Cybernetic Protectors

[1]Pasala Santhosh Kumar, [2]K Madhusudhan Reddy
[1]*Student, Master of Computer Applications, SKIIMS, Srikalahasti, Andhra Pradesh, India*
[2]*Asst.Professor, Master of Computer Applications, SKIIMS, Srikalahasti, Andhra Pradesh, 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 Defence Minister.

I. INTRODUCTION

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 Defiance Minister/Secrete Agency-Chief/Agents for online chatting.

II. 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 systemprovides citizens to view success Stories. This system provides the functionality to Deface Minister/Secrete Agency-Chief/Agents for online chatting.

III. FEASIBILITY REPORT

Technical Feasibility: Evaluating the technical feasibility is the trickiest part of a feasibility study. This is because, at this point in time, not too many detailed design of the system, making it difficult to access issues like performance, costs on (on account of the kind of technology to be deployed) etc. A number of issues have to be considered while doing a technical analysis.

Understand the different technologies involved in the proposed system:

Before commencing the project, we have to be very clear about what are the technologies that are to be required for the development of the new system.

Operational Feasibility: Proposed projects are beneficial only if they can be turned into information systems that will meet the organizations operating requirements. Simply stated, this test of feasibility asks if the system will work when it is developed and installed. Are there major barriers to Implementation?

Here are questions that will help test the operational feasibility of a project:

Is there sufficient support for the project from management from users? If the current system is well liked and used to the extent that persons will not be able to see reasons for change, there may be resistance.

Are the current business methods acceptable to the user? If they are not, Users may welcome a change that will bring about a more operational and useful systems.

Have the user been involved in the planning and development of the project?

Early involvement reduces the chances of resistance to the system and in

General and increases the likelihood of successful project.

Since the proposed system was to help reduce the hardships encountered. In the existing manual system, the new system was considered to be operational feasible.

IV. ALGORITHAM

RSA: The RSA algorithm was publicly described in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman

The RSA algorithm involves three steps: key generation, encryption and decryption.

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: 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.

1. 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.

2. Compute $\varphi(n) = (p - 1)(q - 1)$, where φ is Euler's totient function.
3. 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.[4]

4. 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.

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 $0 \le m < n$ 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.

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.)

Using the 1Chinese remainder algorithm
For efficiency many popular crypto libraries (like OpenSSL, Java and .NET) use the following optimization for decryption and signing based on the Chinese remainder theorem. The following values are precomputed and stored as part of the private key:

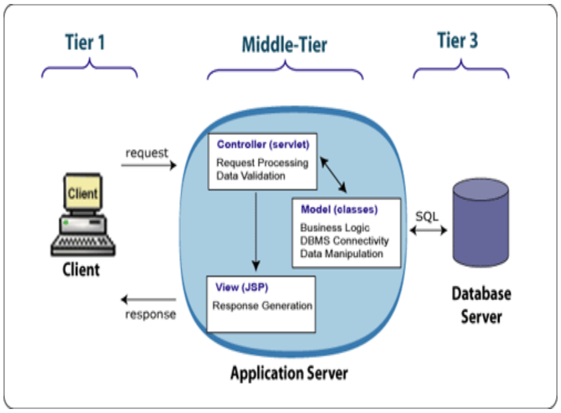
- p and q: the primes from the key generation,
- $d_P = d \pmod{p-1}$,
- $d_Q = d \pmod{q-1}$ and
- $q_{\text{inv}} = q^{-1} \pmod p$.

These values allow the recipient to compute the exponentiation $m = c^d \pmod{pq}$ more efficiently as follows:

- $m_1 = c^{d_P} \pmod p$
- $m_2 = c^{d_Q} \pmod q$
- $h = q_{\text{inv}} * (m_1 - m_2) \pmod p$ (if $m_1 < m_2$ then some libraries compute h as $q_{\text{inv}} \times (m_1 + p - m_2) \pmod p$)
- $m = m_2 + (h * q)$

This is more efficient than computing $m \equiv c^d \pmod{pq}$ even though two modular exponentiations have to be computed. The reason is that these two modular exponentiations both use a smaller exponent and a smaller modulus.

V. ARCHITECTURE



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

VI. FUTURE ENHANCEMENTS

It is not possible to develop a system that makes all the requirements of the user. User requirements keep changing as the system is being used. Some of the future enhancements that can be done to this system are:

- As the technology emerges, it is possible to upgrade the system and can be adaptable to desired environment.
- Because it is based on object-oriented design, any further changes can be easily adaptable.
- Based on the future security issues, security can be improved using emerging technologies.
- sub admin module can be added

VII. CONCLUSION

The Cybernetic Protectors was successfully designed and is tested for accuracy and quality.
During this project we have accomplished all the objectives and this project meets the needs of the organization. The developed will be used in searching, retrieving and generating information for the concerned requests.

GOALS

✓ Reduced entry work
✓ Easy retrieval of information
✓ Reduced errors due to human intervention
✓ User friendly screens to enter the data
✓ Portable and flexible for further enhancement
✓ Web enabled.
✓ Fast finding of information requested

REFERENCES

[1] Wikipedia,URL: http://www.wikipedia.org.

[2] Answers.com, Online Dictionary, Encyclopedia and much more, URL: http://www.answers.com

[3] Google, URL: http://www.google.co.in

[4] Project Management URL: http://www.startwright.com/project.htm