AUTHENTICATED MEDICAL DOCUMENTS RELEASING WITH PRIVACY PROTECTION AND RELEASE CONTROL

V.Sarala [1] E.Venkat Kumar [2],

[1]**Assistant professor, MCA DEPT,** Dantuluri Narayana Raju College**, Bhimavaram, Andharapradesh**
Email:-vedalasarala21@gmail.com
[2]**PG Student of MCA, Dantuluri** Narayana Raju College**, Bhimavaram, Andharapradesh**
Email:-venkatkumar6263@gmail.com

ABSTRACT

In the context of Information Societies, a tremendous amount of information is daily exchanged or released. Among various information-release cases, medical document release has gained significant attention for its potential in improving healthcare service quality and efficacy. However, integrity and origin authentication of released medical documents is the priority in subsequent applications. Moreover, sensitive nature of much of this information also gives rise to a serious privacy threat when medical documents are uncontrollably made available to un trusted third parties.

Redactable signatures allow any party to delete pieces of an authenticated document while guaranteeing the origin and integrity authentication of the resulting (released) subdocument. Nevertheless, most of existing redactable signature schemes (RSSs) are vulnerable to dishonest redactors or illegal redaction detection. To address the above issues, we propose two distinct RSSs with flexible release control (RSSs-FRC). We also analyse the performance of our constructions in terms of security, efficiency and functionality. The analysis results show that the performance of our construction has significant advantages over others, from the aspects of security and efficiency.

1 INTRODUCTION

In the realm of healthcare, the release of medical documents plays a crucial role in ensuring continuity of care, legal compliance, and patient empowerment. However, the process of releasing these documents must be meticulously managed to uphold patient privacy and data security standards. This challenge has led to the development of sophisticated systems for authenticated medical document releasing with robust privacy protection and release control mechanisms.

This introduction explores the intersection of technology and healthcare in managing medical document release, focusing on the importance of privacy protection and release control. It outlines the necessity of balancing patient access to their medical information with safeguarding sensitive data against unauthorized access and breaches. Moreover, it underscores the role of advanced

authentication methods in ensuring the integrity and authenticity of released medical documents.

2 RELEATED WORK

A literature survey on "Authenticated Medical Documents Releasing with Privacy Protection and Release Control" delves into a multifaceted domain at the intersection of healthcare informatics, security protocols, and regulatory compliance. It encompasses an exploration of authentication methods such as digital signatures and blockchain, designed to ensure the integrity and validity of medical documents. Privacy protection mechanisms, including encryption and access control, play a crucial role in safeguarding sensitive patient information from unauthorized access. Release control mechanisms, such as policy-based access controls and consent management systems, are essential for managing the secure dissemination of medical records to authorized parties while adhering to legal frameworks like GDPR and HIPAA. Through case studies and technological innovations, the literature survey evaluates existing implementations, identifies challenges, and highlights opportunities for advancing the security and privacy of authenticated medical document releasing systems.

3 implementation study

Existing System:

The primitive of data verification has been well studied by plenty of researchers in the past decades [1]–[7]. Most of the prior work focused on generic solutions for the integrity and authenticity verification. While they protect data from alteration by malicious attackers, they also prevent data from being processed and thus hinder the further flexible and efficient use of data. Moreover, in some situations they are incompatible with the confidentiality of the data. Therefore, it is meaningful to seek for appropriate protocols for data verification with confidentiality.

Disadvantages:

In the existing work, the system implements the redactable signature scheme (RSS) designed in this work is based on Merkle hash tree and GGM tree. The outstanding disadvantage of this design is that signature is relatively short for the application of Merkle hash tree.

The existing system introduced a new hierarchical redaction control policy whose encoding is dramatically smaller..

Proposed System & alogirtham

The proposed system is to design secure and efficient RSSs with flexible release control (RSSs-FRC) so as to provide privacy preservation and flexible release control guarantee for authenticated medical documents release systems. The main contributions of our work are summarized as follows.

The system proposes two novel RSSs-FRC satisfying different release control requirements in medical document releasing systems. The minimal release control in RSSs-FRC1 is realized by

employing the threshold secret sharing scheme. RSSs-FRC2 achieves hybrid release control through access tree which control not only the minimal release number but also the dependency of releasable subdocument blocks.

Advantages:

In order to preserve the privacy information in the authenticated medical document as much as possible, dishonest patients might not be willing to release a sufficient number of signed medical subdocument blocks to third parties for some services.

The system is more secured since Redactable signatures, a straightforward approach, inherently solve the authentication theoretical incompatibility and practical requirements of privacy information redaction in authenticated medical document releasing.

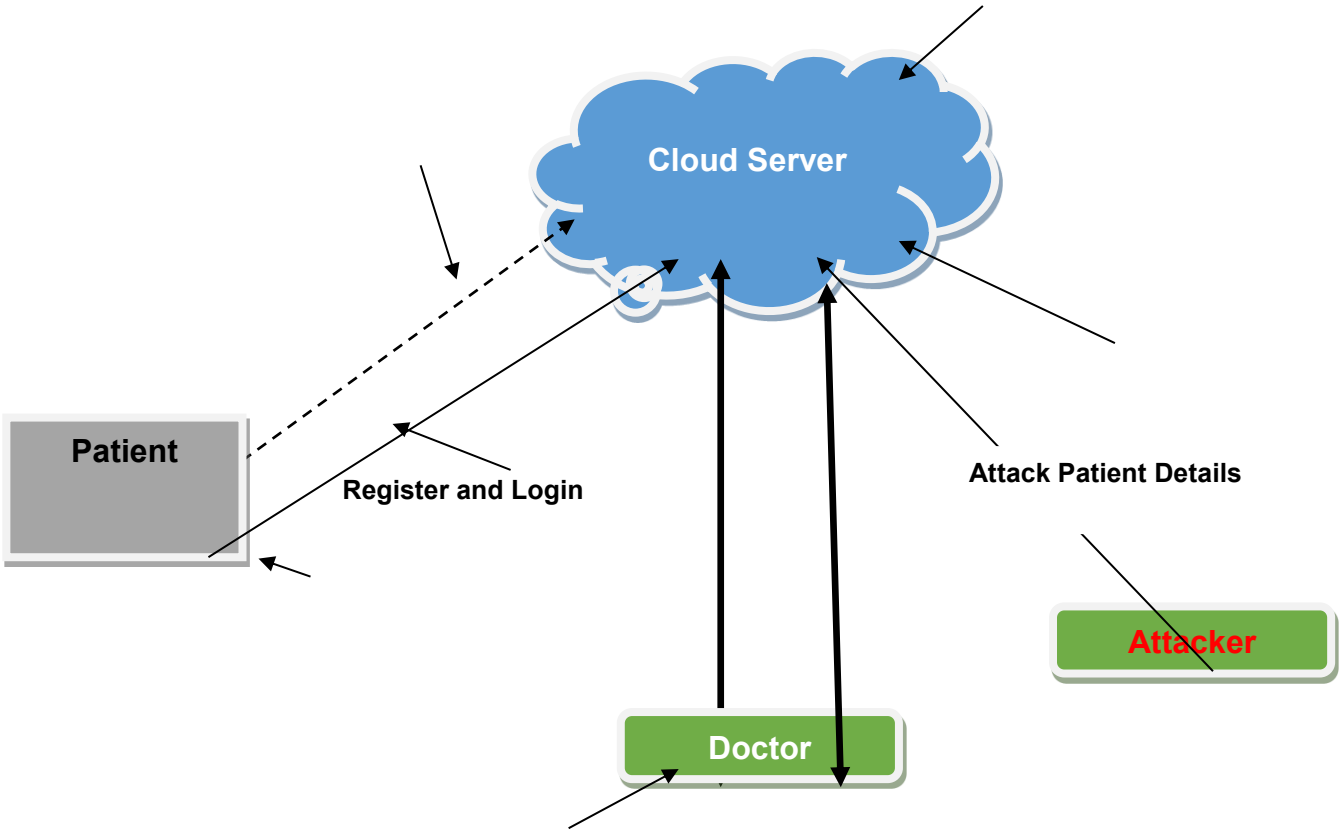


Fig1: SYSTEM ARCHITECTURE

4.IMPLEMENTATION

MODULES

Patient:

A patient outsources her documents to the cloud server to provide convenient and reliable data access to the corresponding search doctors. To protect the data privacy, the patient encrypts the original documents under an access policy using attribute-based encryption. To improve the search efficiency, she also generates some keyword for each outsourced document. The corresponding index is then generated according to the keywords using the secret key of the secure kNN scheme. Afterthat, the patient sends the encrypted documents, and thecorresponding indexes to the cloud server, and submitsthe secret key to the search doctors.

Cloudserver:

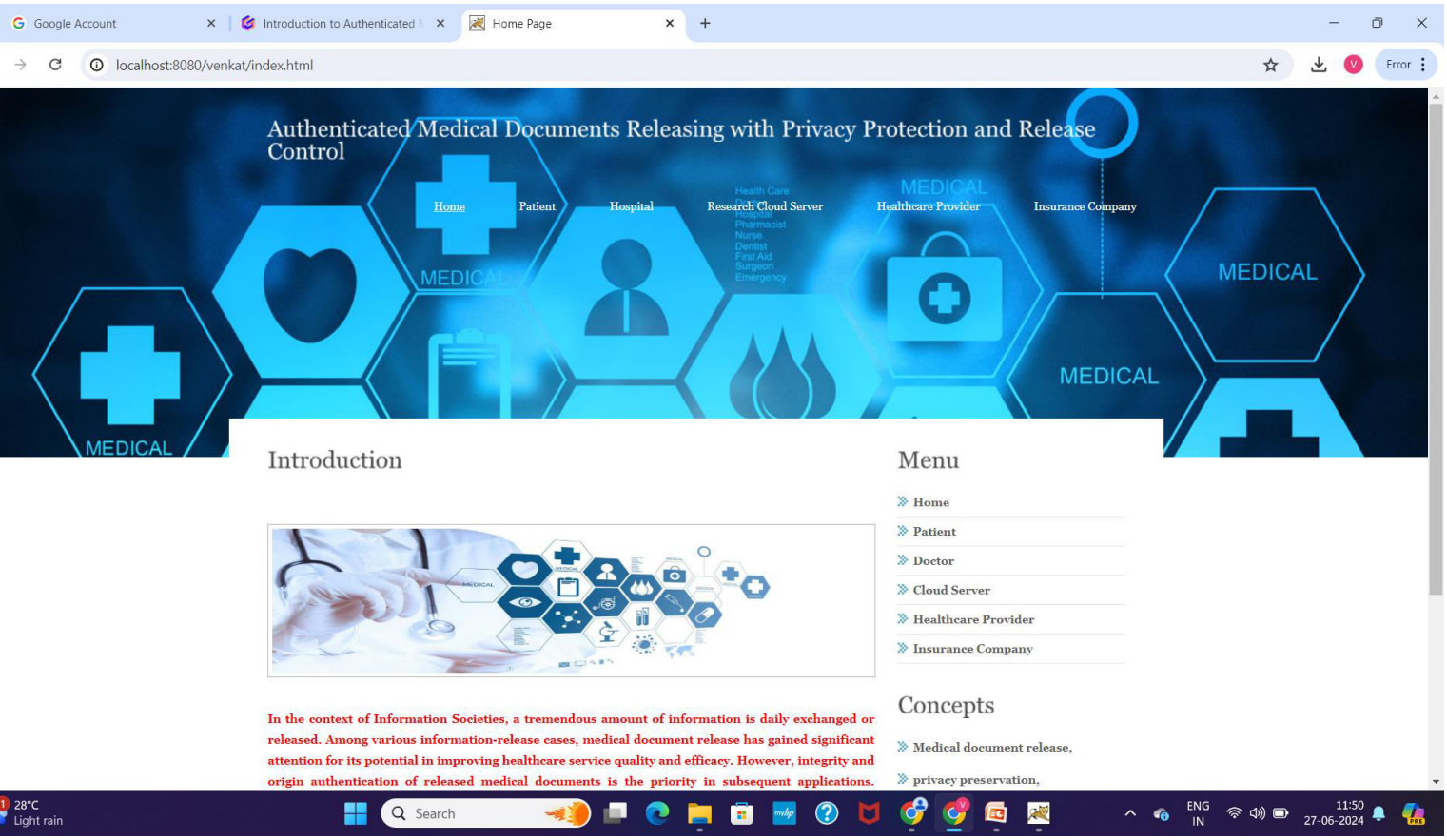
A cloud server is an intermediary entity which stores the encrypted documents and the corresponding indexes received from patients, and then provides data access and search services to authorized search doctors. When a search doctor sends a trapdoor to the cloud server, it would return a collection of matching documents based on certain operations.

Doctor:

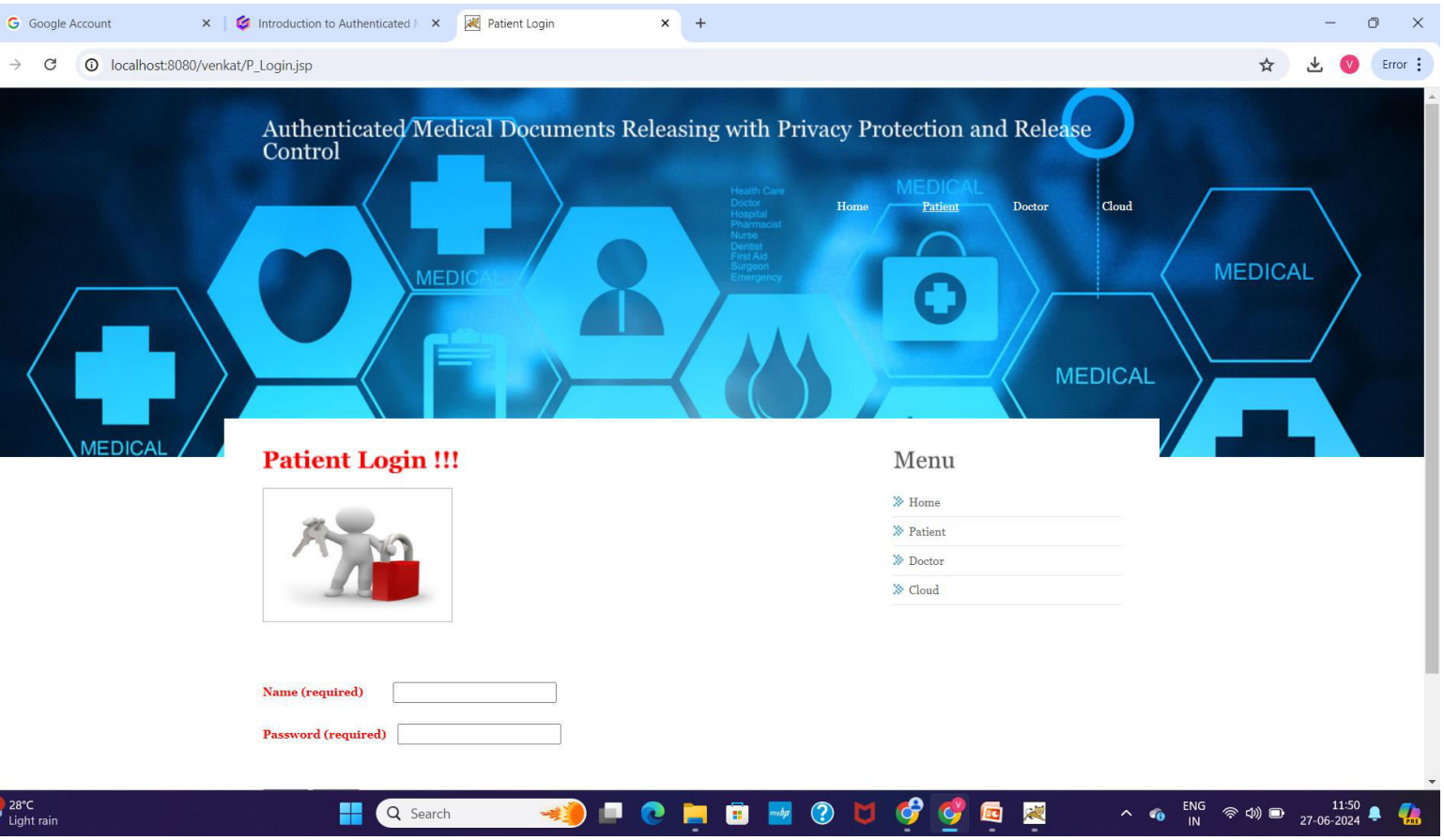
An authorized doctor can obtain the secret key from the patient, where this key can be used to generate trapdoors. When she needs to search the outsourced documents stored in the cloud server, she will generate a search keyword set. Then according to the keyword set, the doctor uses the secret key to generate a trapdoor and sends it to the cloud server. Finally, she receives the matching document collection from the cloud server and decrypts them with the ABE key received from the trusted authority. After getting the health information of the patient, the doctor can also outsource medical report to the cloud server by the same way. For simplicity, we just consider one-way communication in our schemes.

5 RESULTS AND DISCUSSION

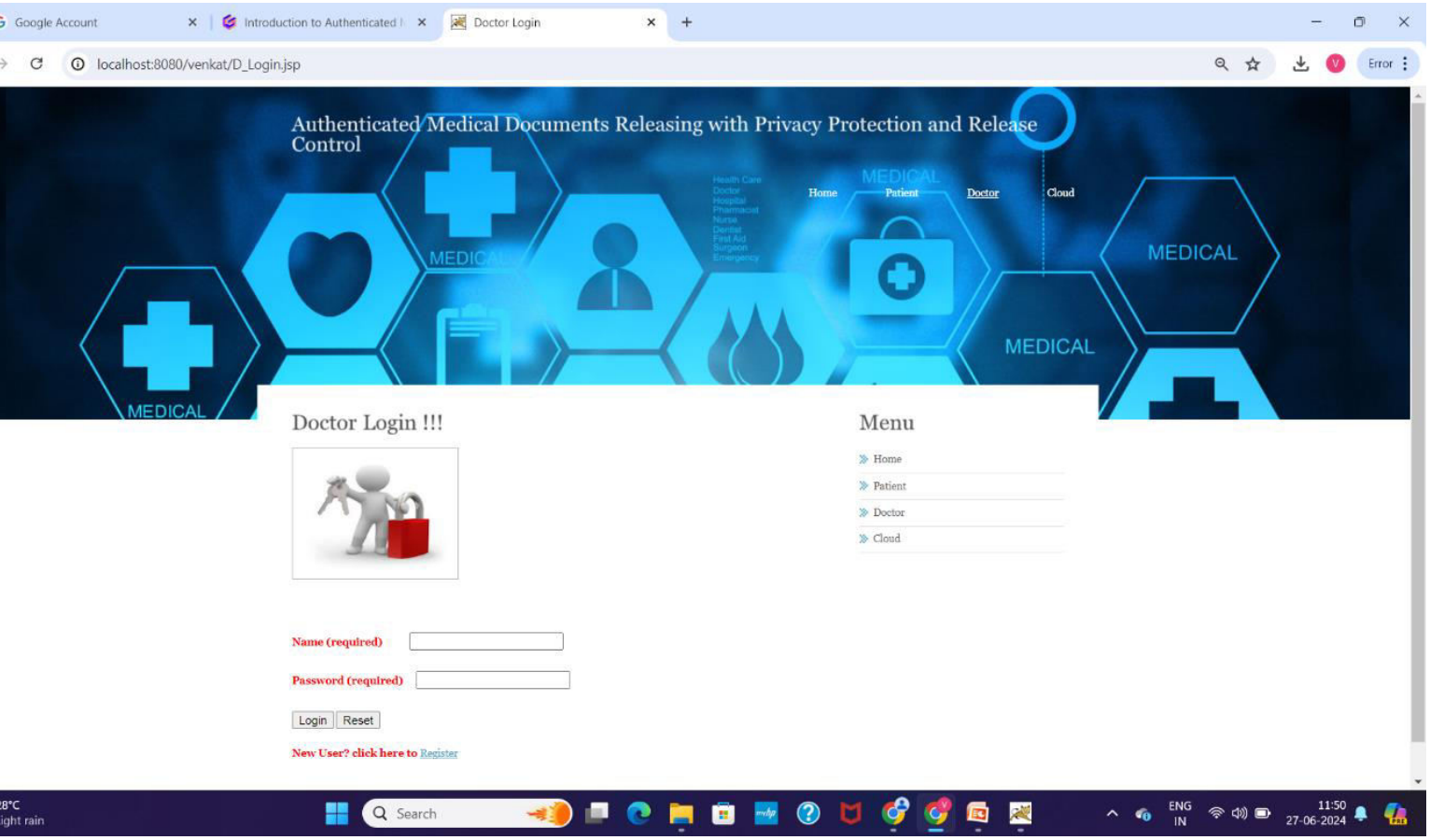
HOME PAGE:-


Google Account
Introduction to Authenticated
Home Page
localhost:8080/venkat/index.html
Error
Authenticated Medical Documents Releasing with Privacy Protection and Release Control
Home
Patient
Hospital
Research Cloud Server
Healthcare Provider
Insurance Company
MEDICAL
Introduction
Menu
Home
Patient
Doctor
Cloud Server
Healthcare Provider
Insurance Company
Concepts
Medical document release,
privacy preservation,
In the context of Information Societies, a tremendous amount of information is daily exchanged or released. Among various information-release cases, medical document release has gained significant attention for its potential in improving healthcare service quality and efficacy. However, integrity and origin authentication of released medical documents is the priority in subsequent applications.
28°C
Light rain
Search
ENG
IN
11:50
27-06-2024

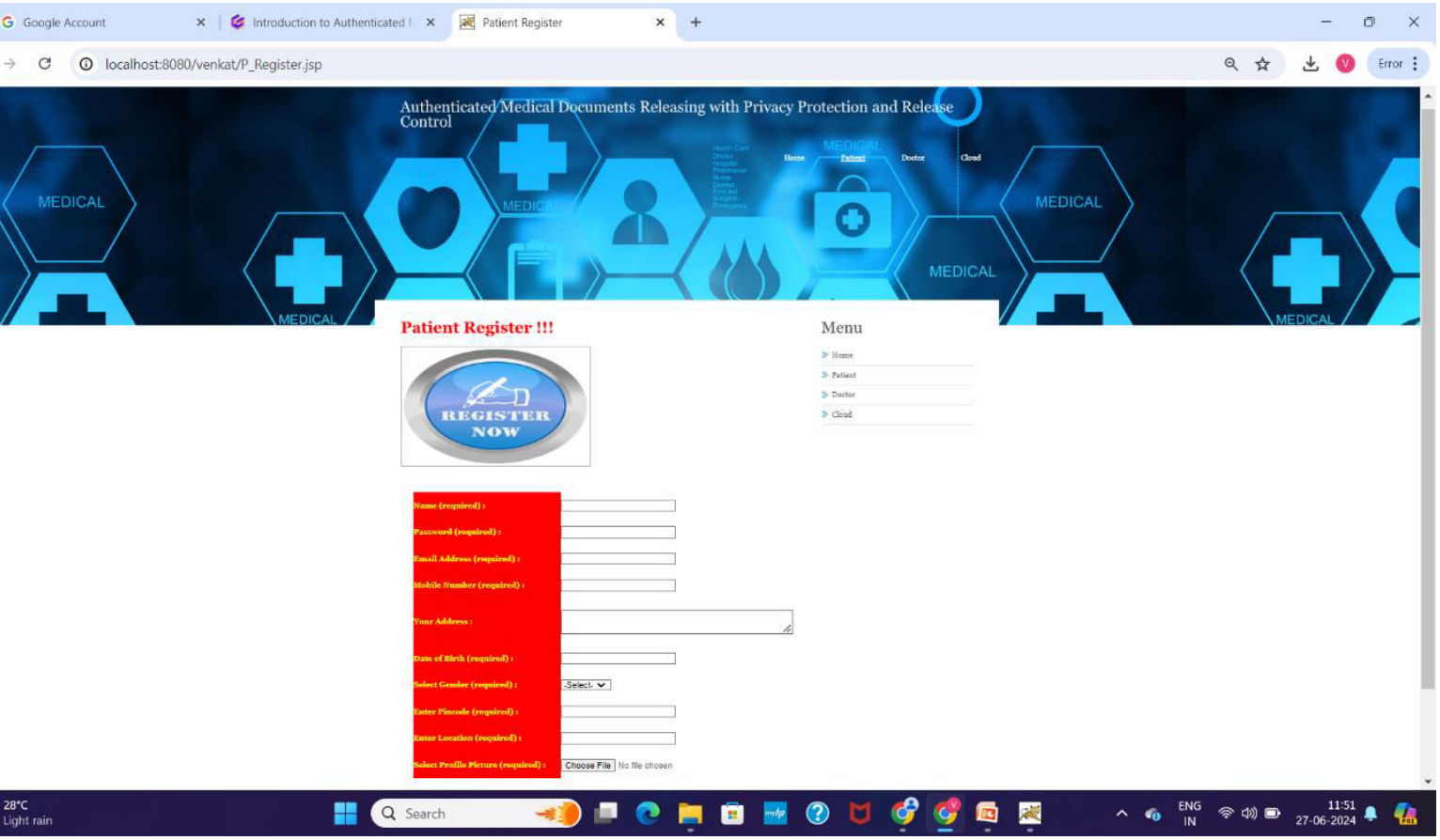
PATIENT LOGIN PAGE:-



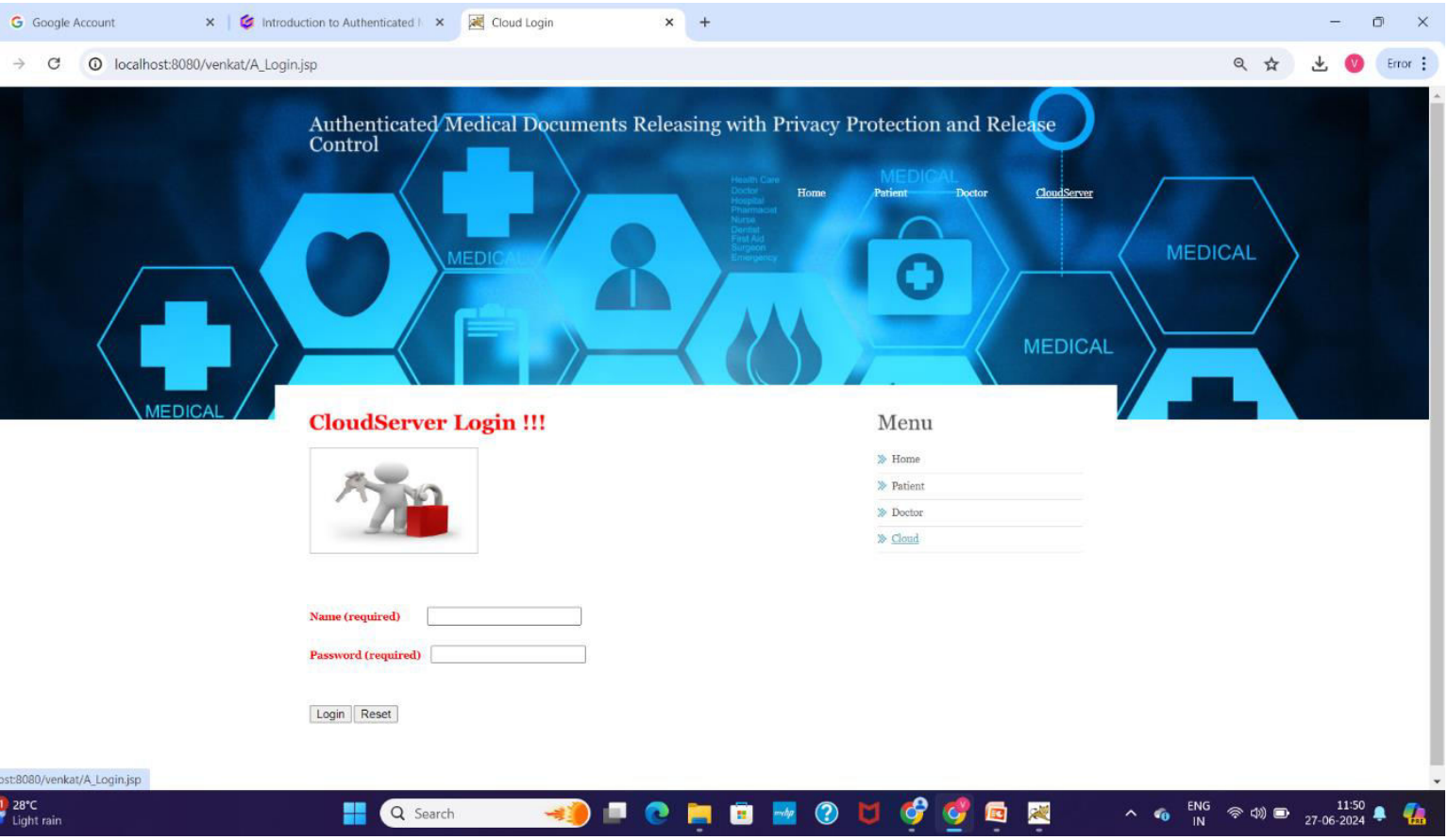
DOCTOR LOGIN PAGE:-



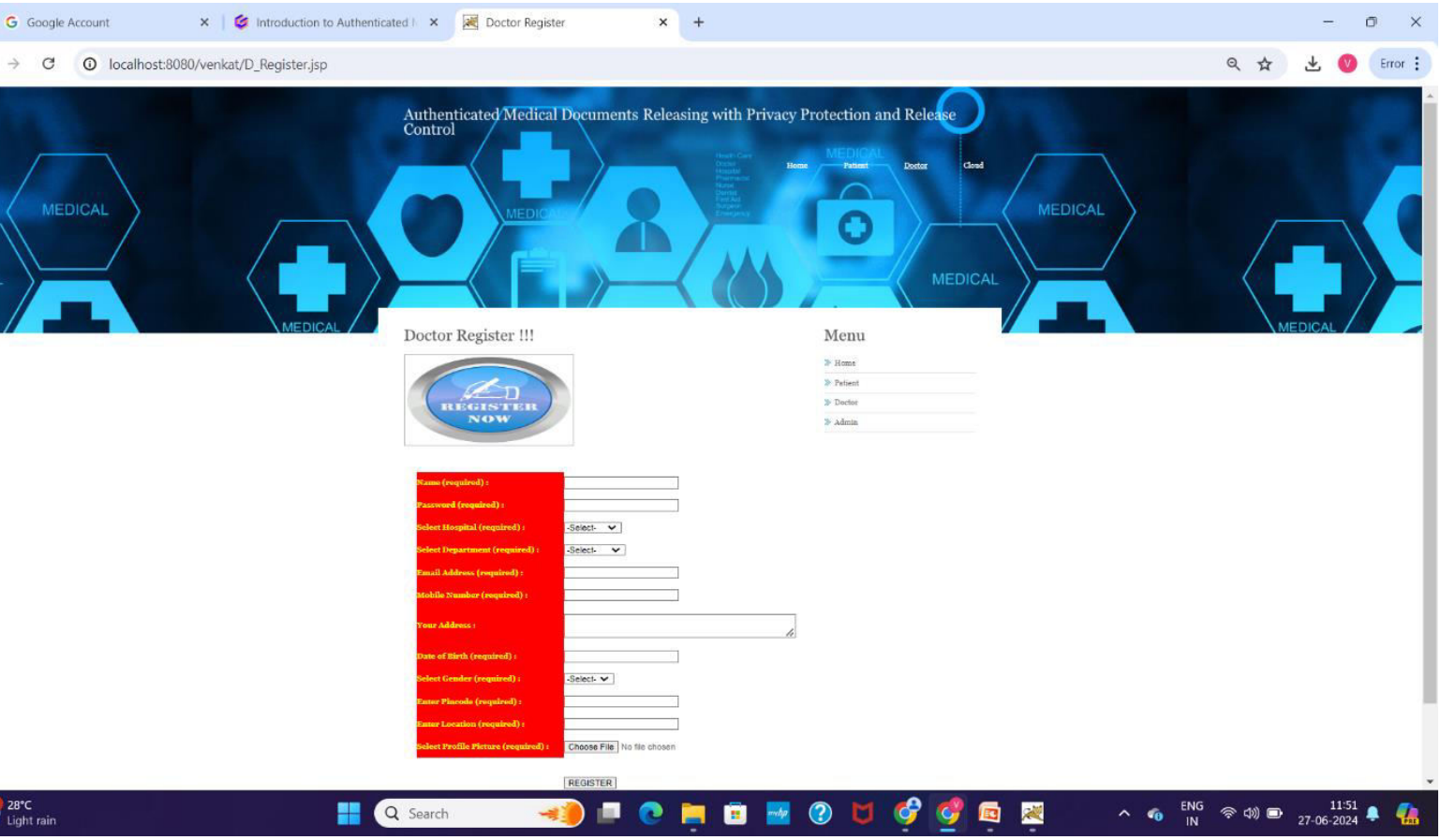
PATIENT REGISTER PAGE:-



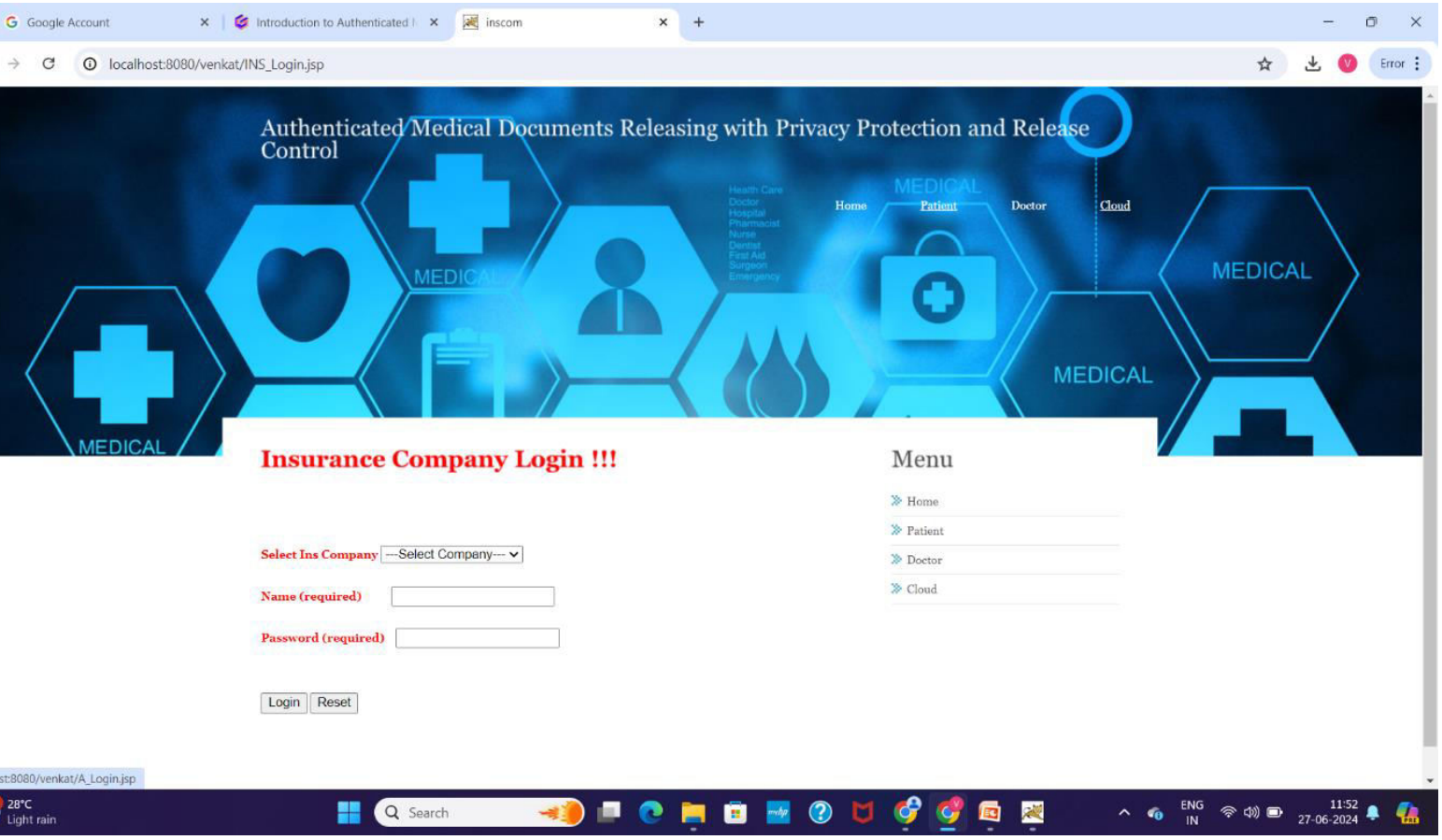
CLOUD SERVER LOGIN PAGE:-



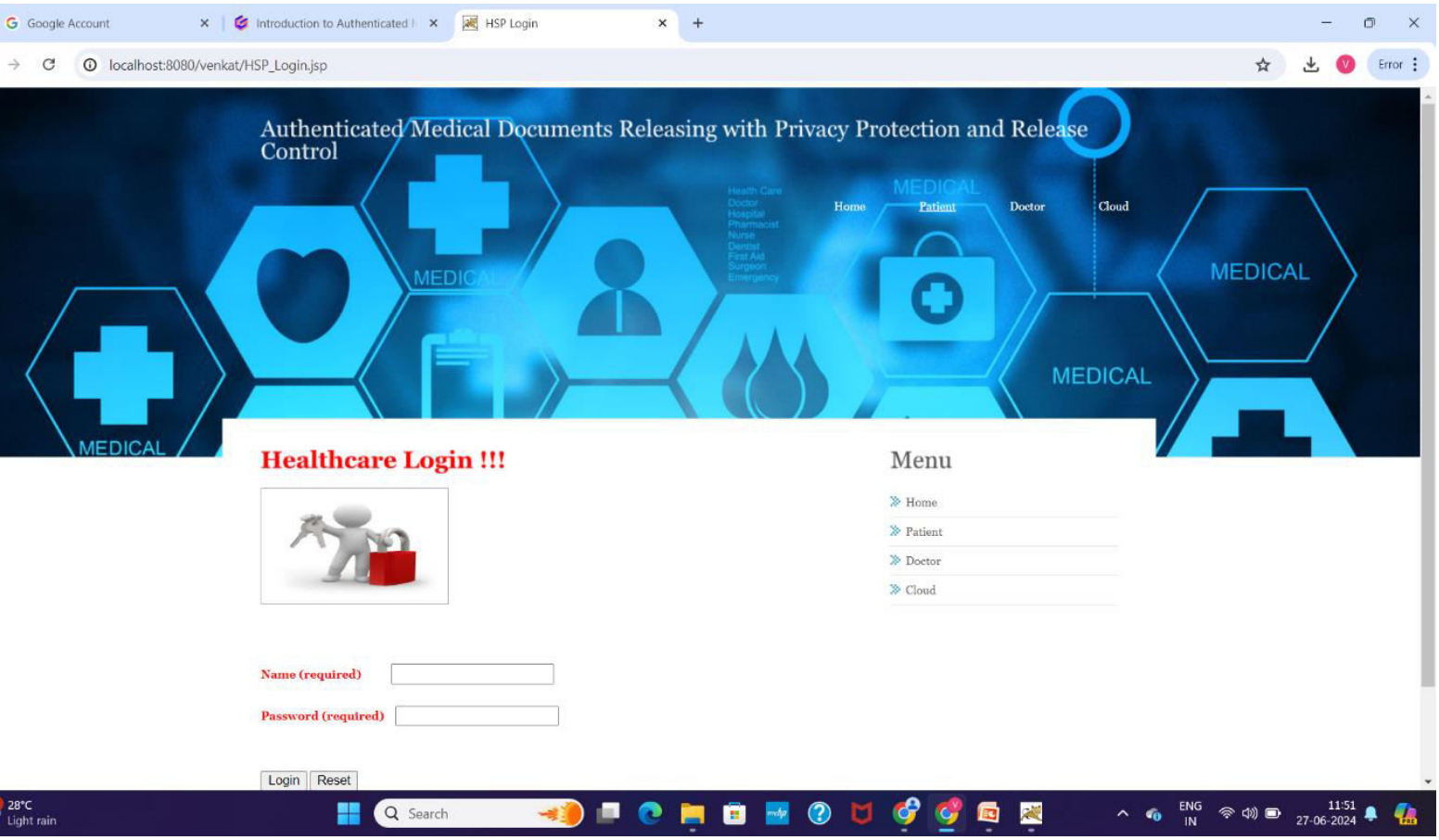
DOCTOR REGISTER PAGE:-



INSURANCE COMPANY LOGIN PAGE:-



HEALTHCARE LOGIN PAGE:-



In this paper, we introduced two constructions of RSSs-FRC with a different flexibility of release control mechanisms to resolve the privacy preservation and release control issues in releasing authenticated medical documents. The RSSs-FRC1 construction allows the signer to specify a minimum number of subdocument blocks that the redactor has to release, while the RSSs-FRC2 construction also empowers signer to regulate the dependence of revealable subdocument blocks.

Our constructions not only prevent the dishonest release from redacting document unrestrictedly but also have the ability to detect illegal redaction by the verifier. Furthermore, the two proposed RSSs-FRC also support multiple redaction manipulations providing the released subdocument is authorized by the signer. Finally, we presented the security proof and efficiency analysis for our RSSs-FRC. For future work, we plan to explore RSSs with redactor accountability for privacy-preserving release of authenticated medical documents.

7. REFRENCES

[1] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, "Verifiable computation over large database with incremental updates," IEEE transactions on Computers, vol. 65, no. 10, pp. 3184–3195, 2016.

[2] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, "New publicly verifiable databases with efficient updates," IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 5, pp. 546–556, 2015.

[3] X. Chen, X. Huang, J. Li, J. Ma, W. Lou, and D. S. Wong, "New algorithms for secure outsourcing of large-scale systems of linear equations," IEEE transactions on information forensics and security, vol. 10, no. 1, pp. 69–78, 2015.

[4] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms for secure outsourcing of modular exponentiations," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 9, pp. 2386–2396, 2014.

[5] J. Wang, X. Chen, X. Huang, I. You, and Y. Xiang, "Verifiable auditing for outsourced database in cloud computing," IEEE transactions on computers, no. 1, pp. 1–1, 2015.

[6] T. Jiang, X. Chen, and J. Ma, "Public integrity auditing for shared dynamic cloud data with group user revocation," IEEE Transactions on Computers, vol. 65, no. 8, pp. 2363–2373, 2016.

[7] X. Zhang, T. Jiang, K.-C. Li, A. Castiglione, and X. Chen, "New publicly verifiable computation for batch matrix multiplication," Information Sciences, 2017.

[8] R. Johnson, D. Molnar, D. Song, and D. Wagner, "Homomorphic signature schemes," in Cryptographers' Track at the RSA Conference. Springer, 2002, pp. 244–262.

[9] G. Becker, "Merkle signature schemes, merkle trees and their cryptanalysis," Online im Internet: http://imperia.rz.rub.de, vol. 9085, 2008.

[10] O. Goldreich, S. Goldwasser, and S. Micali, "How to construct random functions," Journal of the ACM (JACM), vol. 33, no. 4, pp. 792–807, 1986.