A TRAPDOOR HASH-BASED MECHANISM FOR STREAM AUTHENTICATION

MOHAMED SULIMAN MUSTAFA ALI , Mr. N. GANAPATHIRAM

Abstract— This project titled “A Trapdoor Hash-Based Mechanism for Stream Authentication” is aimed to increase the data transmission failure to a large extent by using the hop count packet slicing mechanism. In a network the sharing of data is very important in the mean time the security given to the data what we are sharing is also very important. This project helps sent the required data from source to destination in a secure manner. In this system we focus on the most common and uneasily identifiable attack on the network called “packet access”. In the network the data transmission takes places in pieces called “Packets”.This Project uses Android Programming Language as its Front End and SQLite as its back End. This project helps the user to detect and identify the affected or tampered packets andfilter them easily. When both the system have source and destination, then both the machines are possible to send and receive the data vice versa. The current communication world is most dependent on the data transfer from theservers. All the vital and more secure data transmission from bank to defense sector uses thenetwork for its operation. But the network system that is used by us can be mostly a common target for cyber attack. So the network has to be protected to keep our data transmission secure. This application has the following modules, Authentication Module, Sender Module, Bridge Module (Router Module) and Receiver Module.

Keywords—Packet Access, Data Transmission, Android, SQLite.

I. INTRODUCTION

This aimed to increase the data transmission failure to a large extent by using the hop count packet slicing mechanism. In a network the sharing of data is very important in the mean time the security given to the data what we are sharing is also very important. This project helps sent the required data from source to destination in a secure manner. In this system we focus on the most common and uneasily identifiable attack on the network called “packet access. This project helps the user to detect and identify the affected or tampered packets andfilter them easily. When both the system have source and destination, then both the machines are possible to send and receive the data vice versa. The current communication world is most dependent on the data transfer from the servers.All the vital and more secure data transmission from bank to defense sector uses the network for its operation. But the network system that isused by us can be mostly a common target for cyber attack. So the network has to be protected to keep our data transmission secure.

Group editors are a classic model and research vehicle for distributed interactive groupware applications because they typically manipulate shared data in a coordinated manner. Operational transformation (OT) has been well accepted in group editors for achieving optimistic consistency control OT allows local operations to execute in a nonblocking manner to achieve high local responsiveness and unconstrained collaboration. Remote operations are transformed before they are executed such that inconsistencies are repaired.

Despite the significant progress that has been achieved over the past 15 years, a notable fact in the history of OT is that the discovery and solution of various OT puzzles (i.e., correctness problems in previous OT algorithms) have been a main driver of research. However, the existence of OT puzzles can be largely attributed to the lack of a suitable theoretical framework for guiding the design and verification of OT algorithms. More specifically, the well- established frameworks rely on conditions that are difficult to verify in practice and do not address how to develop correct OT algorithms. In this project, a novel operation transformation framework is developed to overcome the weakness of existing system. Based on a concept called “operation effects relation,” defined two criteria, causality preservation and operation effects relation preservation, for verifying the correctness of OT algorithms.

Mohamed Suliman Mustafa Ali, Student, M.Sc Computer Science, Rathinam College of Arts and Science, Coimbatore, Tamil Nadu, India – 641021, (e-mail: mohmmed1998157@gmail.com).

Mr. N. Ganapathiram, Assistant Professor, Department of Computer Science, Rathinam College of Arts and Science, Coimbatore, Tamil Nadu, India – 641021,
(e-mail: ganapathiram.cs@rathinam.in).

II. SYSTEM DEVELOPMENT

A) Existing System:

The current communication world is most dependent on the data transfer from theservers. All the vital and more secure data transmission from bank to defense sector uses thenetwork for its operation. But the network system that is used by us can be mostly a common target for cyberattack. If an attack is happened it is difficult to identify and prevent.

Disadvantages:

1. Waste of time.
2. Inadequate information Reach.
3. Security Weakness.
4. Loss of Vital Data.
5. Leads to loss of transmission time
6. No Monitoring Mechanism
7. Leads to Mal Practices
8. Lead to delay in work

B) Proposed System:

In a network the sharing of data is very important in the mean time the security given to the data what we are sharing is also very important.

This project helps sent the required data from source to destination in a secure manner.

In this system we focus on the most common and uneasily identifiable attack on the network called “packet access”. In the network the data transmission takes places in pieces called “Packets”.

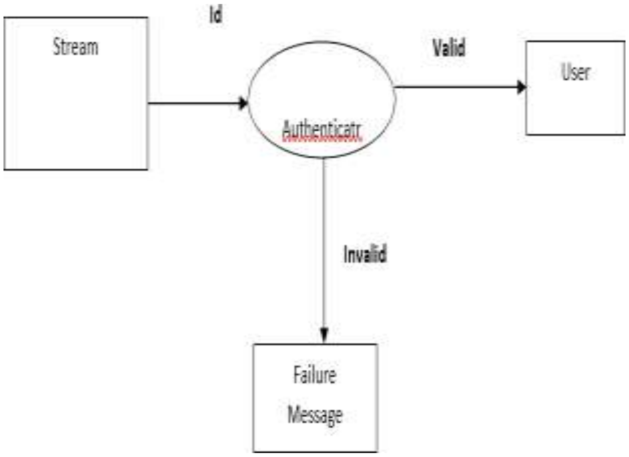
This project helps the user to detect and identify the affected or tampered packets andfilter them easily. When both the system have source and destination, then both themachines are possible to sent and receive the data vice versa.

Advantages of Proposed System:

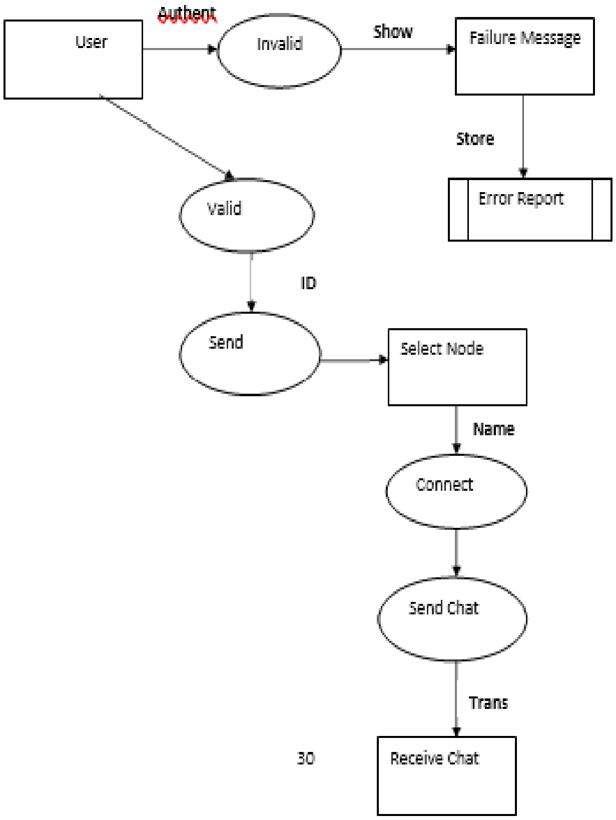
1. The required information can be secured easily.
2. Time will not be wasted in the repeated   n process.
3. Security Increased.
4. Prevents Loss of Vital Data.
5. Effective Monitoring Mechanism
6. Prevents Packet Tampering on the Network
7. Good Guidance
8. Efficient Monitoring Mechanism
9. Less Expensive
10. Prevents Loss of Vital Data.

III. PROPOSED WORK DIAGRAM

Data Flow Diagram:
Level 0:

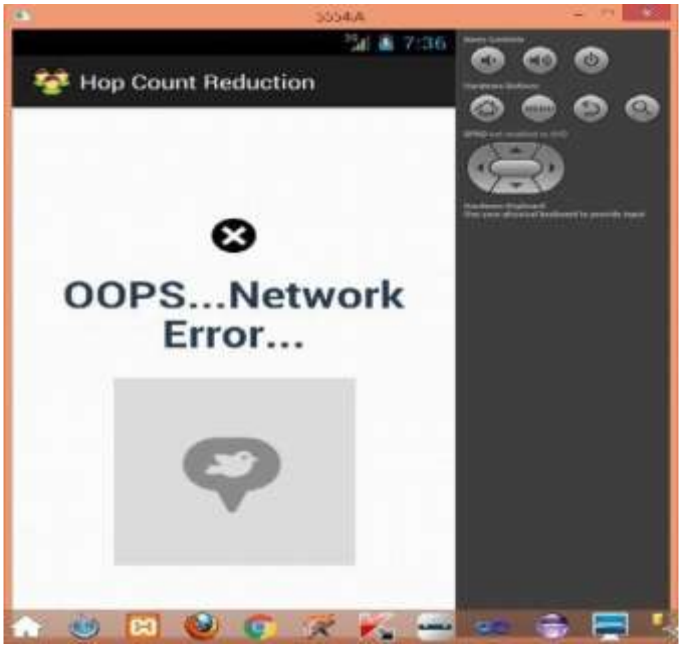


Level 1:



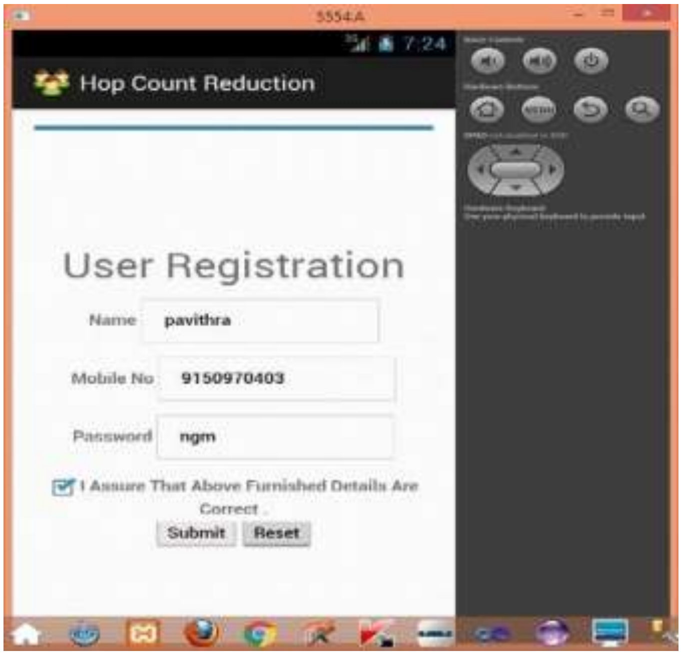
IV. EXPERIMENTAL RESULTS

Hop Count Reduction:



OOPS...Network Error...

User Registration



User Registration

Name pavithra

Mobile No 9150970403

Password ngm

☑ I Assure That Above Furnished Details Are Correct .

V. CONCLUSION

In this project the efficient framework for the text and graphical chatting is developed using operation transformation algorithm. The basic idea of operation transformation is executed in this project and the effectiveness is identified from the output of this project. The front-end application design of this project enables a user or client to send the text and graphical data to any user by accessing a single window. At the same time this project has the capability to send the data to a group of users or any particular user. The general assumption underlying interactive groupware application, such as group editors, is that users are aware of the discover and resolve semantic conflicts in a timely manner.

SCOPE OF FUTURE WORK

In future enhancement this system can be converted into a web based application which makes the user to have more simple and efficient use of data that make the working of this system into a fast and secure one. . In the current situation this application has been designed to work in android in future this concept can be implemented open source platform.

REFERENCES

[1] Brown, B. (2009). Beyond Downadup: Security expert worries about smart phone, TinyURL threats: Malware writers just waiting for financial incentive to strike, F-Secure exec warns. Retrieved from http://business.highbeam.com/409220/article-1G1-214585913/beyond-downadup-security- expert-worries-smartphone.

[2] Bose, A. (2008). Propagation, detection and containment of mobile malware.(Doctoral dissertation, University of Michigan).Retrieved from www.phoenix.edu/apololibrary.

[3] Xie, L., Zhang, X., Chaugule, A., Jaeger, T., & Zhu, S. (2009). Designing system-level defenses against cellphone malware. Retrieved from www.cse.psu.edu

[4] Bhattacharya, D. (2008) Leadership styles and information security in small businesses: An empirical investigation (Doctoral dissertation, University of Phoenix). Retrieved from www.phoenix.edu/apololibrary.

[5] Mulliner, C., & Miller, C. (2009). Injecting SMS messages into smartphones for security analysis. Proceedings of the 3rd USENIX Workshop on Offensive Technologies Montreal, Canada. Retrieved from www.usenix.org.