Performance Comparison of Cryptanalysis Techniques over DES

[1] Anupam Kumar

[1]Assistant Professor, Computer Science & Engineering Department, MAIT,New Delhi-110086, India

[2] Aman Kumar, [3]Sahil Jain,[4]P Kiranmai

[234]Student, Computer Science & Engineering Department, MAIT,New Delhi-110086, India

Abstract:

The primary requirement of a good encryption technique is that it is either impossible or difficult to deduce the plaintext out of a ciphertext without the knowledge of key. Cryptanalysis is the technique that violates this requirement. It focuses on either determining the plaintext out of a ciphertext or guessing the key without trying all the possible combinations of key. Since the development of DES (Data Encryption Standard) in 1977 many cryptanalysis methods have been developed and improved to test security provided by it. Two of the widely used techniques are Linear and Differential cryptanalysis. This paper is aimed at comparing the efficiency of these cryptanalysis methods over Brute Force approach based on experimental results carried out on S-DES. The performances of these methods are compared based on time required for guessing the actual key.

Keywords: S-DES, Plaintext, Ciphertext, Linear cryptanalysis, Differential cryptanalysis, Brute Force attack.

Leave Management System

[1] Alok Kumar Sharma, [2] Dr. Namita Gupta

[1] Lecturer, Computer Science & Engineering Department, MAIT,New Delhi-110086, India

[2]Associate Professor, Computer Science & Engineering Department, MAIT,New Delhi-110086, India

[3] Kajal Goel, [4]P KiranMai

[34]Student, Computer Science & Engineering Department, MAIT,New Delhi-110086, India

---

Abstract:

The project is the design and implementation of an interactive online Leave Management System for any organization. This system automates the process of managing and tracking multiple types of employee leaves. This portal works for any organization and we include the departments, designations, job type and the pay scale accordingly. This system provides with accurate information conveying policy rules, compliance to leave policy, instant information about employees leave history, saves time and improves discipline. Employees are able to submit the leave form, cancel previously submitted leave requests, check the status of leave requests and view completed leave transactions. Any staff can request for leave and the request has to be approved/ disapproved by the authority. Further, the employees can check their leave status. The types of leaves which the staff members can apply for are Casual Leave Earned Leave, Medical Leave, Maternity leave, short Leave, Leave without Pay, On Duty and Study Leave. Based on the leave records employees salary will be generated. If an employee requests for leaves in excess then he/she will be notified and warned. Some leaves if not utilized during a year are carrying forwarded to the next year. The system maintains a database to keep a running balance of each employee's account, accruals employee vacation and sick credits and provides individual reports on employees
leave accruals.

Geolocation Based Recommender System

[1] Yogesh Sharma

[1]Assistant Professor, Computer Science & Engineering Department, MAIT,New Delhi-110086, India

[2] Deepika Bhagwani, [3]Hemant Pandey,[4]Neha Gupta

[234]Student, Computer Science & Engineering Department, MAIT,New Delhi-110086, India

Abstract:

The project entitled "Geo Location based Recommendation System" is recommendation software which is based on the concept of machine learning. The system recommends users by reading the current location of the user, interacting with the database, and provides results based on the calculations. The algorithm takes into account three different parameters to obtain the result. The algorithm used in the project uses Haversine formula to calculate the distance between user and other people in the vicinity. It is capable of recognizing various people and activities related to user's interests. The job profile and organization is also taken into account to obtain the final result. The software recommends people with similar interests with their location to the user.

Keywords: Geolocation, recommender system, machine learning, Haversine formula, recommendations

Network Intrusion Detection & Prevention System: Issues, Challenges & efficiency

[1] Ashish Sharma

[1]Assistant Professor, Computer Science & Engineering Department, MAIT,New Delhi-110086, India

[2] Ishan Tripathi, [3]Prateek Kr. Jindal,[4]Vivek Dixit

[234]Student, Computer Science & Engineering Department, MAIT,New Delhi-110086, India

Abstract:

Network Intrusion Detection & Prevention System is an application which is a part of network security arsenal, considered alongside firewalls and antivirus which are used to protect networked systems. In spite of widespread availability for almost all the operating systems and network platforms, it is one of the least deployed technologies for network security. This technology has been there for more than 20 years but still deployed in very few network systems around the world. Even if they are deployed, they are not used as they are supposed to be due to lack of knowledge of the network administrator about this technology and how to use it. There are various issues with it and it can really be a problem rather than a solution if not used and placed in network architecture properly. A lot of research has been done over the years on this to make it better and more usable. Even after so many improvements over the years, it is still not used as widely as it should be, due to many issues and challenges that are faced while deploying and implementing them. This paper seeks to look into different types of challenges and issues faced while deploying and using IDPS and the reasons behind them. This paper will also look into solutions, which can increase the efficiency of the IDPS.

Keywords: IDPS, recommender system, machine learning, Haversine formula, recommendations