Abstract: In this system we focus on to acquiring volatile data which leave no trails once the system is power off. The volatile data can be in the form of RAM Contents, temporary data used by the OS, data in registers, buffers, unlinked file and unsaved files; and these volatile data may contains information about all running processes, active and recent network connections, open ports and sockets, processes running in background, open files and applications, loaded DLLs, OS kernel module, and active users. These volatile data can have enough information about the anomalous activities on running system.

By collecting this volatile data we train our system using conditional random fields which are more accurate and results in decreasing false alarm rate. In this system we have analysis and prevention as two main blocks. The analysis block is responsible for the system learning and testing. It also alerts the administrator by sending SMS if there is anomalous activity. The prevention block is responsible for preventing the anomalous activity. In this the administrator can stop that anomalous activity, start new activity, shutdown or reboot system or can perform the scanning of the system. The admin may log on to the system locally or remotely. For remote login the user can use Internet or GPRS.

To develop a Hybrid Intrusion Detection System with more accuracy and efficiency and at the same time prevents the suspicious activity on your system or network.

Keywords: DLL, OS Kernel, Volatile data, Conditional Random Fields.
1. Introduction:
This research is concerned with accurate and efficient hybrid intrusion detection system. In this research we combine both the signature based system and anomaly based intrusion detection system. Here we address the two issues of Accuracy and Efficiency using Conditional Random Fields and Encrusted Approach for signature based system and acquiring volatile data once system is turn off For anomaly based system [2]. We demonstrate that high attack detection accuracy can be achieved by using Conditional Random Fields and high efficiency by implementing the Encrusted Approach in signature based system [3]. For the Anomaly based detection we acquire the volatile data when the system is running. From this data we train system and once training is over we are moving for the intrusion detection with conditional random fields and its prevention [2]. We give the authorization to administrator to block the anomalous activity. The administrator may login on system locally or remotely.

2. Literature Survey:
The field of intrusion detection and network security has been around since late 1980s [4]. Since then, a number of methods and frameworks have been proposed and many systems have been built to detect intrusions. Various techniques such as association rules, clustering, naive Bayes classifier, support vector machines, genetic algorithms, artificial neural networks, and others have been applied to detect intrusions.

2.1. Signature Based System:
This approach for detecting intrusion includes the use of genetic algorithm and autonomous and probabilistic agents for intrusion detection [3]. These methods are generally aimed at developing a distributed intrusion detection system. To overcome the Weakness of a single intrusion detection system, a number of frameworks have been proposed, which describe the collaborative use of network-based and host based.

2.2. Anomaly Based System:
In this system we focus on to acquiring volatile data which leave no trails once the system is power off. The volatile data can be in the form of RAM Contents, temporary data used by the OS, data in registers, buffers, unlinked file and unsaved files; and these volatile data may contains information about all running processes, active and recent network connections, open ports and sockets, processes running in background, open files and applications, loaded DLLs, OS kernel module, and active users [6]. These volatile data can have enough information about the anomalous activities on running system.
3. **Proposed System:**

To overcome the drawbacks of the existing intrusion detection systems we proposed hybrid system. This system uses conditional random fields for signature based intrusion detection and for anomaly based intrusion detection and at the same time we are going for intrusion prevention.

i. System Scanning

ii. Anomalous Testing

iii. SMS Alert

iv. Access the System (Locally or Remotely)

v. Kill or Start Activity

Architecture below gives details about application.

Diagram 1

a) In Scanning module the system is scan.

In below diagram, When we scan the system it will display the notepad file which contain all currently running processes.

*Figure 1: System Scanning*
b) Compare the log files and it displays the difference between them. If anomalous activity is there then it alerts the Administrator. Anomalous system testing and SMS alert for the remote administrator.

c) When suspicious activity is found, an alert SMS is sent to the Administrator.

d) The admin may log on to the system locally or remotely. For remote login, the user can use Internet or GPRS.
4. **Advantages:**
This hybrid system combines the advantages of signature-based intrusion detection system (IDS) and the ability of anomaly detection system (ADS) to detect novel unknown attacks. Detection Notified Via SMS. Admin can remotely access to the System. Storage of new attacks in the database.

5. **Disadvantages:**
This application needs internet connection when admin access the system remotely. The main disadvantage of these IDS is that the detection rate of attacks is relatively low, because attacker will try to modify the basic attack signature in such a way that it will not match the known signatures of that attack and it cannot detect a new attack for which a signature is not yet installed in the database.

6. **Future Scope:**
To developing faster implementations of conditional random fields particularly for the domain of intrusion detection requires further investigation. If intrusion detection systems are integrated with the security policy in individual networks would help to minimize the false alarms raised by the intrusion detection systems. I suggest the two issues for continued research and development effort for intrusion detection are prototyping and benchmark. Finally I suggest to improve the real-time detection performance of hybrid intrusion detection system and to decrease the time and cost.

7. **Conclusion:**
Conditional random fields are a strong candidate for building robust and efficient intrusion detection systems. It is observed that system works 100% accurately with the anomaly detection and 95% accuracy with the signature based detection. Apart from the saving money it offers the best one sound quality for the communication.

---------------------------------------------------------------------------------------------------

**Acknowledgement:**

We would like to sincerely thank Mr Amit Zore, our guide, for his support and encouragement.
References:


