IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

# Eliminating Credential Risk: A Lightweight Data Access System For Public Devices

**Sneha Pandey and Nikhil Chauhan**
Department of Computer Science & Engineering
Dronacharya College of Engineering Gurugram, Haryana

**Abstract:** *Nowadays, using typical email-based logins to access confidential documents can result in significant security and privacy breaches in settings where users depend on public or untrusted systems, such as internships, campus placements, and external collaborations. This paper suggests a login-free web-based solution which is secure, and lightweight for temporary data exchange between trusted sender and untrusted receiver devices. In order to guarantee that only the intended receivers can read the data, and only within a restricted window, the system uses an OTP-based secure session-pairing technique that instantly connects a trustworthy sender device and an untrusted receiver device without the need for link sharing or permanent credentials. By limiting default access and personally validating each request, the architecture adheres to the principles of Zero Trust Security. In future, for enhanced data confidentiality, use of protocols such as AES and RSA is proposed to secure real-time communication between the devices. The application, which was created with Express.js and React.js, provides a way to safely share test links, training materials, and onboarding paperwork, particularly in corporate and educational settings. Extensions like Redis-powered session control, blockchain logging for traceability, and QR code-based access are planned*

**Keywords:** Secure Data Transfer, Zero Trust Security, OTP-based session-pairing technique, AES/RSA Encryption, Data Confidentiality, Public Computer Security, Corporate / Educational Data Sharing

## I. INTRODUCTION

The necessity for temporary and secure data sharing has grown in importance in today's digitally connected contexts, especially when users are forced to rely on public or untrusted services. Confidential information like exam links, identity documents, and training materials are frequently shared in common scenarios including internships, university placements, digital onboarding, and cooperative academic projects. This communication has historically relied on cloud storage links or email-based systems, which not only cause delays and annoyance but also put users at risk for persistent data trails, session hijacking, and unwanted access.

When users must access sensitive material on shared or public computers—like those in labs, libraries, cyber cafes, or placement centers—there is a serious risk. These systems might not be adequately secured and could be exploited.

Traditional email-based techniques that expose users to privacy violations, session hijacking, and data persistence hazards are frequently used when accessing sensitive documents through public or untrusted systems, such as during internships, university placements, or cooperative academic assignments. These techniques usually demand for login information on shared computers, which goes against security best practices and leaves users vulnerable to illegal access and credential leaks.

In order to address this, we suggest a web-based, login-free solution that permits safe, transient communication between an untrusted receiver device (such as a public computer) and a trustworthy sender device (such as a personal smartphone). Without requiring links, emails, or permanent credentials, the system establishes a brief connection using an OTP-based session-pairing technique. The architecture was created with React.js and Express.js and adheres to Zero Trust guidelines also offers a safe and convenient substitute for sensitive data transfer by supporting the future inclusion of AES/RSA encryption, Redis-powered session handling, and QR code-based access.


DOI: 10.48175/IJARSCT-25689

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

## II. OVERVIEW

Without requiring user login, email access, or long-term data storage, the suggested solution is a safe web-based application that permits one-time, transient communication between a trusted sender device and an untrusted receiver device. The application, which was created specifically for use in situations requiring public or shared systems—like internship centers, placement laboratories, or co-working spaces—enables users to safely communicate private data in real time, such as documents, onboarding materials, or test links.

The core flow of the system works as follows:

- The sender initiates a session from their device by entering their name and selecting a session expiry time.
- The system generates a secure, short-lived **OTP or token**.
- The receiver accesses the same website on a public system, enters their name and the shared OTP.
- Upon verification, both devices are connected to a common **real-time chat interface** using WebSockets, allowing controlled, session-based data exchange.
- Once the session expires or is manually terminated, all data is deleted from the server to ensure privacy.

The foundation of the entire communication model is Zero Trust Security, which verifies each session separately and does not assume that any device is trustworthy. While basic session integrity is guaranteed by the existing system, planned enhancements include RSA key exchange for hybrid encryption, Redis for session management, AES encryption for message security, and QR code login for ease of use. For a variety of corporate and educational settings, these enable the solution to be scalable and flexible.

## III. USE CASES

At co-working spaces, educators, professionals, or collaborators may need to share temporary resources without leaving digital footprints; during internships or campus placements, students are frequently asked to access onboarding documents or test links on public computers, putting their privacy and account security at risk. The proposed system finds strong relevance in scenarios where users need to access sensitive data on untrusted or shared devices without compromising their personal credentials. This application offers a secure, login-free alternative to traditional email-based transfers, making it ideal for short-lived, high-trust communications across untrusted systems.

### 3.1 Internships and Onboarding

Companies frequently distribute confidential papers, such as offer letters, training materials, and internal guidelines, throughout the onboarding process for internships and jobs. Accessing emails or cloud links poses concerns for interns, particularly when utilizing shared systems in college labs or internet cafés. This technology reduces vulnerability to phishing and credential breaches by enabling businesses to safely transmit such papers through a one-time session, eschewing login-based alternatives.

### 3.2 Campus Placement Drive

Students are regularly asked to browse test links on public computers or enter into company websites during campus placements. Concerns around data misuse and credential theft are raised by this. With the help of a one-time OTP created on their phones, students can access exam instructions or temporary files on public systems using the suggested method, which guarantees access control, session expiration, and no trace is left behind.

### 3.3 Co-working Spaces and Shared Offices

Professionals may need to safely move temporary data to devices that are not theirs in co-working spaces or shared workplace settings. They can use this application to create a secure, OTP-based session and exchange files or instructions without leaving any lasting traces on the recipient's computer, as an alternative to emailing themselves or using USB devices.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

### 3.4 Educational Collaborations and Workshops

Teachers and workshop instructors frequently use public lab systems to exchange project materials, assignments, and comments with students. This solution provides a session-bound, safer way to send such files without the need for manually typed URLs, cloud drives, or email logins.

## IV. RELATED WORK

Several Secure data access has been investigated by a number of current methodologies, particularly when it comes to public networks and untrusted devices. The move from conventional perimeter-based defenses to **Zero Trust Security** models is one of the biggest changes in contemporary cybersecurity.

The **National Institute of Standards and Technology (NIST)** formally introduced the Zero Trust Architecture (ZTA) in its *Special Publication 800-207*, where it emphasizes "never trust, always verify" as the core principle. This architecture mandates continuous authentication, minimal implicit trust, and strict identity-based access control, even within an organization's internal network [1]. Our system reflects these principles by not assuming any default trust and requiring real-time OTP verification for each session, without relying on permanent credentials or logged-in accounts.

A detailed survey titled **"Theory and Application of Zero Trust Security"** explores how the Zero Trust model can be extended to cloud platforms, enterprise systems, and public environments. It highlights how ephemeral sessions, minimal access permissions, and continuous validation help in securing communications on untrusted infrastructure [2]. Inspired by these insights, our system leverages session-based pairing and auto-destruct timers to ensure temporal and scoped data access.

**Gupta et al. (2022)** in their study titled *"Zero Trust Architecture: Trend and Impact on Information Security"* examined how Zero Trust strategies outperform VPN and traditional firewall systems in environments where insider threats or shared device usage is common. Their work supports the design choice in our application of completely avoiding persistent credentials and instead focusing on single-session, use-once tokens for controlled access [3].

In **"Zero Trust: Applications, Challenges, and Opportunities"**, the authors provide a comprehensive overview of how Zero Trust can be integrated with modern technologies like blockchain and AI for traceability, dynamic authentication, and breach response [4]. Our suggested future improvements, such Redis-powered session tracking and blockchain-based activity recording, are inspired by this work and seek to further protect the system from abuse while preserving user ease.

These earlier efforts collectively lay the groundwork for scalable, secure systems that can operate dependably even on devices that are not trusted. Our method bridges the gap between theoretical models and workable lightweight solutions by applying these concepts to a novel use-case scenario: transitory data transfer during internships, test submissions, and onboarding.

## V. SYSTEM ARCHITECHTURE

The system uses a secure, session-based communication mechanism and is built as a client-server web application. The two main user roles are Receiver (an untrusted device, typically a public computer) and Sender (a trusted device, like a phone). They can join using an OTP-based handshake and securely interact during a brief session thanks to the architecture.

Following are the key components:

### 5.1 Frontend – Next.js

**Next.js** is used to build a fast, responsive, and SEO-friendly frontend interface.

Users can access the app via mobile (sender) or desktop (receiver) without logging in.

The interface offers two roles: "Sender" and "Receiver", each with minimal input requirements.

Communicates securely with the backend via HTTPS and WebSockets.

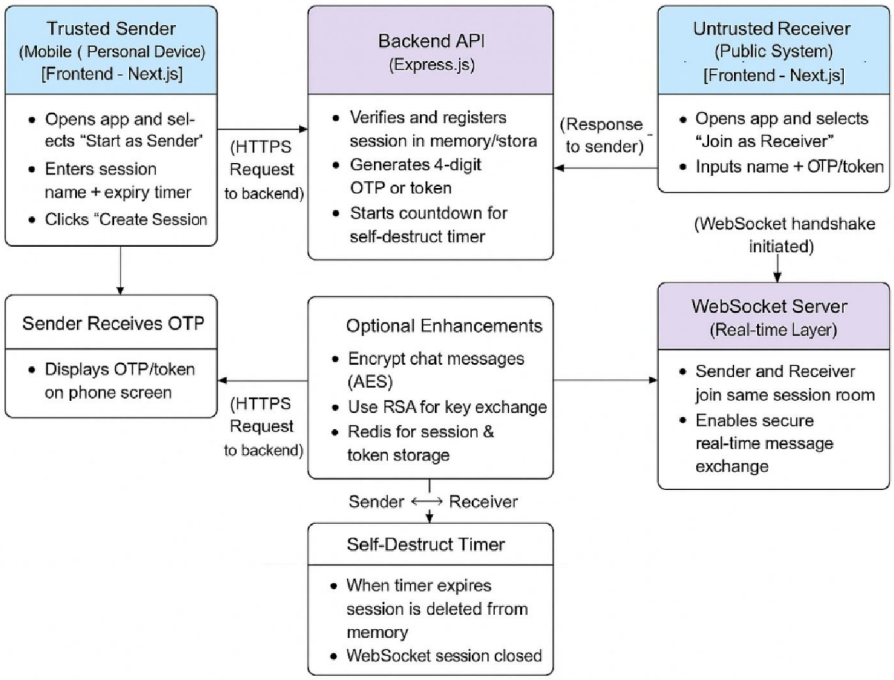
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

### 5.2 Backend – Express.js + WebSocket Server

**Express.js** handles API routes such as session creation, OTP/token generation, and session validation.

A **WebSocket server** manages real-time two-way communication between sender and receiver once the OTP is validated.

Implements session expiry, one-time token checks, and future support for Redis (for session storage) and AES/RSA encryption (for chat security).




### 5.3 Session Management

Each session has:

- A unique session name.
- Self-destruct timer (expiry).
- OTP/token for connection.
- Only the receiver with the correct OTP can access the session, supporting the Zero Trust principle.

### 5.4Security Protocols

Plans to incorporate:

- **AES Encryption** for chat content.
- **RSA Key Exchange** for secure encryption key distribution.
- **Token-based session verification** (currently).
- No emails, passwords, or links — everything is ephemeral and one-time only.

## VI. USER SURVEY & PERCEPTION

To validate the relevance and necessity of a secure, login-free data sharing system, a small-scale user survey was conducted with 7 participants. The aim was to understand user behavior and concerns regarding the use of public computers for accessing personal accounts and transferring data.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

Interestingly, over **70% of respondents admitted to using public or shared devices** to access platforms like Gmail or WhatsApp Web. When asked about their comfort level in entering personal credentials on such devices, a majority indicated feeling **"very uncomfortable"** due to the fear of data leaks or session hijacking. Additionally, some users even confessed to **uncertainty about logging out** after use, highlighting a critical privacy risk.

When questioned about **data-sharing habits between their phone and public computers**, methods such as **WhatsApp, Gmail, USB transfer, or outright avoidance** were mentioned—none of which offer real-time, temporary, and secure communication.

Encouragingly, more than **70% showed strong interest** in using an **OTP-based secure, temporary connection** that doesn't require traditional login credentials. While most users were unaware or unsure about the **Zero Trust Security** model, they showed interest in using a system that **self-destructs sessions post usage** and limits exposure time.

Commonly cited use cases included **internships**, **campus placements**, **cyber café access**, and **friend's or school computers**—validating the project's applicability beyond a single domain. Some participants also added contexts like **online exams** and **shared workspaces** as scenarios needing secure sharing.

This survey underscores a genuine user concern and desire for privacy-conscious tools and affirms the practicality of the proposed solution.

## VII. CONCLUSION

In an era where data privacy and secure communication are paramount, especially in temporary or untrusted digital environments, the need for lightweight and secure data-sharing mechanisms is more relevant than ever. This paper introduced a novel, login-free solution enabling secure, session-based data transfer between a trusted sender and an untrusted receiver device using OTP-based pairing. By eliminating the need for traditional credentials or permanent links, the system mitigates the risk of credential theft, forgotten logouts, and unintended data exposure—challenges commonly faced by users in public or shared computer environments.

Rooted in the principles of Zero Trust Security and supported by encryption techniques like AES and RSA, the proposed system offers an intuitive, real-time solution for sensitive data transfer. The architecture, built on Express.js and Next.js with WebSocket integration, ensures minimal friction and maximum security for users across use cases like internships, campus placements, cyber cafés, and more.

The positive response from initial user surveys further validates the practicality and demand for such a system. Future enhancements—such as QR-based session entry, Redis-powered session control, and blockchain-based traceability—open the door to making this a robust and scalable privacy-first solution.

Ultimately, this project bridges the gap between usability and security in transient digital interactions, offering a foundation that can be extended for wider applications in both educational and corporate settings.

## REFERENCES

**[1].** NIST Special Publication 800-207, *Zero Trust Architecture*, National Institute of Standards and Technology, 2020. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

**[2].** Basu et al., *Theory and Application of Zero Trust Security: A Brief Survey*, PMC, 2023. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10742574/

**[3].** Gupta, A. et al., *Zero Trust Architecture: Trend and Impact on Information Security*, ResearchGate, 2022. https://www.researchgate.net/publication/361758378

**[4].** Fang et al., *Zero Trust: Applications, Challenges, and Opportunities*, arXiv, 2023. https://arxiv.org/abs/2309.03582