

CONFIDENTIAL KEY PRODUCTION FOR SECURE PACKET TRANSFER IN MULTI-NODE MESH NETWORKS

Akshaya.D¹, Chandrika.D.K², Jothirmai Biswal.S³, Kasthuri.K.V⁴, SELVA KUMAR.A⁵

B.E, (Computer Science and Engineering, T.J.S Engineering College, Tamilnadu, India.

ABSTRACT

This paper studies the key generation problem in the two-way relay channel, in which there is no direct channel between the key generating terminals. We propose an effective key generation scheme that achieves a substantially larger key rate than that of a direct channel mimic approach. Unlike existing schemes, there is no need for the key generating terminals to obtain correlated observations in our scheme. Secure key distribution schemes for group communications allow establishing a secure multi cast communication between a group manager and group members through an unreliable broadcast channel. The improved efficiency for key management is realized by periodically refreshing all public private key pairs as well as any multicast keys in all the nodes using only one newly generated function broadcasted by the key generator entity. The article classifies, analyzes and compares the most significant key distribution schemes, by looking at the selective key distribution algorithms, at the predistributed secret data management, and at the self-healing mechanisms. It reviews polynomial-based algorithms, exponential arithmetic based algorithms, hash-based techniques, and others. Propose classification of schemes based on the applied cryptographic primitives.

Keyword: - Networking, Internet Protocol, JAVA, J2EE, JAVA Servlets, My Sql, Modules, Testing, Use Case Diagrams, Net Beans, etc...

1. INTRODUCTION

In the field of networking, the area of network security consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources. The term network security and information security are often used interchangeably. Network security is generally taken as providing protection at the boundaries of an organization by keeping out intruders (hackers). Information security, however, explicitly focuses on protecting data resources from malware attack or simple mistakes by people within an organization by use of data loss prevention (DLP) techniques. One of these techniques is to compartmentalize large networks with internal boundaries. There are various ways in which a network can be attacked by intruders/hackers. Some common attacks and threats are discussed below: DoS (Denial-of-Service) attacks are probably the nastiest, and most difficult to address. These are the nastiest, because they're very easy to launch, difficult (sometimes impossible) to track, and it isn't easy to refuse the requests of the attacker, without also refusing legitimate requests for service. The premise of a DoS attack is simple: send more requests to the machine than it can handle. There are toolkits available in the underground community that make this a simple matter of running a program and telling it which host to blast with requests. The attacker's program simply makes a connection on some service port, perhaps forging the packet's header information that says where the packet came from, and then dropping the connection. If the host is able to answer 20 requests per second, and the attacker is sending 50 per second, obviously the host will be unable to service all of the attacker's requests, much less any legitimate requests. "Unauthorized access" is a very high-level term that can refer to a number of different sorts of attacks. The goal of these attacks is to access some resource that your machine should not provide the attacker. For example, a host might be a web server, and should provide anyone with requested web pages. However, that host should not provide command shell access without being sure that the person making such a request is someone who should get it, such as a local administrator. There are two main classifications of the severity of this problem: normal user access, and administrator access. A normal user can do a

number of things on a system (such as read files, mail them to other people, etc.) that an attacker should not be able to do. This might, then, be all the access that an attacker needs. On the other hand, an attacker might wish to make configuration changes to a host (perhaps changing its IP address, putting a start-up script in place to cause the machine to shut down every time it's started or something similar). In this case, the attacker will need to gain administrator privileges on the host. Among the destructive sorts of break-ins and attacks, there are two major categories. The data diddler is likely the worst sort, since the fact of a break-in might not be immediately obvious. Perhaps he's toying with the numbers in your spreadsheets, or changing the dates in your projections and plans. Maybe he's changing the account numbers for the auto-deposit of certain paychecks. In any case, rare is the case when you'll come in to work one day, and simply know that something is wrong. Some of those perpetrate attacks are simply twisted jerks who like to delete things. In these cases, the impact on your computing capability – and consequently your business – can be nothing less than if a fire or other disaster caused your computing equipment to be completely destroyed.

1.1 Existing System

- Insecure mechanisms provided in the existing network.
- Almost none of the schemes is suitable for large scale WSN in real- world applications.
- Existing solutions usually present some tradeoff between scheme performance and security level.
- Identifies basic building blocks of the scheme and describes in details all major types of existing solutions.
- It also contains a thorough security and efficiency analysis of each solution, and points out issues not identified.

1.2 Objective

The main objective of our project is to improve the network security. To overcome these threats and data loss and provide a safe network that overcomes these threats we have to produce an advanced safety technique. So this project proposes a mechanism is to advertise the routing path information for IP prefixes. Improve the security that flexible communication infrastructures which provide a diverse set of operations. Improvement in signature verification and signature generation.

1.3 Contribution

The main objective of our project is to improve the network security. To overcome these threats and data loss and provide a safe network that overcomes these threats we have to produce an advanced safety technique. So this project proposes a mechanism is to advertise the routing path information for IP prefixes. Improve the security that flexible communication infrastructures which provide a diverse set of operations. Improvement in signature verification and signature generation.

2. LITERATURE SURVEY

Due to the broadcast nature of wireless channels, wireless communication is vulnerable to eavesdropping, message modification, and node impersonation. Securing the wireless communication requires the shared secret keys between the communicating entities. Traditional security schemes rely on public key infrastructures and cryptographic algorithms to manage secret keys. Recently, many physical-layer-based methods have been proposed as alternative solutions for key generation in wireless networks. These methods exploit the inherent randomness of the wireless fading channel to generate secret keys while providing information-theoretical security without intensive cryptographic computations. This article provides an overview of the existing PHYbased key generation schemes exploiting the randomness of the wireless channels. Specifically, we first introduce the fundamental and general framework of the PHY-based key generation schemes and then categorize them into two classes: received-signal-strength-based and channel-phase-based protocols. Finally, we present a performance comparison of them in terms of key disagreement probability, key generation rate, key bit randomness, scalability, and implementation issues.

This paper investigates generation of a secret key from a reciprocal wireless channel. In particular we consider wireless channels that exhibit sparse structure in the wideband regime and study the impact of sparsity on the secret key capacity. We explore this problem in two steps. First, we study key generation from a state-dependent discrete memory less multiple source. The state of the source captures the effect of channel sparsity. Secondly, we consider a wireless channel model that captures channel sparsity and correlation between the legitimate users' channel and the eavesdropper's channel. Such dependency can significantly reduce the secret key capacity.

According to system delay requirements, two performance measures are considered: (i) ergodic secret key capacity and (ii) outage probability. We show that in the wideband regime when a white sounding sequence is adopted, a sparser channel can achieve a higher ergodic secret key rate than a richer channel can. For outage performance, we show that if the users generate secret keys at a fraction of the ergodic capacity, the outage probability will decay exponentially in signal bandwidth. Moreover, a larger exponent is achieved by a richer channel.

3. PROPOSED SYSTEM

- Functionality of the scheme is decomposed into three separate aspects, namely: selective key distribution mechanism, predistributed secret data management and self-healing mechanism, which are used to classify and compare schemes.
- We introduce a three-dimensional classification, based on each aspect of the scheme separately, which allows for more flexibility.
- Self-healing group key distribution schemes can be used in multicast networks with centralized management, which are established over an unreliable broadcast channel, such as machine-to-machine systems, embedded and sensor networks, cellular networks and wireless networks.
- Communications security is achieved by message encryption and authentication using shared symmetric secret group key.
- A prospective group key distribution scheme should satisfy the following requirements:
 - **Authorization:** The scheme should prevent adversaries or unauthorized user nodes, which are not in G, from learning the group key.
 - **Key freshness:** Key distribution scheme has to provide fresh keys.

3.1 Advantages of Proposed System

- Individualized encryption is done over this project
- Robust network connectivity
- Efficiency is increased.
- Hacker cannot easily detect the server.
- The proposed system is harder to shutdown, monitored, hijacked and shutdown.

4. RESULT

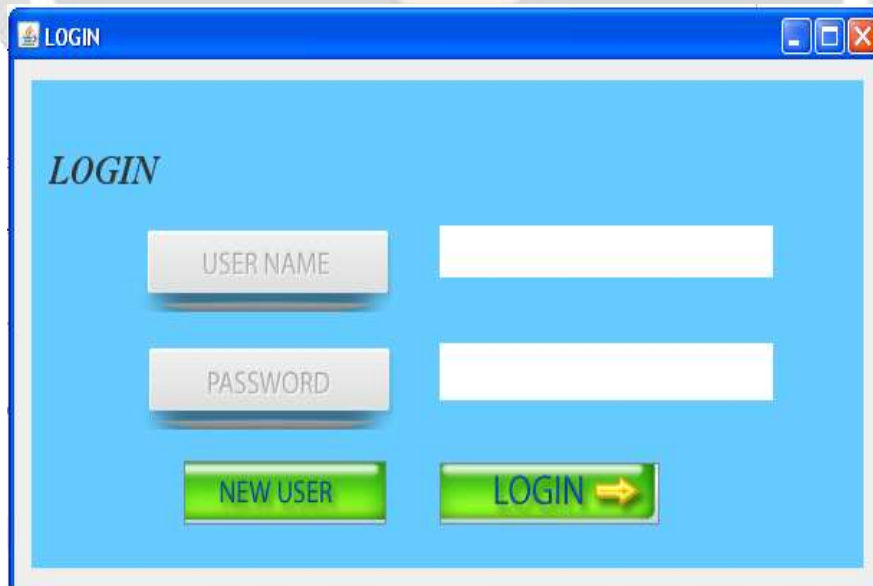
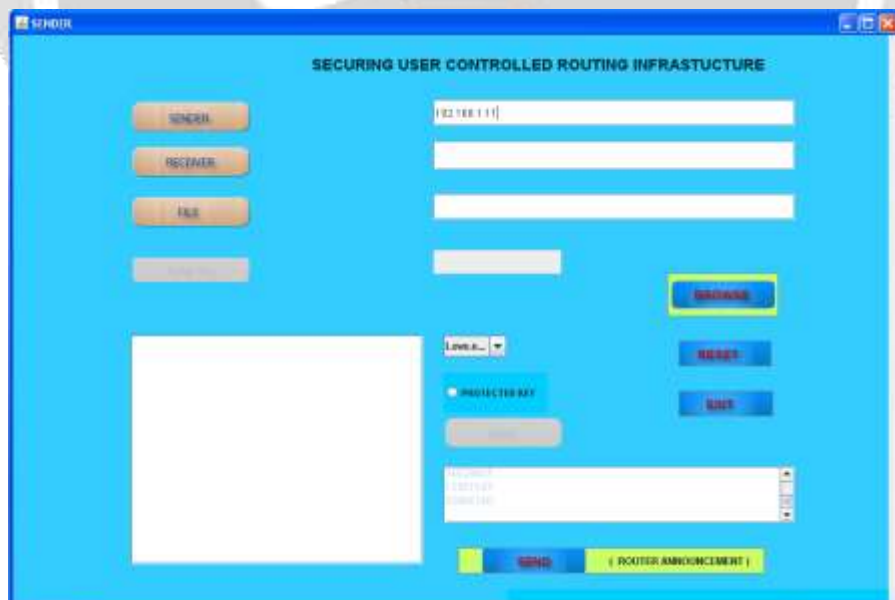


Fig.No.1 Screenshot of the Project

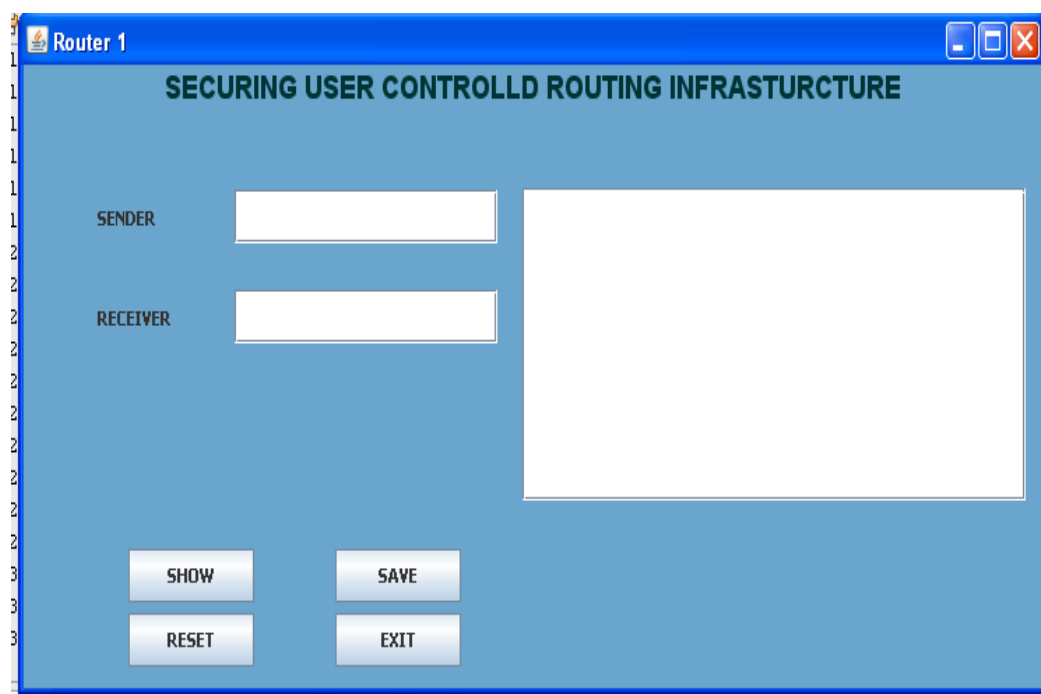
Registration Page for new User:

A screenshot of a Windows-style application window titled "ADD NEW USER". The window has a light blue background. It contains five text input fields labeled "Username", "Password", "Email Address", "Age", and "Address". At the bottom right, there are three buttons: "Submit", "Reset", and "Exit".

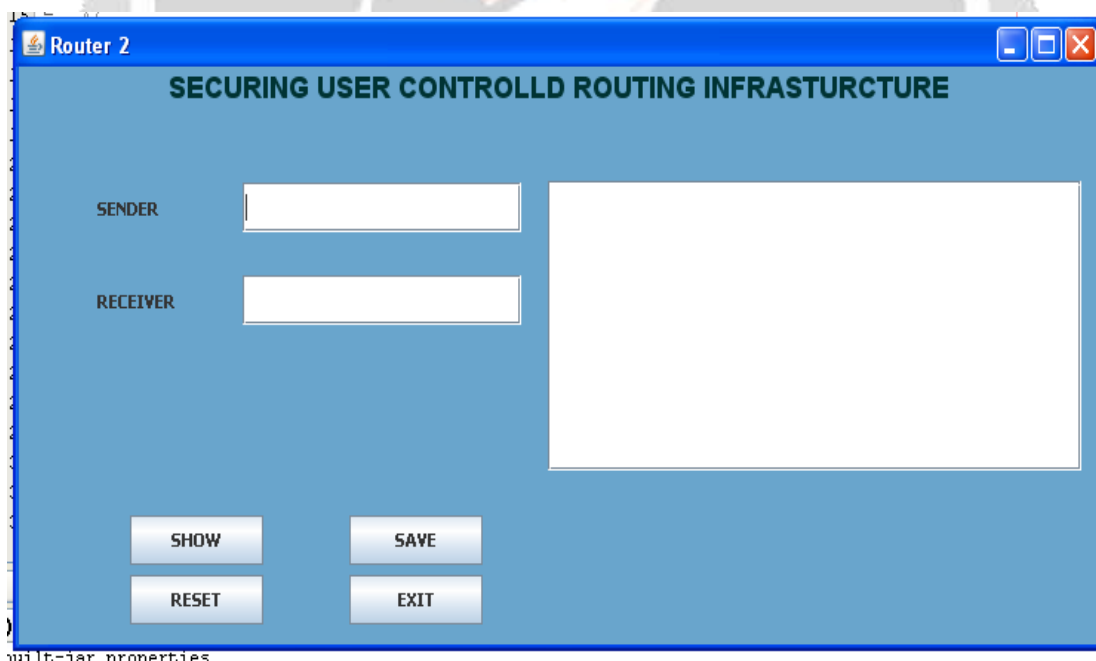
Fig.No.2 Screenshot of the Project**Sender Page:**

A screenshot of a Windows-style application window titled "SENDER". The window has a light blue background. On the left side, there are four buttons: "SENDER", "RECEIVER", "FILE", and "SEND". On the right side, there are several input fields and buttons. At the top right, there is a text input field labeled "IP ADDRESS". Below it are two more text input fields. Further down, there is a "SEND" button. Below the "SEND" button, there is a "RECEIVE" button and a "QUIT" button. At the bottom right, there is a "ROUTER ANNOUNCEMENT" button. On the left side, there is a large empty rectangular area. At the bottom left, there is a "SEND" button. At the bottom right, there is a "ROUTER ANNOUNCEMENT" button.

Fig.No.3 Screenshot of the Project

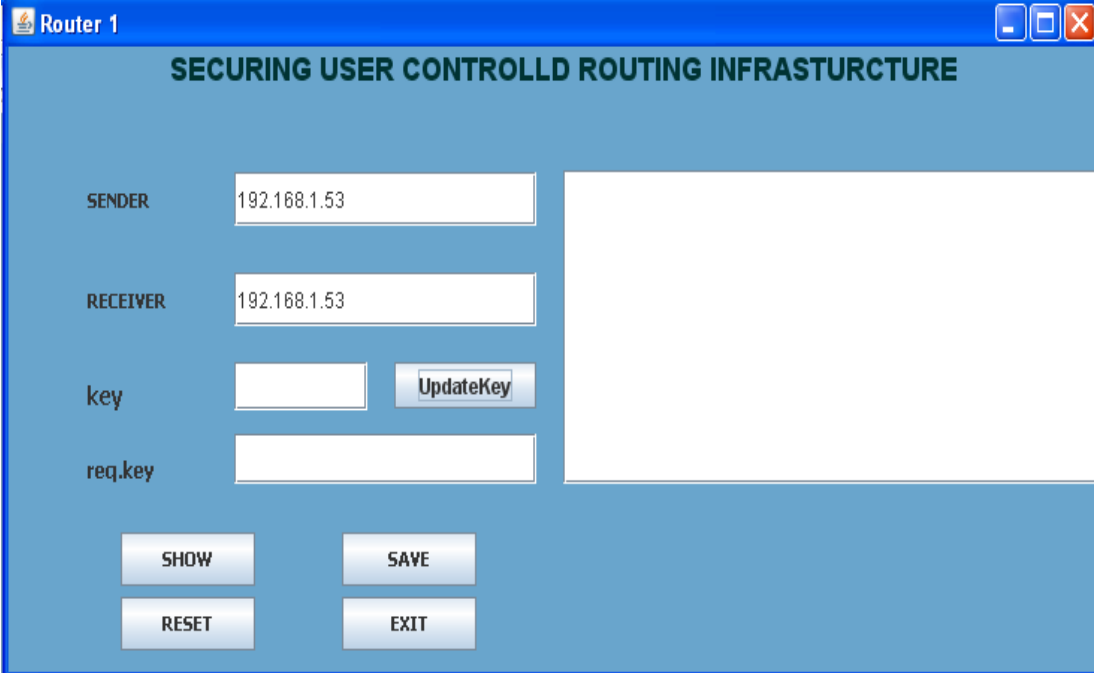
Router 1&2 Before Sending file:

The screenshot shows a window titled "Router 1" with a blue border and standard Windows window controls. The main area has a blue background and is titled "SECURING USER CONTROLLED ROUTING INFRASTRUCTURE". It contains two input fields: "SENDER" and "RECEIVER", both of which are empty. To the right of these fields is a large, empty white rectangular area. At the bottom, there are four buttons arranged in a 2x2 grid: "SHOW", "SAVE", "RESET", and "EXIT".

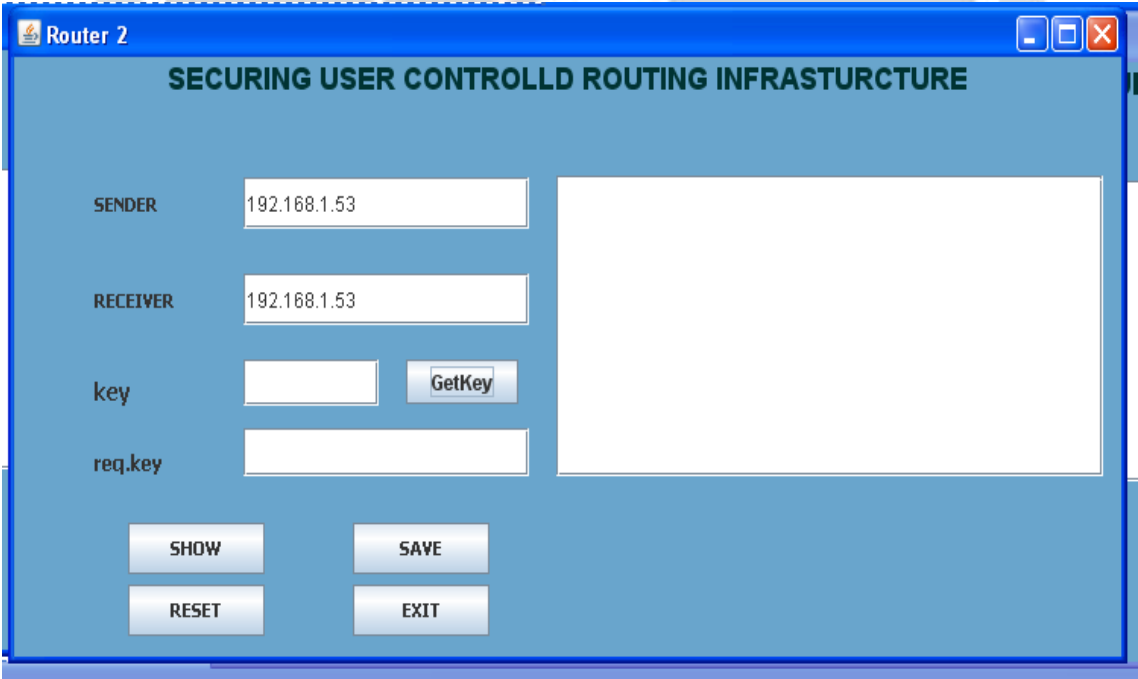
Fig.No.4 Screenshot of the Project

The screenshot shows a window titled "Router 2" with a blue border and standard Windows window controls. The main area has a blue background and is titled "SECURING USER CONTROLLED ROUTING INFRASTRUCTURE". It contains two input fields: "SENDER" and "RECEIVER", both of which are empty. To the right of these fields is a large, empty white rectangular area. At the bottom, there are four buttons arranged in a 2x2 grid: "SHOW", "SAVE", "RESET", and "EXIT".

Fig.No.5 Screenshot of the Project

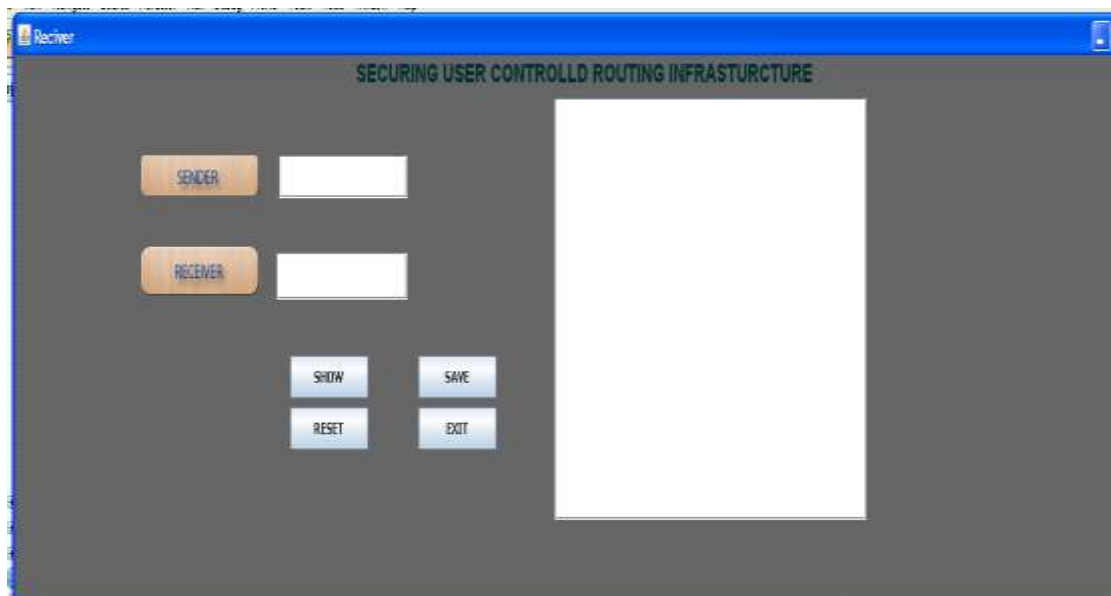
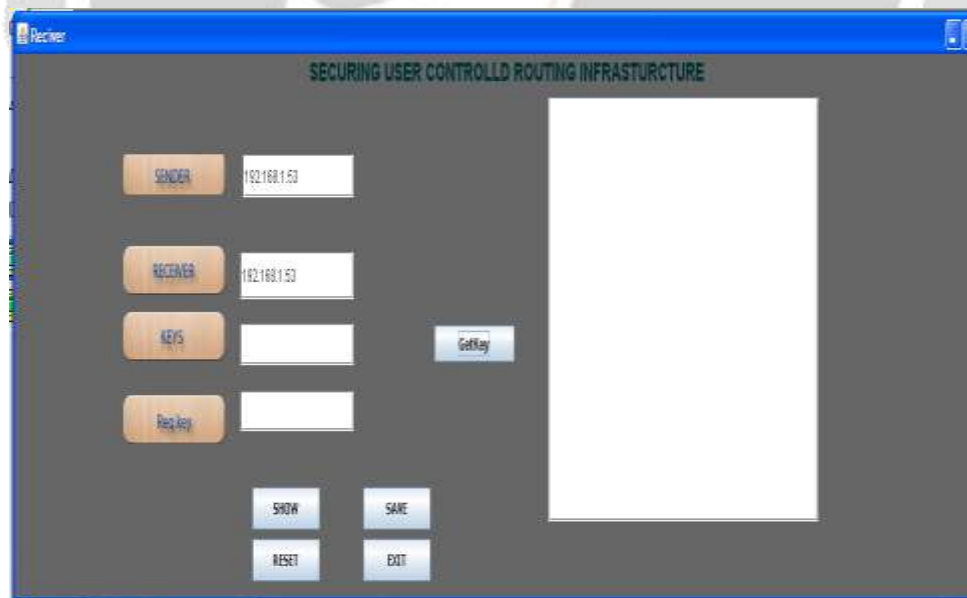
Router 1&2 After Sending file:

The screenshot shows a window titled "Router 1" with a blue header bar. Below the header, the text "SECURING USER CONTROLLED ROUTING INFRASTRUCTURE" is displayed. The interface contains several input fields and buttons. The "SENDER" field is set to "192.168.1.53". The "RECEIVER" field is also set to "192.168.1.53". There are two empty input fields labeled "key" and "req.key". A button labeled "UpdateKey" is positioned next to the "key" field. At the bottom, there are four buttons: "SHOW", "SAVE", "RESET", and "EXIT".

Fig.No.6 Screenshot of the Project

The screenshot shows a window titled "Router 2" with a blue header bar. Below the header, the text "SECURING USER CONTROLLED ROUTING INFRASTRUCTURE" is displayed. The interface contains several input fields and buttons. The "SENDER" field is set to "192.168.1.53". The "RECEIVER" field is also set to "192.168.1.53". There are two empty input fields labeled "key" and "req.key". A button labeled "GetKey" is positioned next to the "key" field. At the bottom, there are four buttons: "SHOW", "SAVE", "RESET", and "EXIT".

Fig.No.7 Screenshot of the Project

Receiver before Receiving File:**Fig.No.8 Screenshot of the Project****Receiver after Receiving File:****Fig.No.9 Screenshot of the Project**

5. CONCLUSIONS

A secure multi-keyword ranked search scheme over encrypted cloud data, which simultaneously supports dynamic update operations like deletion and insertion of documents. The cloud server traverses different paths on the index, and the data user receives different results but with the same high level of query accuracies in the meantime. The keyword-based search is such one widely used data operator in many database and information retrieval applications, and its traditional processing methods cannot be directly applied to encrypted data. Therefore, how to process such queries over encrypted data and at the same time guarantee data privacy. Then, in order to improve the search efficiency, we design the group multi-keyword top- k search scheme, which divides the dictionary into multiple groups and only needs to store In the sense no need to give exact filename to download the file, if you are going to give maximum number of time repeated words, that time also original file will be downloaded in decrypted format. This helps to maintain the security of the files in the cloud.

6. REFERENCES

1. D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in IEEE Symposium on Security and Privacy, 2000, pp. 44–55.
2. B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in IEEE International Conference on Computer Communications, 2014, pp. 2112–2120.
3. M. Kuzu, M. S. Islam, and M. Kantarcioglu, "Efficient similarity search over encrypted data," in IEEE 28th International Conference on Data Engineering (ICDE), 2012, pp. 1156–1167.
4. C. Wang, K. Ren, S. Yu, and K. M. R. Urs, "Achieving usable and privacy-assured similarity search over outsourced cloud data," in 2012 Proceedings of IEEE INFOCOM, 2012, pp. 451–459.
5. C. Orencik, M. Kantarcioglu, and E. Savas, "A practical and secure multi-keyword search method over encrypted cloud data," in IEEE Sixth International Conference on Cloud Computing (CLOUD), 2013, pp. 390–397.
6. M. Li, B. Lang, and J. Wang, "Compound concept semantic similarity calculation based on ontology and concept constitution features," in Tools with Artificial Intelligence (ICTAI), 2015 IEEE 27th International Conference on, 2015, pp. 226–233.