

Corporate Message Filtration & Security via 3-DES

Nischal Jakhar¹, Puranjai Mendiratta², Vinay Singh³, Utsav Chadha⁴, Varsha Sharma⁵

^{1,2,3,4}Department of Information Technology, Bhagwan Parshuram Institute of Technology, New Delhi, India

⁵Assistant Professor, Department of Information Technology, Bhagwan Parshuram Institute of Technology, New Delhi, India

Abstract - In today's corporate world loyalty has become a necessity. This can't be purchased but can be monitored. This system is developed to monitor the communication between different employees by the manager. This system filters the unwanted and inappropriate messages which are against the corporate policies and gives manager the power to take actions against the defaulters using a defaulter score matrix which is maintained for all the employees working in the organization. This application respects the privacy and the presence of sensitive data and hence uses a good encryption and decryption system which is 3-DES triple key version. This system prevents the flow of spam, sensitive data within the organization.

Key Words: 3-DES, Corporate, Message Filtration, Privacy, Security

1. INTRODUCTION

This system is going to help the corporates maintain a loyal environment within the organization. Since communication within the organization is the backbone of effective functioning of any corporate, preserving integrity and confidentiality of messages is paramount. Without a proper communication system, corporate world can't survive the battle. There is a need of a secure, safe, system that can facilitate the manager with the features that include monitoring the employee's communication. This system allows filtration of messages based on blocked words list. Any dubious content that is being sent will be blocked and the employee will be assigned defaulter points in the defaulter score matrix. Messages in the inbox are given priority rating. This system uses 3-DES encryption algorithm to enhance the security of communication.

1.1 3-DES TRIPLE KEY ALGORITHM

3-DES has two-key and three-key versions. In the two-key version, the same algorithm runs three times, but uses K1 for the first and last steps where K means key. In other words, $K1 = K3$. Note that if $K1 = K2 = K3$, then Triple DES is Single DES.

We use three-key version of Triple DES.

Triple DES operates in three steps: Encrypt-Decrypt-Encrypt (EDE).

It works by taking three 56-bit keys (K1, K2 and K3), and encrypting first with K1, decrypting next with K2 and encrypting a last time with K3.

Two-key Triple DES (which is no longer approved for encryption due to its susceptibility to brute force attacks) thus has 112 bits of strength (56 multiplied by two). Because of meet-in-the-middle attacks, Double DES is only one bit stronger than Single DES. So, we are using Three-key version.

Triple DES is stronger than 112 bits. It is somewhere between 113 and 167.

Due to its Feistel structure and uncomplicated logic, DES is relatively easy to implement. However, it uses eight distinct S-Boxes, which increases its footprint. DES is broken but 3DES is safe and cracking it would be very time consuming and tuff.

2. PROPOSED SYSTEM

"Corporate Message Filtration & Security via 3-DES" provides an effective way of communication which preserves integrity and confidentiality of the message. Messages containing suspicious contents will be blocked and can be viewed by the admin/manager. Triple-DES encryption technique is used to encrypt message contents for secure communication. An employee feed is provided similar to a discussion forum. Other basic functionalities related to messaging are provided.

2.1 Functions

- Monitoring and filtration of messages.
- Provides secure communication between admin and employee.
- Maintain a Defaulter Score Matrix.
- Provides an employee feed which acts a discussion forum within the organization.

2.2 Important Features

- Login and registration system is provided where employees can register and login into the system
- Employee feed is provided where employees can post, comment and like. These posts can be viewed by all the other employees
- This system helps managers to see the blocked messages and gives them power to act against that employee (e.g. terminating employee’s account)
- A Defaulter Score Matrix is created and updated based on the professional behavior of the employees
- This system uses 3-DES triple key algorithm to encrypt and decrypt the communication.

3. IMPLEMENTATION

3.1 Authorization & Authentication Module

- One step authentication is used to determine the identity of employee or admin/manager.
- Login credentials are read from input text field and the record with same credentials is fetched via SQL query from database.
- If the credentials match, then identity of the user is confirmed and the now the user is granted access.
- User registration functionality is embedded in the system which takes necessary user information to create an account.
- In case user forgets password he/she can answer the security question to set the password again.
- There are two types of user entities: employee and admin (manager). Functionalities provided to them after authorization and authentication are provided as follows

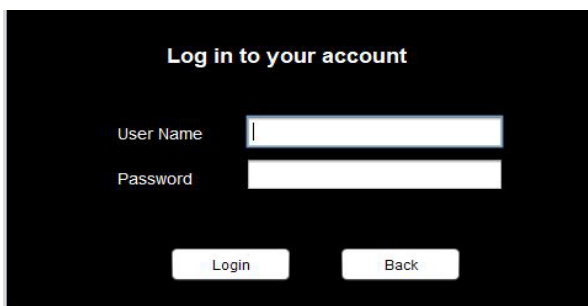


Fig -1: Log In Panel

The figure above is login panel screenshot which is asking for Username and Password.

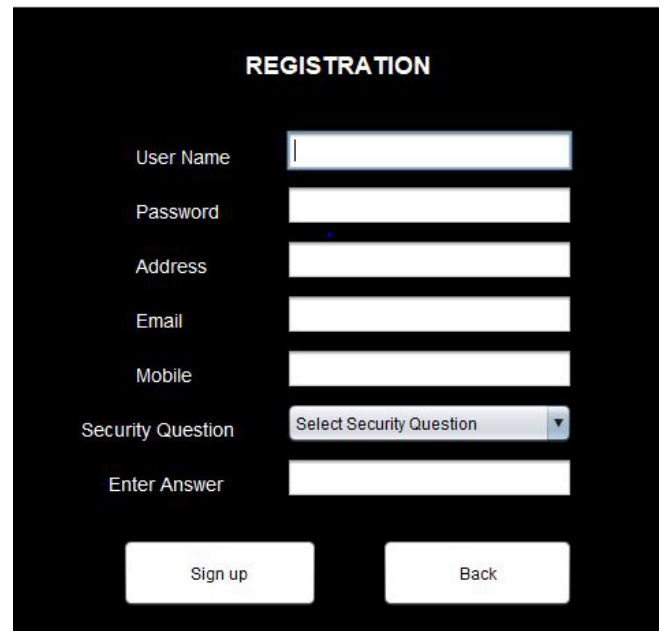


Fig -2: New Employee Registration Panel

The figure shows the registration page for new employees.

3.2 Employee Module

- Each employee is assigned a unique employee id.
- Compose message – employee name is selected from the drop-down list and subject, message body is composed and message is sent.
- Message inbox – A list of received messages appear with subject, message body, sender, message id and any message can be viewed/deleted upon selection. Each message is assigned a priority rating. Messages received from admin needs to be decrypted with the help of a key.
- Sent Messages - A list of send messages appear with subject, message body, recipient, message id and any message can be deleted upon selection.
- Employee feed – can be accessed by employees where any registered user can create a post, view likes, view comments, like, comment on the post. It can be used as a discussion forum within an organization.

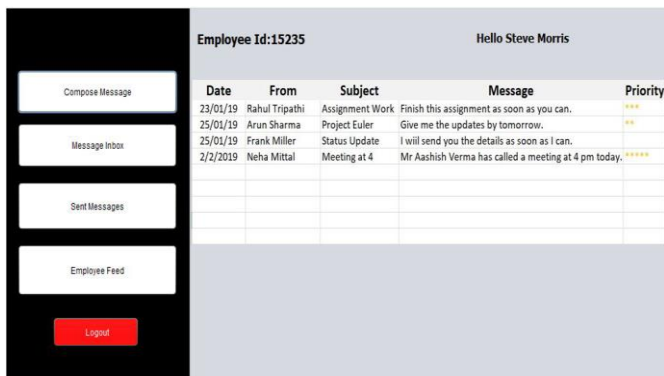


Fig -3: Employee message area

The above figure shows that employee can send and access messages.

3.3 Admin/Manager Module

- Blocked Messages - A list of blocked messages is displayed with sender name, recipient name, message id and message contents. Blocked messages can be viewed and deleted from the list.
- Add blocked words/phrases - Words or phrases can be added to the blocked words list. Messages containing these words will be blocked.
- Blocked words - A list of blocked words is displayed where words can be deleted upon selection.
- Employee list - A list of registered employees is displayed with their username, email id, address and employee id. Admin is authorized to delete any user from the list which would result in termination of that user's account.
- Compose secure message - A secure message is composed with the help of triple DES encryption where the sensitive information sent by admin to other employees is encrypted. Employee name is selected from the drop-down list and subject, message body is composed. Appropriate key is chosen by admin for encryption.

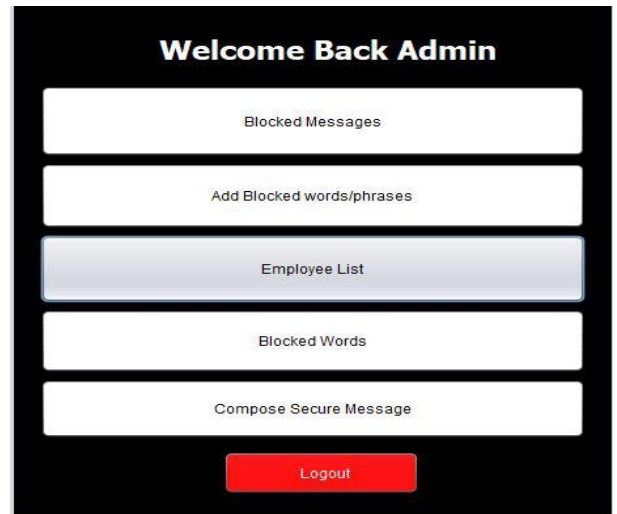


Fig -4: Admin Panel

The above figure shows the admin panel menu.

3.4 Message Flow

- Employee to Employee - Employee to Employee messages are sent via the admin. Admin monitors the content of the message. A search algorithm is applied on the message, if any dubious content (which matches the content in 'blocked words list' is found, message is blocked.
- Admin to Employee - 3-DES encryption algorithm is used to encrypt the message sent by admin to an employee. Employee decrypts via a key to view message received from admin. MIME, SSL, SMTP protocols are used via javax.mail.package.

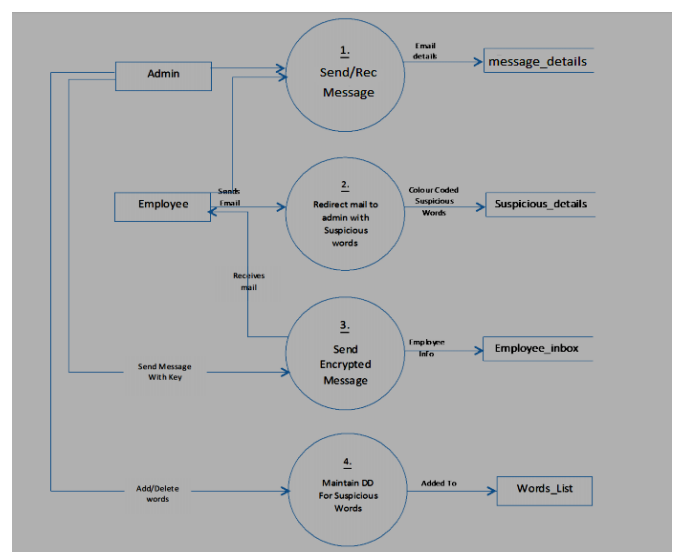


Fig -5: Level-1 Data flow diagram

The figure above shows the flow of data in our system.

3.5 Triple DES Encryption

- Classes from javax.crypto and javax.crypto.spec package are used to design 3-DES encrypt and decrypt methods.
- Both the methods take message and key as the parameters.
- Encryption is done on the admin module. Decryption is done on the employee module. Same key is used by both the entities for encryption and decryption. Admin can send sensitive information to an employee easily.

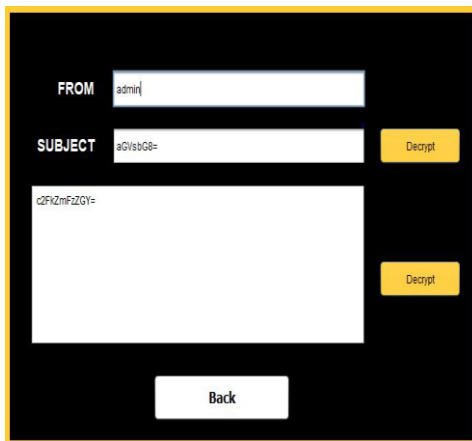


Fig -6: Message Encrypt and decrypt panel

The figure shows the decrypt option in employee module.

3.6 Defaulter Score Matrix

- A defaulter score matrix is created to track an employee's professional behavior.
- An Employee x Points matrix is created where each employee is assigned some points.
- Points are assigned based on how frequently an employee uses words from blocked words list.
- An algorithm is designed in such a way that it maps blocked words used per message to the defaulter points.
- Input given to the algorithm is number of blocked words used per message.

- Output is the number of defaulter points which is added to the final tally of the employee.
- Higher defaulter score means an employee is susceptible to disciplinary actions (stripping off perks, sacking).

4. CONCLUSION

Our approach of developing “Corporate message Filtration Using Triple DES” will prove successful and practical, as it will demonstrate its suitability for solving many issues among employees and avoid creating terrific problem due to bad messages. From this Message system, we can obtain useful information for future work. Further development includes Triple DES algorithm for security problem of more than one department at same time. Also, improving problem modeling and search technique, reducing execution time and enhancing graphical user interface. More research is needed to complete our interactive, automatic message system. The methods, techniques and concepts developed will be tested on more datasets and applications. This application avoids the manual work and the problems concerned with it. In future, we can add more security algorithms to increase the security of the messages. Functionalities such as generating automatic notification and scheduling of messages can be added. 2-step or 3-step authentication can bolster the security of the system preventing brute force attacks.

REFERENCES

- [1] "A Detailed Description of DES and 3DES Algorithms (Data Encryption Standard and Triple DES) | CommonLounge", *Commonlounge.com*, 2019. [Online]. Available: <https://www.commonlounge.com/discussion/5c7c2828bf6b4724b806a9013a5a4b99>. [Accessed: 01- Jan-2019]
- [2] "Triple DES: How strong is the data encryption standard?", *SearchSecurity*, 2019. [Online]. Available: <https://searchsecurity.techtarget.com/tip/Expert-advice-Encryption-101-Triple-DES-explained>. [Accessed: 10- Jan- 2019]
- [3] Patrick Norton & Herbert Schildt - Java 2: The Complete Reference, McGraw Hill Education (India) Private Limited; 8th edition
- [4] Comparison of DES, T. Pornin, B. RAM, K. Gera and I. Boyd, "Comparison of DES, Triple DES, AES, blowfish encryption for data", *Stack Overflow*, 2019. [Online]. Available:





<http://stackoverflow.com/questions/5554526/comparison-of-des-triple-des-aes-blowfish-encryption-for-data/5559132#5559132>. [Accessed: 02- Feb- 2019]

- [5] Roger S. Pressman - Software Engineering: A Practical Approach, McGraw Hill Higher Education, 8th edition, 2014
- [6] Abraham Silberschatz, Henry F. Korth, S. Sudarshan – Database System Concepts, McGraw Hill Education; 6th edition



Ms Varsha Sharma : is an assistant professor in Information Technology department at Bhagwan Parshuram Institute of Technology, New Delhi, India

BIOGRAPHIES

	<p>Nischal Jakhar : a bachelor's student in the Information Technology at Bhagwan Parshuram Institute of Technology, New Delhi, India</p>
	<p>Puranjai Mendiratta : a bachelor's student in the Information Technology at Bhagwan Parshuram Institute of Technology, New Delhi, India</p>
	<p>Vinay Singh : a bachelor's student in the Information Technology at Bhagwan Parshuram Institute of Technology, New Delhi, India</p>
	<p>Utsav Chadha : a bachelor's student in the Information Technology at Bhagwan Parshuram Institute of Technology, New Delhi, India</p>