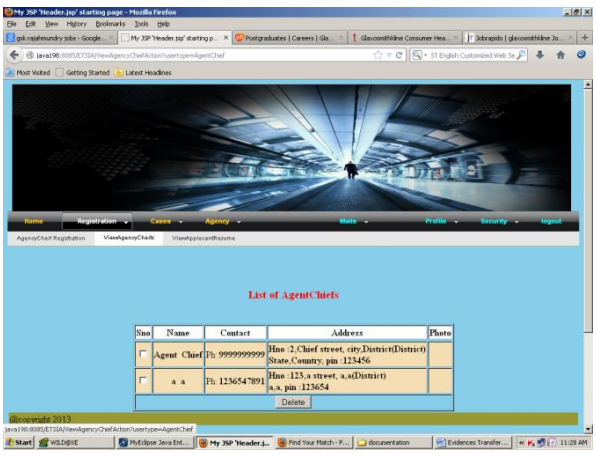
VI. RESULT DISCUSSION

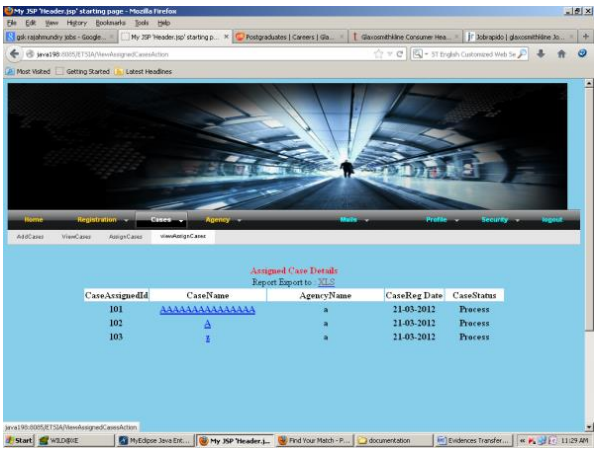




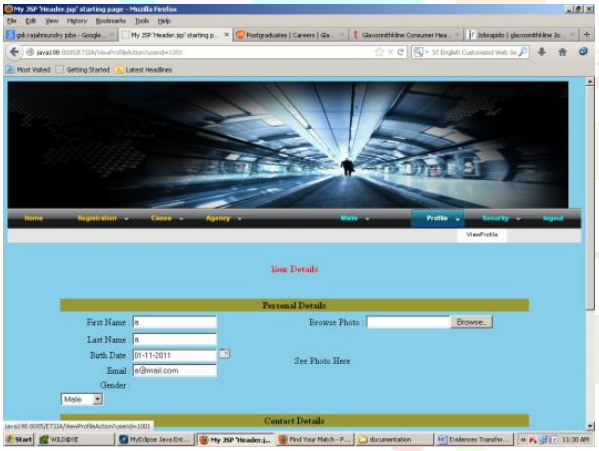
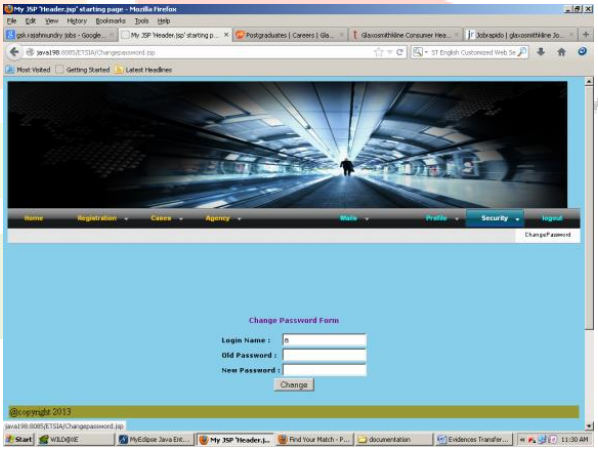










VII. CONCLUSION

It has been a great pleasure for us to work in this project. This Cybernetics Protector project is successfully designed for crime investigation and is tested for quality and accuracy. During this project we have accomplished all the objectives and this project meets the needs of the organization. This will provide better opportunities and guidance in future in developing projects independently. The developed will be used in searching, retrieving and generating information for the concerned requests.

REFERENCES

[1] www.codeproject.com.
[2] The Complete Reference “Crystal Reports 2008” by George peck.
[3] Training and placement website of IIT,Patna.
[4] Google, URL: http://www.google.co.in
[5] “Microsoft Visual Basic 2010” by Michael Halvorson.
[6] Tynjälä, P., Perspective into learning at the workplace, Educational Research Review, 3, 2008, pp.130-154.
[7] Answers.com, Online Dictionary, Encyclopedia and much more, URL: http://www.answers.com
[8] “The Complete Reference ASP.NET” book by Robert Standefer III.
[9] Project Management URL: http://www.startwright.com/project.html

AUTHOR'S PROFILE

Dr. Abhay Shukla is the Associate Professor, CSE Department, Axis Institute of Technology and Management. He is having 12 year of experience in teaching and 2 years of experience as Software Engineer. His area of interest includes DBMS, Operating System, Compiler Design, Artificial Intelligence, Natural Language Processing. He has supervised several B.Tech projects. He is associate member of NCSSS and Institute for Engineering Research and Publication. He has participated in various workshops, seminars and FDP. He published 13 research papers in various national and international journals.

Mohd Ahmad, Student of Computer Science and Engineering Department, Axis Institute of Technology and Management. He is final Year student and His areas of interest include Java.

Shweta Gond, Student of Computer Science and Engineering Department, Axis Institute of Technology and Management. She is final Year student and Her areas of interest include Machine Learning, Data Science and web development.

Shreya Tiwari, Student of Computer Science and Engineering Department, Axis Institute of Technology and Management. She is final Year student and Her areas of interest include Machine Learning, Data Science and web development.