DEFENDING VIRTUAL GROSS SYSTEM FROM SOFTWARE GUSTY

A.SUBASH[1] AND SAHAYA JENITHA[2] ALLEN STEVE[3]

[1]Department of Computer Application,Francis Xavier Engineering college

[2]AP.Department of Computer Application,Francis Xavier Engineering college

[3]Department of Computer Application,Francis Xavier Engineering college

ABSTRACT

The aim of our project is to build a secure Web Application platform for auditing. The auditee uploads their financial records to the platform and the uploaded records can only be accessed by an authorized auditor. The data integrity is ensured by using cryptography. We can prevent malware like Trojan. The data will be in an encrypted format. Even if a hacker manages to get his hands on the data, it cannot be exploited.

KEYWORDS

Network Protocols, Mobile Network, Virus, Trojon

1. INTRODUCTION

To evaluate the proposed secure communication frame-work, a set of studies have been conducted, a discrete event-driven network simulator built with java. In real time auditing application there is a major drawback in security side because of illegal advertisement run on the app with owner permission on that same time Trojan malicious should be injected on the system by hackers to avoid this we can secure the applications confidential details by using our concept. Researchers have proposed a broad range of defense strategies against XSS attacks. Park and Sandhu's [36] cookie-securing mechanism can be adopted to eliminate XSS, but it requires explicit modifications to existing Web applications. Scott and Sharp [50] have proposed using gateways for filtering malicious input at the application level. In addition to preventing XSS, the gateway also prevents SQL injection—another widespread Web application vulnerability. Next, we describe how information flow testing is performed in order to identify XSS vulnerabilities, and then report our results from two experiments. In experiment 1, we installed and scanned five Web applications that were found vulnerable by WebSSARI, and a) compared testing coverage with WebSSARI (static verification), and b) studied the results of our proposed non-detrimental scanning techniques and their impact on testing coverage.The second section discuss about the literature review and continued by problem statements. The fourth section gives the experiments and results followed by the conclusion and future enhancement.

D. Angeline, A. Arul et al.(Eds): ICICI-2021
pp. 259-267, 2021. IJCI – 2021 DOI:10.5121/ijci.2021.100229

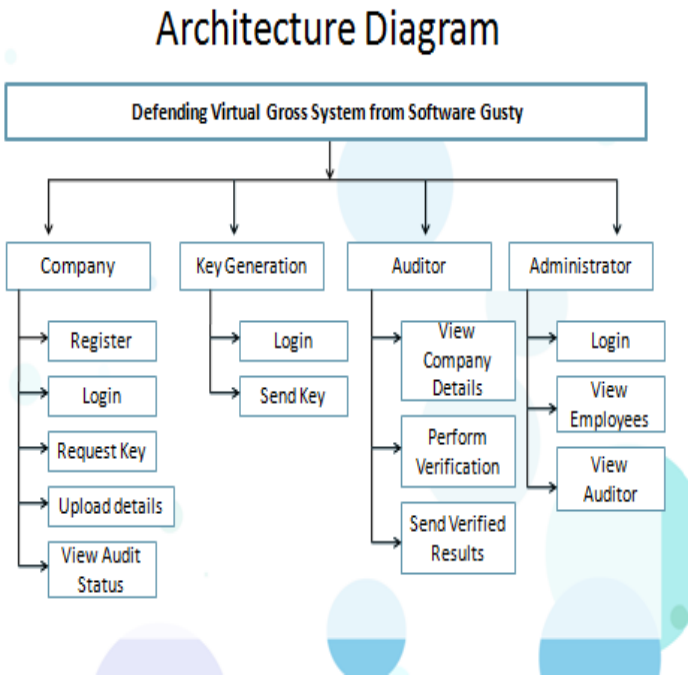

Figure 1:Architecture diagram

2. PROBLEM STATEMENTS

Modules

- **Economic feasibility** : The proposed system is economically feasible because the cost involved in purchasing the hardware and the software is within approachable. Working with this system need not require a highly qualified professional. The operating-environment costs are marginal. The less time involved also helps in its economic feasibility.

- **Technical feasibility** : Earlier no system existed to cater to the needs of 'Audit Business Information'. The current system developed is technically feasible. It is a browser based user interface for construction workflow. Thus, it provides an easy access to the users.

- **Social Feasibility** : The analyst considers the extent that the proposed system will fulfill his departments. That is, whether the proposed system covers all aspects of the working system and whether it has considerable improvements. We have found that the proposed "Trojan Security" will certainly have considerable improvements over the existing system.

3. EXPERIMENTS AND RESULTS

Output Screen

Figure 2:Admin page

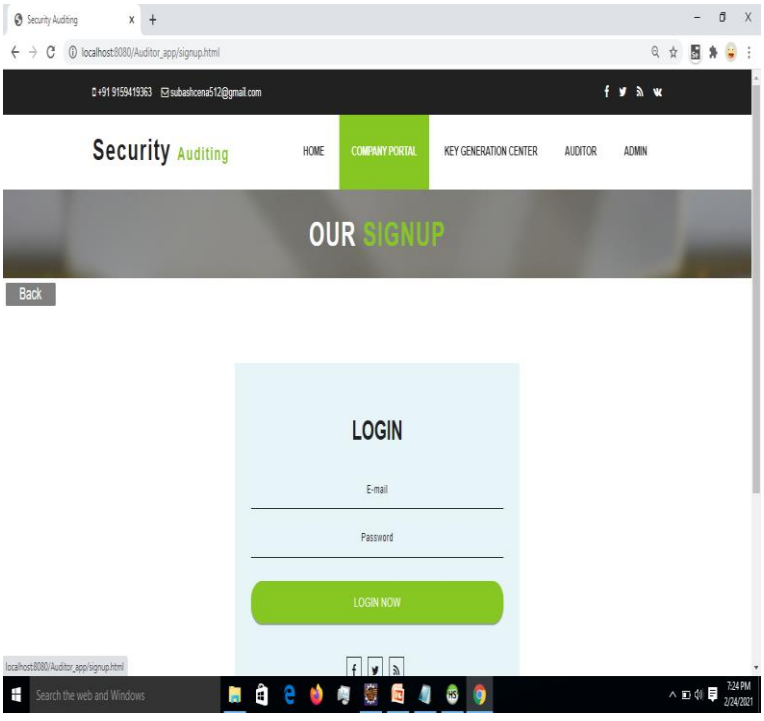

Figure 3:login page

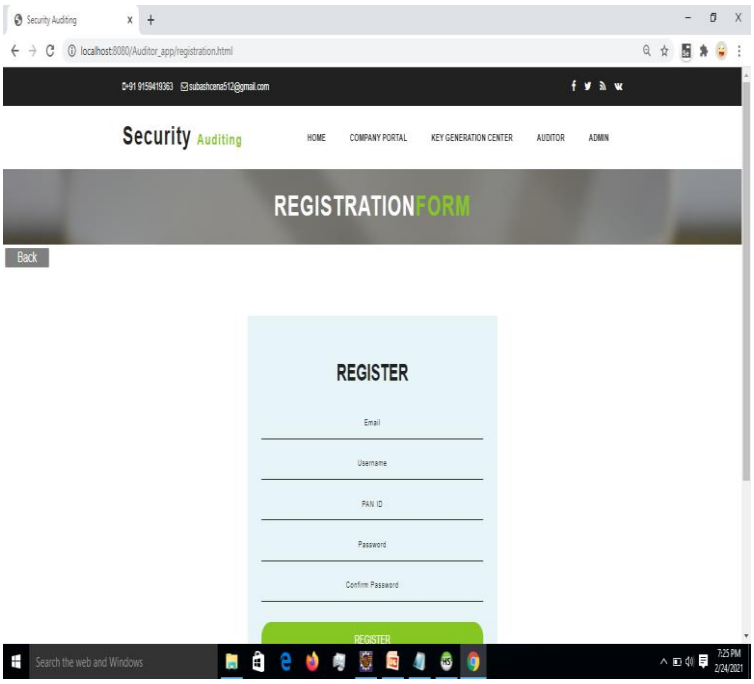

Figure 4:Registration page

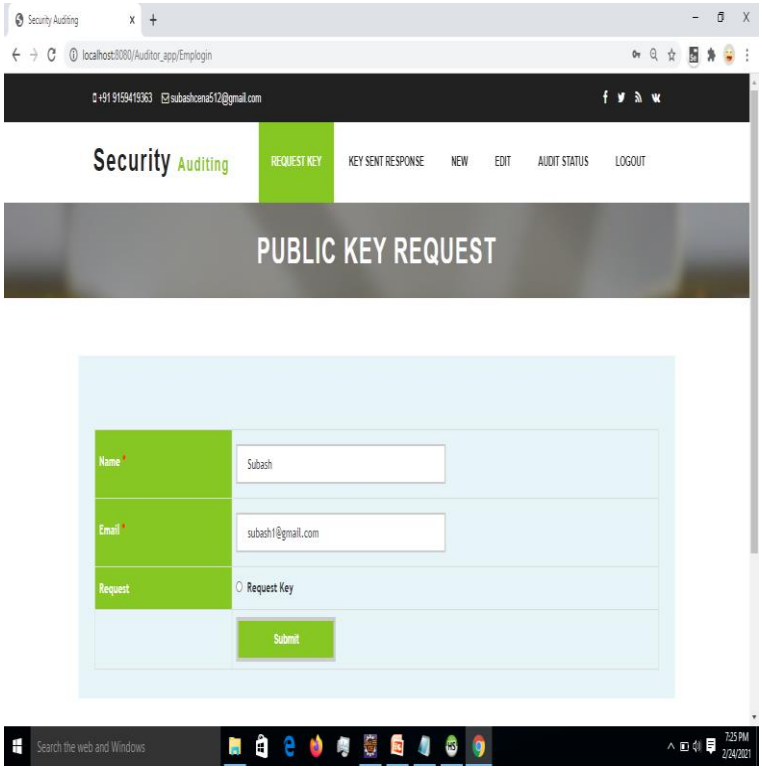

Figure 5:Request page

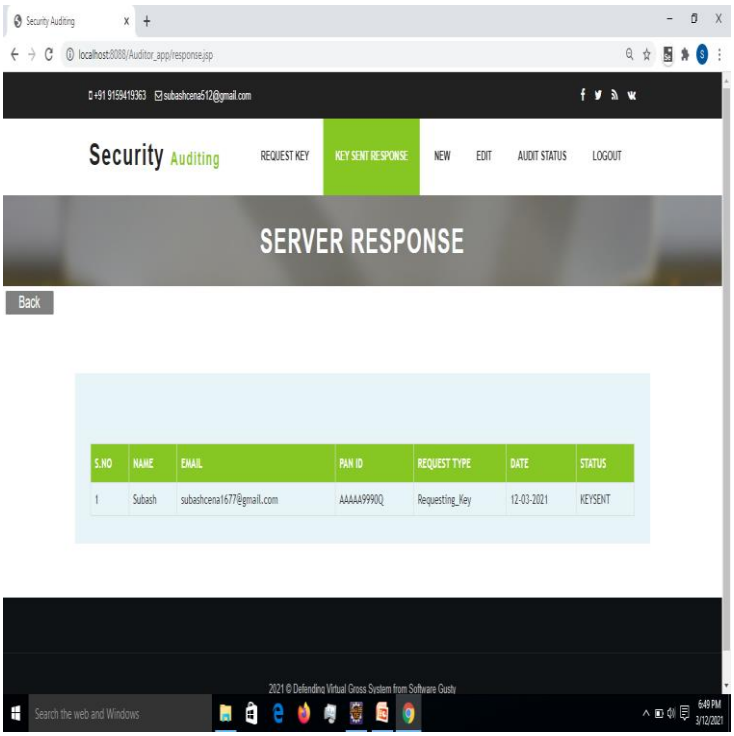

Figure 6:Server page

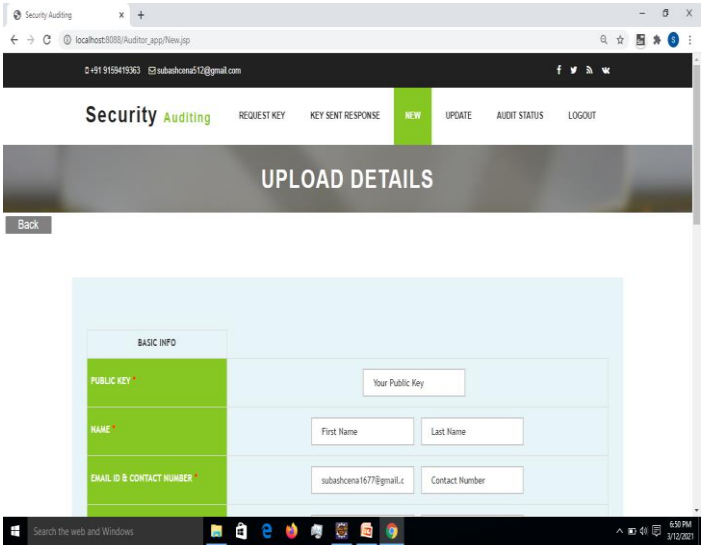

Figure 7:Upload page

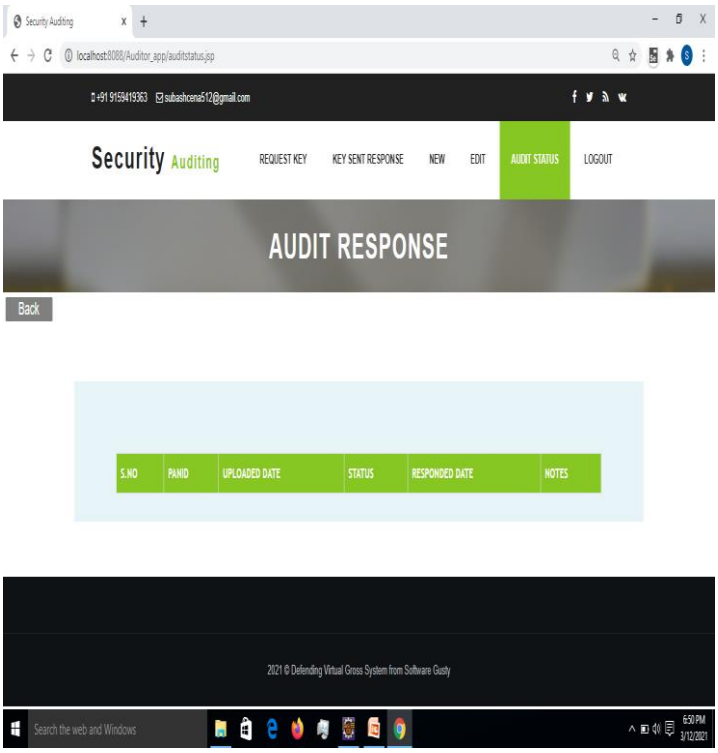

Figure 8:Response page

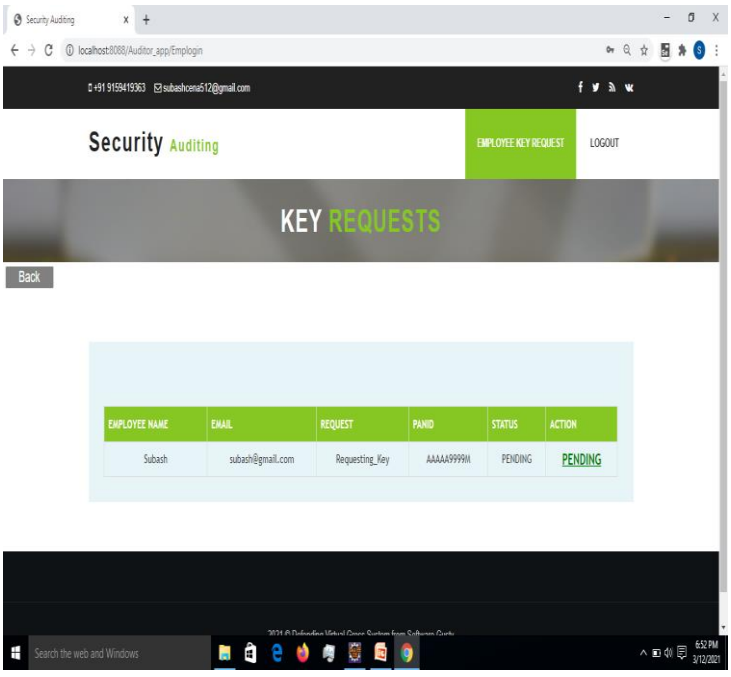

Figure 9:Key Request page

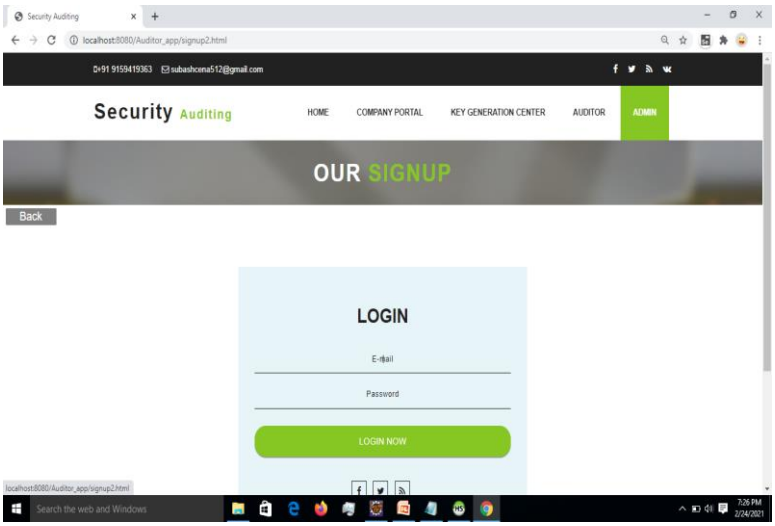

Figure 10:Login page

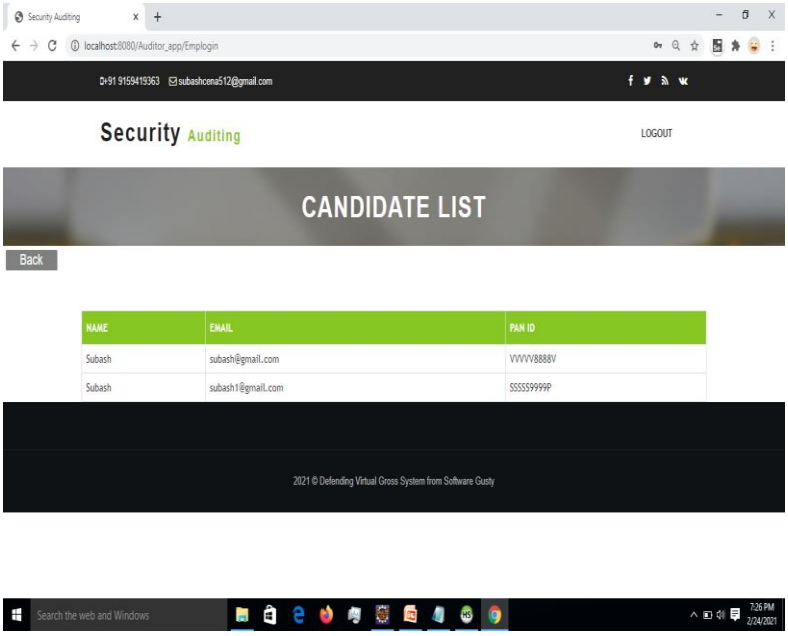

Figure 11:List page

4. PERFORMANCE ANALYSIS

The existing and proposed system are analysed, The problem identified in existing is Because declarative security always appears at the beginning of the application element, it's easier to find the security settings. That makes it a better option from a documentation perspective This assumption has prevented them from automating nearly , 70% performance has been increased.

5. CONCLUSION

In this application, we have presented followed by the basic framework for message encryption and mutual auditing as the interlinked upstream and downstream stages. We have mainly implemented by the all data's converted by the encryption method, all the data secured and

efficiently delivered by the customers side. Privacy will be increasingly important, as our society become more networked and data about individuals are increasingly digitalized. Such a tool has several potential applications. Experimental results showed that the proposed security framework effectively precluded hardware Trojan collusion. It only imposed constant low overhead on communication latency, with negligible impact on packet arrival rate and network throughput. The only major overhead was the cost of utilizing nodes from extra vendors, which could be mitigated by wisely deploying the network.

REFERENCES

[1] M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection," IEEE Des. Test Comput., pp. 10–25, 2010.

[2] Swarup Bhunia; Miron Abramovici; Dakshi Agrawal; Paul Bradley; Michael S. Hsiao; Jim Plusquellic; Mohammad Tehranipoor,"Protection Against Hardware Trojan Attacks: Towards a Comprehensive Solution,"Published in: IEEE Design & Test in 2013.

[3] Veronika Reinauer; Christian Magele; Christian Scheiblich; Andrej Stermecki; Remus Banucu; Jan Albert; Michael Jaindl and Wolfgang M. Rucker,"Object-Oriented Development of an Optimization Software in Java Using Evolution Strategies,"Published in: IEEE Transactions on Magnetics in 2012.

[4] H. Salmani, M. Tehranipoor, and J. Plusquellic, ''A novel technique for improving hardware Trojan detection and reducing Trojan activation time,'' IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 20, no. 1, pp. 112–125, Jan. 2011.

[5] Swarup Bhunia, Michael S. Hsiao, Mainak Banga, Seetharam Narasimhan, "Hardware Trojan Attacks: Threat Analysis and Countermeasures", Proceedings of the IEEE, vol. 102, no. 8, pp. 1229-1247, 2014.

[6] Andrews, A., Offutt, J., Alexander, R. "Testing Web Applications by Modeling with FSMs." Submitted for publication, January 2004.

[7] Bell, D. E., La Padula, L. J. "Secure Computer System: Unified Exposition and Multics Interpretation." Tech Rep. ESD-TR-75-306, MITRE Corporation, 1976.

[8] Bertolino, A. "Knowledge Area Description of Software Testing," In Guide to the Software Engineering Body of Knowledge SWEBOK (v. 0.7), Chapter 5, Software Engineering Coordinated Committee (Joint IEEE Computer Society-ACM Committee), April, 2000. http://www.swebok.org

[9] Benedikt M., Freire J., Godefroid P., "VeriWeb: Automatically Testing Dynamic Web Sites." In Proc. 11th Int'l Conf. World Wide Web, Honolulu, Hawaii, May 2002.

[10] Bergman, M. K. "The Deep Web: Surfacing Hidden Value." Deep Content Whitepaper, 2001.

AUTHOR

A,Subash doing final year MCA in Francis Xavier Engineering College

Mrs. S. Sahaya Jenitha working as Assistant Professor in the Department of Computer Applications, Francis Xavier Engineering College. Her area of interest is Wireless Sensor networks

w

Allen steve E doing first year MCA in Francis Xavier Engineering College