SECURE, ID PRIVACY AND INFERENCE THREAT PREVENTION MECHANISMS FOR DISTRIBUTED SYSTEMS

[1]Kohila R, [2]Sathiyapriya P, [3]P Srikanth, [4]R Sidda Reddy, [5]K Deepak Reddy

[1,2]Assistant Professor, Department of CSE(Cyber Security), Muthayammal Engineering College.

[3,4,5]Student, Department of CSE(Cyber Security), Muthayammal Engineering College.

[1]kohilamca@gmail.com, [2]sathiyapriya18mec@gmail.com, [3]srikanthputta9999@gmail.com, [4]rajulasiddareddy9193@gmail.com, [5]deepakreddy2811@gmail.com

ABSTRACT - This paper investigates facilitating remote collection of a patient's data in distributed system while protecting the security of the data, preserving the privacy of the patient's ID, and preventing inference attack. The paper presents a novel framework called SPID stand for a Secure, ID Privacy, and Inference Threat Prevention Mechanisms for Distributed Systems. In designing this framework, we make the following novel contributions. The SPID presents a novel architecture that supports the use of a distributed set of servers owned by different service providers. The SPID allows the patient to access these servers using certificates generated by the patient. The SPID allows the patient to select one server to be the home server, and select a number of servers to be the foreign servers. The patient uses the foreign servers to upload data. The home server is responsible for collecting the patient's data from the foreign servers and sending them to the healthcare provider.

KEYWORDS - Distributed Systems, Identity Privacy, Inference Attack Prevention, Privacy-Preserving Authentication, Cryptographic Security, Elliptic Curve Cryptography.

1. INTRODUCTION

The The Internet of Things (IoT) can be defined as the paradigm of connecting smart things (e.g. sensors, devices) together by means of information and communication technologies to build intelligent systems and services to obtain required information. The smart things can sense the surrounding environment and communicate with each other to exchange information. These features (i.e. sensing and communicating) facilitate many emerging attractive applications. One of these applications is Patient Health Monitoring (PHM) systems. A PHM system involves the use of mobile computing and wireless communication technologies to regularly collect data from a patient for the purpose of analyzing the patient's health and making health-related decisions [1], [2]. A typical PHM system, as shown in Figure 1, consists of

body sensors and a mobile or fixed device at the patient's end (e.g. home) and remote servers at the healthcare provider's end. The body sensors worn by the patient are connected wirelessly to the device that is, in turn, connected to the servers via wireless and/or wired networks. The health related data (e.g. heart rate, blood pressure, etc) collected by the body sensors are sent to the device, which are then delivered to the healthcare provider for further analysis and decision making.

1.1 SCOPE OF THIS PROJECT

This project aims to:

- Develop a secure framework for identity privacy and inference threat prevention in distributed systems.
- Implement a privacy-preserving SPID architecture using multiple service providers.
- Apply Protect user identities through pseudonyms and anonymous authentication.
- Prevent inference attacks by distributing and rotating data upload servers.
- Ensure data confidentiality, integrity, and authenticity using cryptographic techniques.
- Support secure data aggregation and transmission in distributed environments.

2. PROPOSED WORK

The proposed system aims to support clinicians, researchers, and healthcare institutions by improving diagnostic accuracy and enhancing screening efficiency for colorectal cancer.

With the increasing adoption of artificial intelligence in medical imaging, numerous studies have investigated AI-based techniques for colorectal cancer detection and classification.

In particular, recent research has demonstrated that deep learning approaches, especially Convolutional Neural Networks (CNNs), significantly outperform traditional machine learning methods by automatically learning discriminative features directly from endoscopic image data.

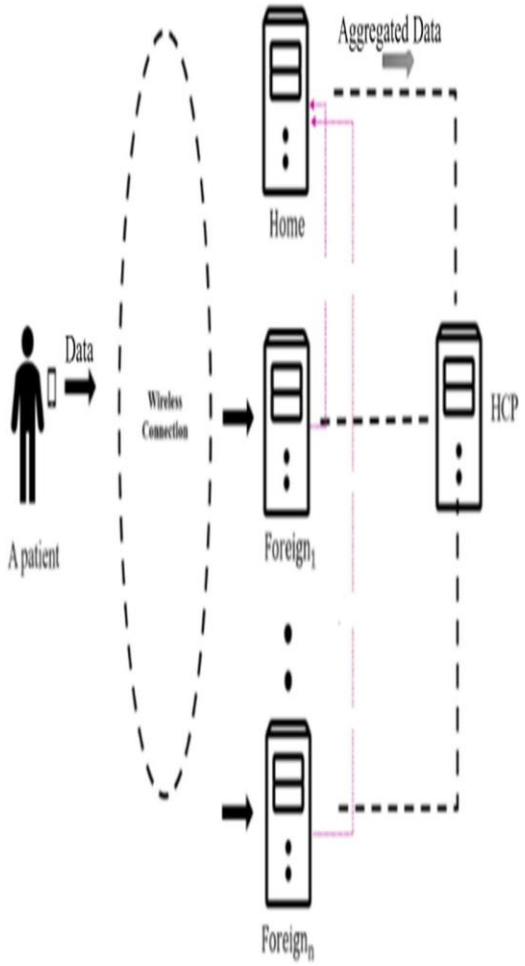
Despite their success, many existing deep learning models suffer from high computational complexity, limiting their applicability in real-time clinical environments.

This paper proposes an AI-driven framework for automated colorectal cancer classification using endoscopic images.

The Sequential CNN architecture is designed to efficiently capture spatial and texture-based features relevant to cancer detection while maintaining low inference latency.

The proposed framework assists clinicians by providing accurate and consistent predictions, thereby reducing reliance on interpretation and inter-observer variability.

2.1 System Architecture



3.1 Data Processing & Preprocessing

To ensure secure data handling, identity privacy preservation, and effective inference threat prevention in distributed systems framework incorporates the following data processing and preprocessing steps:

- **Image Secure Data Collection:** Collects sensitive data from distributed environments using multiple authorized service providers.
- **Encrypted Data Input:** Encrypts and signs raw data before transmission to ensure confidentiality and integrity.
- **Identity Anonymization:** Generates pseudonyms and privacy-preserving certificates to protect user identity.
- **Distributed Data Storage:** Uploads encrypted data to dynamically selected foreign servers.
- **Secure Data Delivery:** Transfers aggregated and verified data to the healthcare provider for authorized analysis and decision-making without disclosing identity.

3.2 SPID-Based Secure Data Collection and Privacy Preservation

3.2.1 Secure Identity Privacy and Authentication Mechanism:

The SPID module uses a distributed authentication approach with pseudonym-based identities and patient-generated certificates to ensure secure access while preserving identity privacy. Elliptic Curve Cryptography (ECC) enables efficient request verification without database lookups, ensuring data confidentiality and authenticity.

3.2.2 Inference Threat Prevention and Secure Data Aggregation Deployment:

Encrypted patient data is distributed across multiple service providers to prevent inference attacks based on access patterns. A home server aggregates data from foreign servers and forwards it securely to the healthcare provider. System performance and inference resistance are evaluated using benchmarking, queuing theory, and Shannon entropy.

3.3 TOOLS AND LIBRARIES

The SPID framework uses the following tools and technologies:

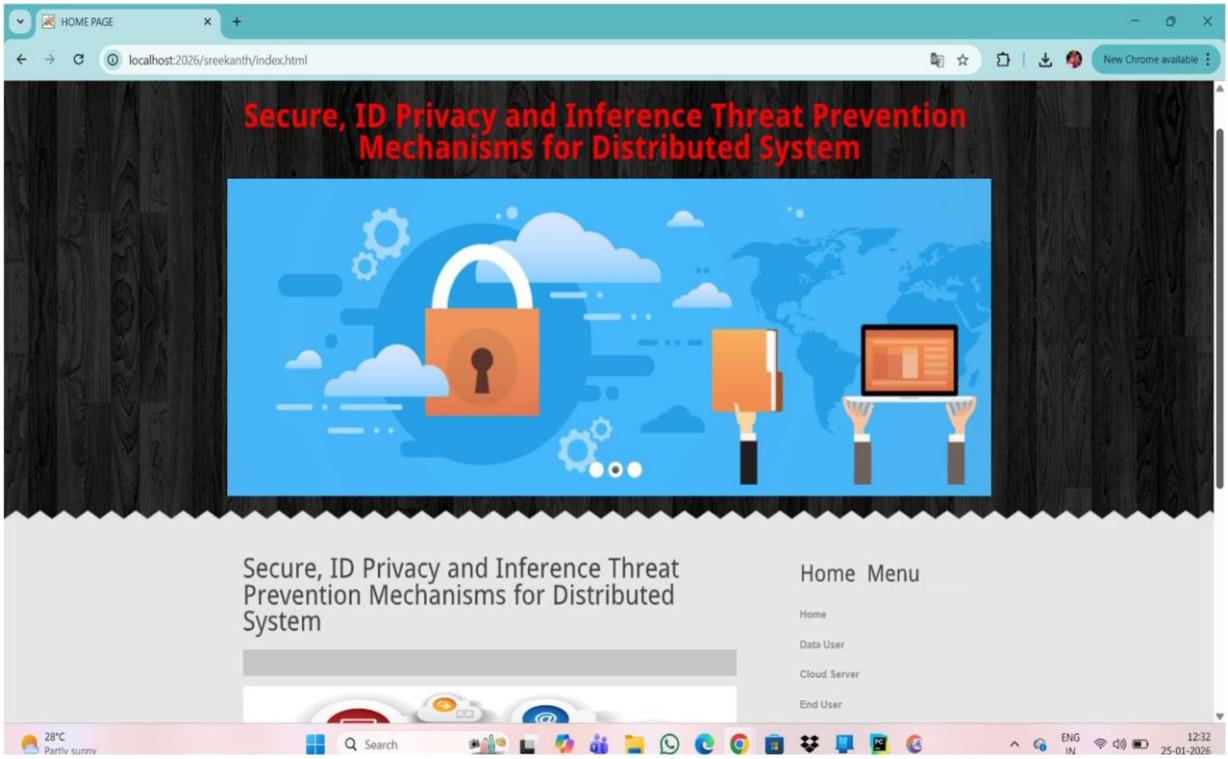
- **Java / J2EE:** Core programming platform for system implementation.
- **Elliptic Curve Cryptography (ECC):** Used for secure authentication and key management.
- **MySQL:** Backend database for storing encrypted data and system records.
- **Apache Tomcat**: Application server for deploying web-based modules.
- **Queuing Theory:** Used for performance evaluation and scalability analysis.
- **Shannon Entropy:** Measures anonymity and inference attack resistance.
- **Swarming Algorithm:** Distributes data uploads across multiple servers.

4. PROGRAM

```
<title>Owner Registration</title>
<%@page import="com.oreilly.servlet.*,java.sql.*,java.lang.*,java.text.SimpleDateFormat,java.util.*,java.io.*,javax.servlet.*,javax.servlet
<%@ page import="java.sql.*"%>
<%@ include file="connect.jsp" %>
<%@ page import="java.util.Date" %>


<%
        ArrayList list = new ArrayList();
        ServletContext context = getServletContext();
        String dirName =context.getRealPath("Gallery\\");
        String paramname=null;
        String file=null;
        String a=null,b=null,c=null,d=null,image=null;
        String ee[]=null;
        String checkBok=" ";
        int ff=0;
        String bin = "";
        String uname=null;
        String pass=null;
        String email=null;
        String mno=null;
        String addr=null;
        String dob=null;
        String location=null;
        String sk="Rejected";
        String gender=null;
        String pincode=null;
```

5. RESULTS AND OUTPUT



The system analyzes user authentication requests and data transmission patterns across distributed service providers to ensure security and privacy.

- **Disease Threat Detection Result:** The framework successfully verifies user authenticity while preserving pseudonymous identity across multiple service providers.
- **Precautionary Privacy Protection Outcome:** Prevents identity disclosure and linkage by dynamically distributing encrypted data uploads, mitigating inference and traffic-pattern attacks.
- **Security Assurance Output:** Ensures data confidentiality, integrity, and secure aggregation using cryptographic mechanisms before forwarding data to the healthcare provider.
- **Decision Support:** Provides secure and privacy-preserving support for distributed data collection, enabling reliable analysis and decision-making without exposing sensitive user identities.

6. CONCLUSION

To protect the security and ID privacy in data collection distributed system we designed a secure anonymous data collection framework called SPID. The proposed framework has advantages of using multiple service providers to collect a patient's data to prevent a single provider from inferring the patient's identity based on the pattern of interactions, allow the patient to generate pseudonym identities and certificates to access these service providers, and allow each patient's home service provider for anonymously linking the patient's data which are scattered across different foreign service providers.

REFERENCES

[1] K. T. Kadhim, A. M. Alsahlany, S. M. Wadi, and H. T. Kadhum, "An overview of patient's health status monitoring system based on internet of things (iot)," Wireless Personal Communications, pp. 1–28, 2020.

[2] S. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The internet of things for health care: a comprehensive survey," IEEE Access, vol. 3, pp. 678–708, 2015.

[3] G. Paliwal and A. W. Kiwelekar, "A comparison of mobile patient monitoring systems," in International Conference on Health Information Science. Springer, 2013, pp. 198–209.

[4] P. Pawar, V. Jones, B.-J. F. Van Bejmin and H. Hermens, "A framework for the comparison of mobile patient monitoring systems," Journal of biomedical informatics, vol. 45, no. 3, pp. 544–556, 2012.

[5] M. reporter, "The nhs is about to take an 'important' step into the cloud, says microsoft," Jan. 2018.

[6] P. Kakria, N. Tripathi, and P. Kitipawang, "A real-time health monitoring system for remote cardiac patients using smartphone and wearable sensors," International journal of telemedicine and applications, vol. 2015, p. 8, 2015.

[7] J. Lopez and R. Dahab, "An overview of elliptic curve cryptography," 2000.

[8] W. Tang, K. Zhang, D. Zhang, J. Ren, Y. Zhang, and X. S. Shen, "Fogenabled smart health: Toward cooperative and secure healthcare service provision," IEEE Communications Magazine, vol. 57, no. 5, pp. 42–48, 2019.

[9] J. H. Abawajy and M. M. Hassan, "Federated internet of things and cloud computing pervasive patient health monitoring system," IEEE Communications Magazine, vol. 55, no. 1, pp. 48–53, 2017.