QLink: A Secure IoT-Integrated System for RFID-Based Document Access and Cloud-Enabled Sharing via URL Shortening Services

Priyansh Neel[1], Shaily Giri[2]

[1]Department of Computer Science, SRM Institute of Science and Technology Delhi-NCR Campus Modinagar, Ghaziabad, Uttar Pradesh, India

[2]Department of Electronics and Communications Engineering, SRM Institute of Science and Technology, SRM Nagar, Kattankulathur, Chengalpattu District, Tamil Nadu, India

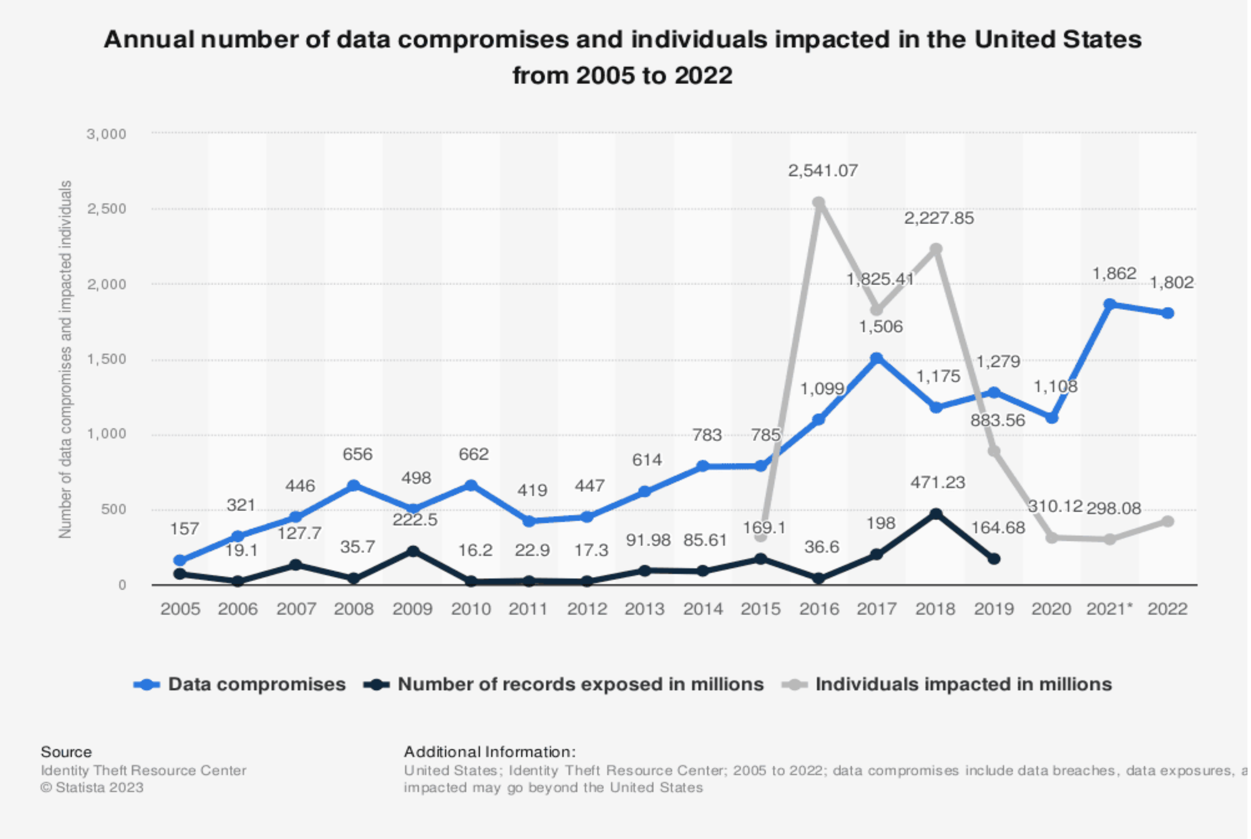
Abstract

Secure and efficient document distribution remains a significant challenge in organizations where identity-based access is critical. Manual sharing methods are prone to human error, unauthorized access, and lack contextual automation. This becomes especially problematic in time-sensitive and identity-dependent environments like academic institutions or field-level deployments. This paper introduces **QLink**, a lightweight, RFID-enabled document access system designed to link physical identities with digital files stored securely in the cloud. The aim is to streamline access control using affordable hardware and real-time server-side integration.

Keywords: *RFID, IoT, Cloud Storage, Secure Document Access, AWS S3, URL Shortening, Node.js, Express.js, Information Security.*

1 Background

In an increasingly digital world, the need for secure, efficient, and user-friendly mechanisms for document sharing has become more critical than ever. With data breaches and cyberattacks on the rise, traditional file-sharing platforms often fall short in addressing the growing concerns of data privacy, access control, and traceability. According to a 2024 Statista report, over 422 million data records were exposed globally due to unauthorized document access and insecure sharing methods. In highly regulated environments such as government offices, corporate HR departments, educational institutions, and medical facilities secure document handling isn't just a matter of convenience but a legal and ethical obligation. One of the critical challenges lies in verifying and validating the identity of individuals requesting access to sensitive information. While many platforms offer encrypted storage, few provide physical verification coupled with digital authorization, making them vulnerable to phishing links, leaked URLs, and unauthorized downloads. To address these gaps, we propose QLink, a novel, RFID-backed secure document-sharing system that integrates physical verification via RFID scanning with encrypted cloud-based storage using Amazon Web Services (AWS S3). The system generates time-bound, shortened URLs using a secure Node.js-based backend. This hybrid approach ensures that access to sensitive documents is only granted after real-world RFID-based identification, significantly reducing the possibility of digital impersonation or unauthorized access. Furthermore, URL shortening with expiration controls ensures that shared links cannot be reused, leaked, or exploited beyond their intended time frame or user. The growing demand for context-aware, location-sensitive document access (such as university campuses, hospitals, or corporate branches) further necessitates such intelligent, user-verified systems. By combining cloud storage, RFID authentication, and smart link generation, QLink represents a modern approach to solving a real-world problem at the intersection of cybersecurity, physical authentication, and cloud computing.


Annual number of data compromises and individuals impacted in the United States from 2005 to 2022

Source
Identity Theft Resource Center
© Statista 2023

Additional Information:
United States; Identity Theft Resource Center; 2005 to 2022; data compromises include data breaches, data exposures, a
impacted may go beyond the United States

Fig. 1. Data Breach over the years in United States from 2005 to 2022

Unauthorized access to confidential information such as personal details, financial records, intellectual assets, or proprietary business data is referred to as a data breach. Over time, these breaches have evolved in complexity, with cyber attackers deploying more advanced methods to infiltrate security defenses and extract sensitive data. Common tactics include the use of malicious software, deceptive phishing schemes, and psychological manipulation to obtain user credentials or system access. The impact of such breaches can be highly damaging for both individuals and organizations. On a personal level, compromised information can lead to identity fraud, financial setbacks, and a decline in credit ratings. For businesses, the fallout may include significant reputational harm, customer trust erosion, financial losses, and potential legal consequences.

2 Methods

2.1 Approach Overview