

# bradscholars

## Zero Trust Model Implementation Considerations in Financial Institutions: A Proposed Framework

Item Type	Conference paper
Authors	Daah, Clement;Qureshi, Amna;Awan, Irfan
Citation	Daah C, Qureshi A and Irfan A (2023) Zero Trust Model Implementation Considerations in Financial Institutions: A Proposed Framework. In: 10th International Conference on Future Internet of Things and Cloud (FiCloud) Marrakesh, Morocco 14-16 August 2023. IEEE. pp. 71-77.
DOI	<a href="http://doi.org/10.1109/ficloud58648.2023.00019">http://doi.org/10.1109/ficloud58648.2023.00019</a>
Publisher	IEEE
Rights	© 2023 IEEE. Reproduced in accordance with the publisher's self-archiving policy.
Download date	2025-09-26 20:19:32
Link to Item	<a href="https://bradscholars.brad.ac.uk/handle/10454/20415">https://bradscholars.brad.ac.uk/handle/10454/20415</a>

# Zero Trust Model Implementation Considerations in Financial Institutions: A Proposed Framework

Clement Daah  
Faculty of Engineering & Informatics  
University of Bradford  
Bradford, United Kingdom  
cdaah@bradford.ac.uk

Amna Qureshi  
Faculty of Engineering & Informatics  
University of Bradford  
Bradford, United Kingdom  
a.qureshi19@bradford.ac.uk

Irfan Awan  
Faculty of Engineering & Informatics  
University of Bradford  
Bradford, United Kingdom  
i.u.awan@bradford.ac.uk

**Abstract** — The finance industry faces an evolving threat landscape and increasing regulatory obligations, necessitating a comprehensive security framework. This paper proposes implementing the Zero Trust model in financial institutions, focusing on data protection, Identity and Access Management (IAM), and device and network security. The framework is evaluated through the development of a demo bank app, and its effectiveness in addressing security challenges is discussed. The IAM component demonstrates robust authentication and authorization processes, while device and network security measures protect against internal and external threats. Data protection mechanisms ensure the confidentiality and integrity of sensitive information. The implementation highlights strengths in comprehensive coverage and effective integration of security measures. Challenges include integration with legacy systems and managing the user experience. Insights and recommendations are provided. This framework enables financial institutions to establish a robust security framework, mitigating cyber threats and enhancing consumer trust.

**Keywords**— Zero Trust, Identity and Access Management, Device and Network Security, Data Protection, Financial Institution

## I. INTRODUCTION

Banks, credit unions, and insurance companies bear the responsibility of protecting vast amounts of sensitive information and critical infrastructure. While perimeter-based security measures are still necessary and should be built upon, they still need to be improved to sufficiently safeguard these assets against increasingly complex and robust cyber threats. Financial institutions' challenges in securing their networks have been further exacerbated by the increasing interconnectedness of systems, the popularity of cloud computing, and the widespread use of mobile and IoT devices.

The Zero Trust model has become a possible security framework that could help solve these problems by shifting the focus from traditional perimeter-based security to a more all-encompassing and granular approach [1]. The Zero Trust model is based on the principle "never trust, always verify", and it calls for the continuous verification of users, devices, and applications before providing them access to confidential data and resources [2]. The ever-changing nature of today's threats makes this model's more dynamic and adaptable security stance crucial. The finance sector is just one area where Zero Trust is beneficial, according to numerous studies.

This research proposes a tailored Zero Trust framework for financial institutions that emphasises Identity and Access Management (IAM), device and network security, and data protection and addresses the specific challenges these

organisations face in protecting confidential data and vital infrastructure from cyber threats.

The Zero Trust model is a paradigm shift from traditional security approaches, advocating for continuous verification and authentication of users, devices, and applications. By adopting this model, financial institutions can establish a more granular and adaptive security stance, ensuring that only authorised entities can access sensitive resources.

The strengths of the proposed strategy lie in its comprehensive coverage of the Zero Trust model's components and its effective integration of security measures. The framework incorporates strong authentication and authorization processes, robust device and network security mechanisms, and advanced data protection techniques. These strengths empower financial institutions to mitigate cyber threats effectively and maintain critical financial data's confidentiality, integrity, and availability.

This research contributes to advancing secure practises in financial institutions by proposing a tailored Zero Trust framework that addresses their specific challenges. Through practical examples and insights gained from implementing a demo bank app, this study demonstrates the framework's effectiveness.

The remaining part of this paper is organised as follows: Section II discusses the related work. Section III explains the Zero Trust model. Section IV describes the adopted approach and the proposed framework. Section V provides implementation details of the demo bank app, highlighting the technologies and tools used and critical aspects of the implementation and testing approach. Section VI presents the results and discussion, evaluating the framework's effectiveness in addressing security challenges specific to financial institutions, highlighting the challenges encountered during the implementation, and providing insights and recommendations. Finally, Section VII concludes the paper.

This study aims to provide financial institutions with a robust security framework based on the Zero Trust model. By implementing this framework, financial institutions can enhance their security posture, protect sensitive data, and effectively mitigate cyber threats, ultimately increasing consumer confidence in their services.

## II. RELATED WORK

The Zero Trust model has gained significant attention in recent years due to the increasing complexity of cyber threats and the inadequacy of traditional perimeter-based security measures. Several studies have explored the application of the Zero Trust model in various industries, including the finance sector.

In a study by Forrester Research, Kindervag [1] proposed the Zero Trust model as an alternative to traditional perimeter-based security measures. The model is based on the principle "never trust, always verify", and it calls for the continuous verification of users, devices, and applications before providing them access to confidential data and resources. The study emphasised the importance of a comprehensive security framework that includes IAM, device and network security, and data protection.

Tao Chuan et al. [3] suggested a zero-trust architecture implementation technique for small and medium-sized businesses whose partial applications are hosted on cloud servers but require access to the internal network. The Token Generate Centre (TGC), application servers, evaluation servers, and gateways are the primary building blocks of the proposed architecture. The research also emphasised proposing a method that guarantees the security of data exchange between the external network application server and the internal network of small and medium-sized businesses, based on the Zero Trust model.

Furthermore, a Zero Trust framework was suggested for cloud computing by D'Silva et al. [4]. Authentication, authorization, and the application (AAA) server form the backbone of the architecture, serving as the sole intermediary between the proxy server and the application to which access is granted. Zeng et al. [5] suggested security for IoT networks using the Zero Trust security model. Identity-based access control, continuous trust assessment, and dynamic access control are prioritised in the design. Assigning unique digital identifiers to users and network nodes, the model combines these identifiers in real time to construct the access subject.

In a study by Microsoft [6], the company proposed the concept of "assume breach," a key principle of the Zero Trust model. The concept assumes that a breach has already occurred and focuses on preventing lateral movement and limiting the breach's impact. The study also emphasised the importance of continuous monitoring, multi-factor authentication, and adaptive access control.

Much research has been done on the Zero Trust model to stop cyberattacks on modern businesses. For instance, PwC analysed the Zero Trust security approach, which protects bank resources from attackers and secures transactions via a blockchain consensus mechanism, noting that security devices and controls would be implemented to protect the banks' hardware, software, cloud deployments, and other sensitive resources and that all communications would need to be encrypted to prevent "man-in-the-middle" attacks. Data and information stored should be classified, labelled, and encrypted [7].

Despite the increasing adoption of the Zero Trust model, no Zero Trust framework is specifically tailored for financial institutions. This research addresses this gap by proposing a Zero Trust framework designed to address financial organisations' unique challenges.

The proposed framework in this study builds upon the previous research on the Zero Trust model and tailors it to financial institutions' specific needs and challenges. The framework includes authentication and authorization, access policies, role-based access controls, firewall policies, endpoint protection, network segmentation, data loss prevention, and encryption.

### III. ZERO TRUST MODEL

Zero Trust is a strategic initiative for cybersecurity that can keep an organisation safe [8]. It does this by getting rid of blind trust and continuously validating each step of digital interaction. Zero Trust is based on the principle "never trust, always verify." Its goal is to protect today's technological environment while making digital transformation easier. It uses multi-factor authentication, network segmentation, eliminating lateral movement, Layer 7 threat prevention, and streamlining granular "least access" policies.

The concept of "Zero Trust" arose from the realisation that conventional security models are based on the out-of-date idea that everything within an organisation's network can be trusted without further investigation [9]. Because there are not enough fine-grained security controls, users (including threat actors and malicious insiders) can freely move around the network, access sensitive data, and send it out because the network trusts them.

In the last decade, businesses have begun to spread their DAAS (data, assets, applications, and services) across different servers and cloud storage options. Due to this decentralisation, it is no longer possible to secure a network by isolating it within a single location, group of devices, or group of users. The zero-trust framework was made in this distributed, cloud-native environment to help businesses protect their most valuable assets.

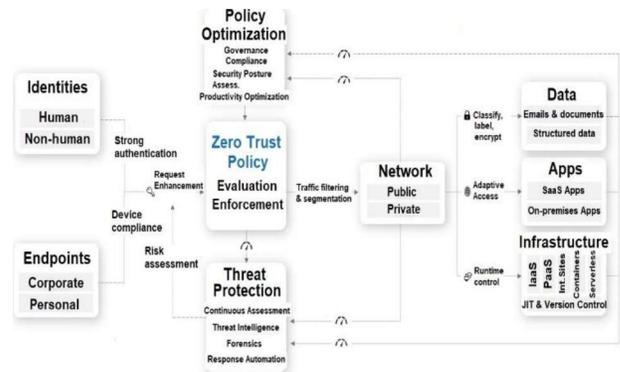


Fig. 1. Zero-trust security Architecture by Microsoft [6].

Based on the idea that there is no secure network perimeter, zero trust requires designing a system in which every user and service is treated as a possible security risk, no matter how deeply they are embedded in the network. Access requests must be constantly checked so that your system can connect to your applications and services [10]. Users and devices would undergo continuous authentication of their identities and privileges, and logins, connections, and API tokens would have a finite lifespan.

User DAAS access can be closely monitored with this "never trust, always verify" strategy. Access control, constant evaluation, and maximum observability are essential in the cloud-native world, where consumers may be geographically dispersed, using various devices, and actively trying to access DAAS via secure and unsecured networks [11].

The Zero Trust model treats every request as if it came from the public Internet rather than trusting that anything behind the company firewall is secure. Zero Trust teaches us to "never trust, always verify," regardless of the source or target of a request [12]. Each request is checked for

authentication, authorization, and encryption before access is given, as shown in Fig. 1. The principles of micro-segmentation and least-privileged access are used to restrict communication between nodes. Anomalies are identified and dealt with instantly by employing sophisticated intelligence and analytics.

#### IV. PROPOSED FRAMEWORK

This section proposes a framework for implementing the Zero Trust model in financial institutions, emphasising three key areas: Data protection, Identity and Access Management (IAM), and Device and network security.

##### A. Identity and Access Management (IAM)

The Identity and Access Management (IAM) component ensures that only authorised users gain access to an organisation's resources, particularly in financial institutions where sensitive data and transactions are involved. Implementing strong authentication and authorization mechanisms, such as Multi-Factor Authentication (MFA), Role-Based Access Controls (RBAC), and Access Control Policies, is essential for maintaining security.

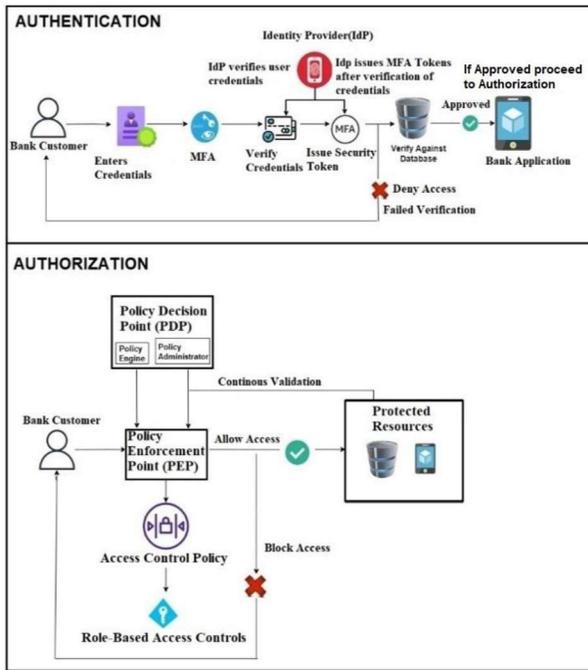


Fig. 2. Identity and Access Management (IAM)

Fig. 2 illustrates the proposed Identity and Access Management process, in which users first enter their credentials, which are then verified by the Authentication Server or Identity Provider (IdP). This verification process may involve checking against stored user data in the system and analysing behavioural factors. Upon successfully verifying the user's credentials, the system proceeds to the MFA stage, where the user must provide additional proof of identity, such as a one-time password (OTP) sent to their registered device.

After verifying the MFA token, the system moves to the authorization phase, where the Policy Enforcement Point (PEP) intercepts the user's request and forwards it to the Policy Decision Point (PDP) for evaluation against the defined access control policies. These policies can be tailored

to accommodate various factors, such as user roles, access levels, and the specific needs of financial institutions. The PDP then decides based on the evaluated policies and sends it back to the PEP, which carries out the decision.

RBAC are applied at this stage, granting users access to the resources and actions they are authorised to perform based on their assigned roles. This ensures that users can only access the data and perform actions relevant to their job functions, thus reducing the risk of unauthorised access and data breaches.

Finally, the system provides access to the resources and continuously monitors and audits user activities to ensure compliance with security policies and detect potential threats or anomalies. This constant monitoring makes it possible to find and fix security risks in real time, which makes the financial institution even safer overall.

In conclusion, it is important for financial institutions to have a well-designed IAM system to protect sensitive data and make sure that resources can be accessed safely.

##### B. Device and Network Security

Device and network security are integral to the Zero Trust model, designed to protect against internal and external threats. This is achieved by incorporating various security components such as firewalls, intrusion detection systems (IDS), Demilitarized Zone (DMZ), and network segmentation.

Financial institutions are highly susceptible to security threats due to the sensitive data they manage and the value of their transactions. To mitigate such risks, the implementation of robust security measures is essential. For instance, IDS can detect and stop advanced threats that target organization.

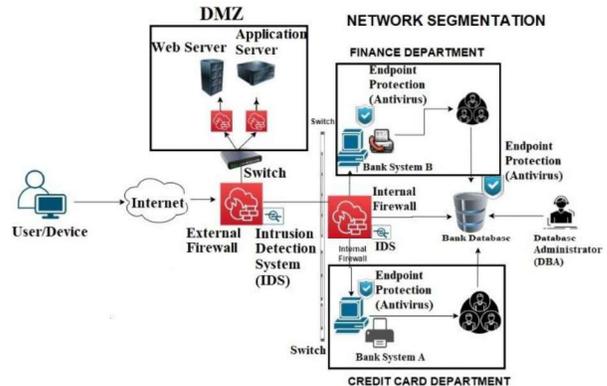


Fig. 3. Device and Network Security

Fig. 3 illustrates the proposed device and network security mechanism, in which all user and device traffic is treated as untrusted and verified before accessing any network resources. The framework begins by implementing an external firewall, which regulates incoming and outgoing traffic to allow legitimate traffic while blocking unauthorised traffic. IDS is also deployed to detect and prevent intrusion attempts into the network.

Next, network segmentation is implemented by dividing the network into separate segments based on functionality and security requirements. The Finance Department and Credit Card Department are two examples of network segments with their own security measures, including

internal firewalls, IDS, and endpoint protection. A DMZ is created to house public-facing services while isolating them from the internal network. This includes web and application servers with firewalls to limit access and protect against potential threats.

The database component is crucial for financial institutions, and its security is maintained through endpoint protection and database administration. The vulnerability scanning is conducted using automated scanning tools such as Nessus and OpenVAS to detect and remediate potential security vulnerabilities in the network infrastructure.

In conclusion, implementing comprehensive device and network security measures tailored to financial institutions' unique requirements and challenges is critical to the Zero Trust model. This ensures that the institution's network infrastructure remains secure and resilient against cyber threats.

### C. Data Protection

Data protection is critical to the Zero Trust model, particularly for financial institutions that handle sensitive customer data and financial transactions [6]. Implementing effective data protection measures ensures that sensitive information is secure from potential data breaches and unauthorised access.

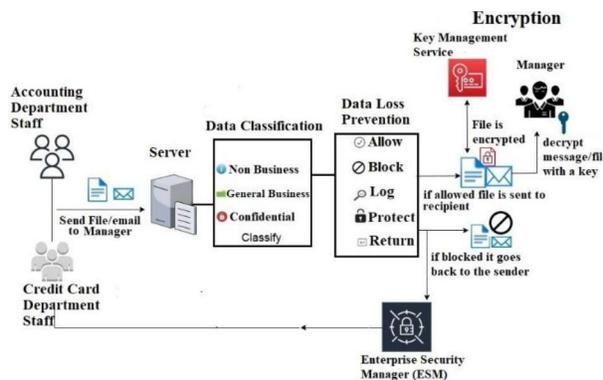


Fig. 4. Data Protection

Fig. 4 shows the proposed data protection method, which includes data classification, data loss prevention (DLP), encryption, and enterprise security management (ESM). The first step in data protection is to classify the data based on its sensitivity level. This can range from non-business data to confidential data, requiring the highest protection level. Data classification helps organisations identify the types of data they hold and prioritise security measures accordingly.

Data Loss Prevention (DLP) is a set of technologies and policies that help prevent data from leaving an organisation's network. This can be achieved by blocking, allowing, logging, protecting, or returning data based on predefined policies. DLP tools can monitor and control the movement of sensitive data within the organisation, helping to prevent unauthorised access, sharing, or exfiltration.

Encryption is another essential data protection technique used to secure sensitive information. This protects sensitive data at rest, in transit, and in use, ensuring that it remains confidential even if intercepted or accessed by unauthorised parties. Key management services and managers play a crucial role in the encryption process, helping to ensure that encryption keys are generated, stored, and managed securely.

The Enterprise Security Manager (ESM) is a centralised management platform that provides visibility and control over an organisation's security infrastructure. This includes monitoring and managing security events, policies, and configurations, analysing security data, and generating reports. The ESM helps financial institutions identify and respond to security threats and vulnerabilities proactively. This ensures that sensitive data remains secure and confidential, reducing the risk of data breaches and ensuring compliance with data protection regulations.

Financial institutions can better protect sensitive information and reduce the risk of data breaches and unauthorised access by using a comprehensive data protection strategy that includes data classification, data loss prevention, and encryption. Combined with a strong IAM system and robust device and network security controls, these measures create a holistic approach to implementing the Zero Trust model in financial institutions, ensuring a secure and compliant environment for handling sensitive financial data.

## V. IMPLEMENTATION DETAILS (DEMO BANK APP)

This section provides an overview of the demo bank application, discusses the technologies and tools used in its development, and presents the implementation details of the Zero Trust Model components within the app and the testing approach.

### A. Overview of the Demo Bank App

The demo bank application serves as a practical demonstration of the proposed framework for implementing the Zero Trust Model in financial institutions. It incorporates the three main components of the Zero Trust Model: Identity and Access Management (IAM), device and network security, and data protection. Through the development of this application, we showcase how these components work together to enhance the security of financial transactions and protect sensitive customer data.

### B. Technologies and Tools Used in Development

The demo bank app was developed using several technologies and tools that enable the implementation of the Zero Trust Model. JavaScript (version 1.8.5), HTML5, and CSS3 were used for front-end development, providing a user-friendly interface and responsive design. On the server side, we utilised Node.js (version 14.17.0) as the runtime environment and Express.js (version 4.17.1) as the web application framework. These technologies allowed for efficient server-side processing and routing of requests.

We employed MySQL (version 8.0.23), a robust relational database management system, for data storage and management. MySQL provided a secure and scalable solution for storing sensitive customer information and transactional data.

### C. Implementation of the Zero Trust Model Components

#### 1. Identity and Access Management (IAM)

IAM is crucial in ensuring secure authentication and authorization processes within the demo bank app. A comprehensive IAM framework using Node.js, Express.js, and JSON Web Tokens (JWT, version 8.5.1) was implemented. This framework facilitated the secure

management of user identities, authentication, and authorization processes. JSON Web Tokens (JWT) served as a stateless and scalable authentication mechanism, allowing for the generation and validation of tokens. Any inputted password and OTP are validated against stored user data. If successful, a JWT token is generated for subsequent authentication.

Robust password hashing using bcrypt (version 5.0.1), was implemented for secure password storage. Role-Based Access Control (RBAC) was incorporated to restrict user privileges based on their roles within the financial institution. Middleware functions were used to check the role of each user and verify their permissions before allowing access to specific resources or performing privileged operations. To enhance security, we integrated Multi-Factor Authentication (MFA) using the speakeasy library (version 2.0.0) to generate and verify One-Time Passwords (OTPs) during the login process.

## 2. Device and Network Security

Device and network security are critical aspects of the Zero Trust model. To ensure the security of devices and network communications, we implemented several measures within the demo bank app.

Secure communication between the client and the server was achieved using HTTPS. We utilised the built-in HTTPS module in Node.js and SSL/TLS certificates to configure secure connections. During the establishment of secure connections, we validated SSL/TLS certificates to ensure their trustworthiness.

Network traffic monitoring middleware was implemented to log and analyse incoming requests. The middleware function was used to log the details of each request, including the HTTP method and URL. This allowed for the monitoring and analysis of network traffic, providing insights into the app's security posture and detecting potential suspicious activities. Device authentication was incorporated to verify the identity and integrity of connecting devices. Middleware functions perform device authentication checks before granting access to protected resources. The "performDeviceAuthentication" function validated the user-agent header of the incoming request to ensure that only trusted devices were authorised to access sensitive resources.

The "deviceAuthenticationMiddleware" middleware function enforced device authentication checks, allowing only authenticated devices to proceed to the protected route.

## 3. Data Protection

Data Protection is a crucial aspect of the Zero Trust Model. In the demo bank app, we implemented comprehensive measures to ensure the protection of sensitive data. Sensitive data in the demo bank app was encrypted both at rest and in transit. Encryption techniques were employed using cryptographic algorithms and keys. We utilised the "encryptData" and "decryptData" functions, leveraging the cryptographic capabilities of the "crypto" module in Node.js. These functions securely transformed the data into an unreadable format and ensured its confidentiality.

To prevent unauthorised data exfiltration, data loss prevention mechanisms were implemented. The app incorporated data loss prevention rules and checks to detect

and respond to potential data breaches or unauthorised data access. When data is received through a POST request to the "/api/data" endpoint, the data loss prevention mechanism, applies data loss prevention rules to verify if the data exfiltration is detected. If the data passes the checks and is deemed secure, it is saved to the database. However, if data loss prevention rules are triggered, indicating a potential data breach, an appropriate error response is sent to the client.

The "encryptData" function utilises the public key obtained from the "MyCertificate.crt" file to encrypt the sensitive data. The "decryptData" function uses the private key from the "MyKey.key" file to decrypt the encrypted data. The "crypto" module from Node.js is used for cryptographic operations. The encrypted data is stored as a Base64-encoded string for further use.

By implementing these encryption techniques and data loss prevention mechanisms, the demo bank app ensures the confidentiality and integrity of sensitive data, reducing the risk of unauthorised access and data breaches.

## D. Testing Approach

A thorough testing regimen was implemented to validate the effectiveness of the components in a controlled environment.

### 1. IAM Testing

This included the verification of user authentication and authorization processes, the assessment of different user roles and permissions, and the evaluation of password strength and encryption techniques, which played a crucial role in enhancing the security of the IAM system. The password policy defined requirements such as minimum password length, complexity, and periodic password updates. Functional Multi-Factor Authentication (MFA) testing was also conducted during the IAM testing.

### 2. Device and Network Security Testing

Network traffic analysis was performed using Wireshark (version 4.0.2) for packet inspection. The app's SSL/TLS certificates were validated, and request and response details were inspected for possible security threats.

### 3. Data Protection Testing

The app's encryption techniques were evaluated for data at rest and in transit, and data loss prevention mechanisms were tested using OpenSSL (version 1.1.1) to prevent unauthorised data exfiltration.

The results obtained from this extensive testing phase confirmed the successful implementation of the Zero Trust Model's components in the demo bank app. This enhanced the secure environment for financial transactions, ensuring the safety and integrity of sensitive customer data. Further iterations of the testing process will continue to refine and perfect the model's implementation.

## VI. RESULTS AND DISCUSSION

This section presents the results and discussion of the implemented framework in the demo bank app. It evaluates the framework's effectiveness in addressing security challenges such as IAM, device and network security, and data protection. The discussion highlights the challenges encountered during the implementation and provides insights and recommendations to overcome these challenges.

### A. Identity and Access Management (IAM)

During the IAM testing, the demo bank app demonstrated its capability to control access effectively, prevent unauthorised entry, and enforce appropriate authentication and authorization processes. User authentication for different roles and credentials successfully ensured that only authorised users gained access to their respective accounts and functionalities. Role-Based Access Control (RBAC) was adequately enforced, allowing users to perform actions based on their assigned roles and preventing unauthorised access to sensitive financial data. Password strength and complexity requirements were correctly enforced, and session management and timeout functionality were appropriately implemented. Multi-Factor Authentication (MFA) added an extra layer of security, mitigating the risk of unauthorised access to critical financial operations.

### B. Device and network security

The analysis of network traffic using Wireshark confirmed that the implemented device and network security measures effectively protected against unauthorised access and network-based attacks. During the testing period of 1 hour, the captured packets encompassed various protocols, including HTTPS, and DNS. Noteworthy details from the captured packets include source and destination IP addresses, ports, and packet payloads.

The analysis of the captured network traffic yielded several important insights. Notably, all communication between the demo bank app and client devices occurred over secure HTTPS connections as shown in Fig. 5, ensuring the confidentiality and integrity of the data transmitted.

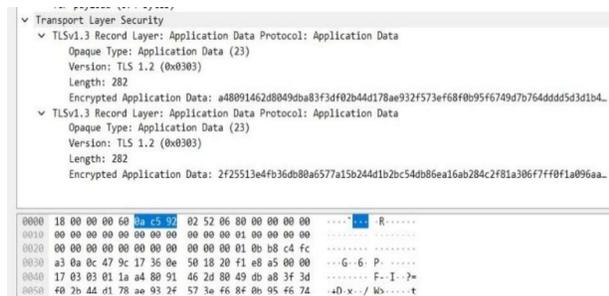


Fig. 5. Wireshark screenshot showing the start of a TLS handshake, with details of the server hello message and the chosen cypher suite.

Furthermore, the implemented access controls were effective in preventing unauthorised network access attempts. No suspicious or unauthorised network activity was observed, indicating the robustness of the network security measures.

### C. Data Protection

To evaluate the effectiveness of the data protection measures in the demo application, comprehensive testing was conducted using OpenSSL to establish a secure connection to the application running on localhost:3000. During the testing, a self-signed certificate was used to establish the SSL/TLS connection, as shown in Fig. 6. While self-signed certificates are not recommended for production environments, they can be suitable for local development and testing purposes.

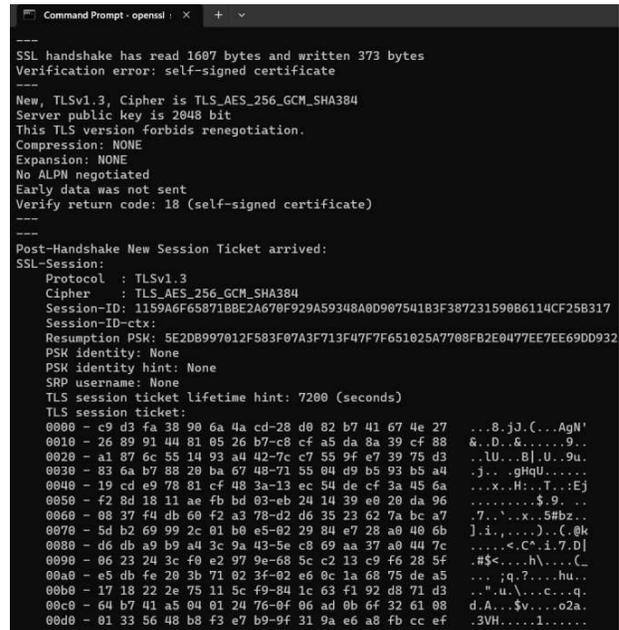


Fig. 6. Testing results from OpenSSL

The connection between the client and the server employed strong encryption. The OpenSSL output indicated that the session protocol used was TLSv1.3, and the cypher TLS\_AES\_256\_GCM\_SHA384, as shown in Fig. 6, was used for secure communication. This encryption ensures that the data transmitted between the client and the server remains confidential and protected from eavesdropping.

The demo application guarantees data integrity during transmission by establishing a secure connection. The integrity of the data was ensured through secure protocols, such as TLSv1.3. These measures verify that the data received by the client matches the data sent by the server, mitigating the risk of data tampering or unauthorised modification.

Although the self-signed certificate used in the testing may not be trusted by default, it still provides a mechanism for authentication. The client can verify the server's identity by comparing the information in the certificate, such as the common name (CN) and the issuer details, with the expected values. This ensures that the client communicates with the intended server and helps protect against man-in-the-middle attacks.

The OpenSSL testing confirmed the practicality of the data protection measures implemented in the demo application. The application demonstrated strong encryption, data integrity, and authentication capabilities. These measures provide a secure environment for transmitting sensitive data and help ensure the confidentiality and integrity of the information exchanged between the client and the server.

### D. Challenges and Recommendations

Despite the successful implementation and testing, several challenges were identified. One of the challenges includes integration with legacy systems, which can pose compatibility and interoperability issues. The integration procedure must be carefully planned and executed to provide smooth communication and data interchange between existing systems and the Zero Trust framework.

Another problem is maintaining a high level of security while maintaining control over the user experience. It is vital to balance strong security measures with a user-friendly interface. Future updates should prioritise improving the user interface and making security measures easy and unobtrusive.

Insights and recommendations emerged from the implementation and testing phases. Future work could integrate artificial intelligence and machine learning technologies to improve anomaly detection and response times. Additionally, implementing a more comprehensive audit trail and event logging system would provide greater visibility into user activities and potential security breaches, aiding in timely detection and response. It is essential to prioritise continuous evaluation, proactive monitoring, and regular updates to address emerging security threats and ensure compliance with industry standards and regulations.

The results obtained from the testing phase validate the successful implementation of the Zero Trust Model components in the demo bank app. Integrating Identity and Access Management (IAM), device and network security, and data protection measures contributes to a secure environment for financial transactions, ensuring the safety and integrity of sensitive customer data.

## VII. CONCLUSION AND FUTURE WORKS

In conclusion, this paper has presented a comprehensive framework for implementing the Zero Trust Model in financial institutions, as demonstrated by developing a demo bank app. The app successfully incorporated the key components of the Zero Trust Model, including Identity and Access Management (IAM), device and network security, and data protection. Through the implementation of the demo bank app and rigorous testing, we have shown that the proposed framework effectively addresses the security challenges specific to financial institutions. The use of robust authentication and authorization processes, secure communication channels, and data encryption techniques ensures sensitive consumer data's privacy, availability, and integrity. By implementing the proposed framework, financial institutions can establish a robust security posture, thereby mitigating cyber threats and boosting consumer confidence. The Zero Trust Model principles enable a proactive security strategy, shifting away from traditional perimeter-based defences and embracing a continuous and dynamic security approach. However, there are areas that need further investigation and improvement.

Future research should evaluate the framework's scalability, adaptability, and effectiveness in complex environments through its practical implementation in real-world financial institutions. In addition, ongoing research is required to address obstacles such as legacy system integration and finding the optimal balance between security and user experience. Financial institutions can continually enhance and refine the framework to remain ahead of

emerging security threats and changing regulatory requirements. This will allow them to maintain a robust security posture, secure sensitive data, and protect their reputation and customers' confidence. In conclusion, the proposed framework provides financial institutions with a firm foundation for implementing the Zero Trust Model, which offers a proactive and comprehensive security approach. By adopting this model, financial institutions can navigate the ever-changing threat landscape and maintain the security and integrity of their operations.

## ACKNOWLEDGEMENT

We express our deepest gratitude to the Ghana Scholarship Secretariat for their financial support throughout this research project. Their assistance played a crucial role in the successful completion of this study.

## REFERENCES

- [1] J. Kindervag, "Build Security Into Your Network's DNA: The Zero Trust Network Architecture," Forrester Research, 2010.
- [2] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," Aug. 2020, Published, doi: 10.6028/nist.sp.800-207.
- [3] T. Chuan, Y. Lv, Z. Qi, L. Xie, and W. Guo, "An Implementation Method of Zero-trust Architecture - IOPscience," in Proceedings of the 5th International Conference on Industrial Engineering and Applications, Nov. 01, 2020, pp. 012010. doi: 10.1088/1742-6596/1651/1/012010.
- [4] D. D'Silva and D. D. Ambawade, "Building A Zero Trust Architecture Using Kubernetes," in Proceedings of the 2021 6th International Conference for Convergence in Technology (I2CT), Maharashtra, India, 2021, pp. 1-8. doi: 10.1109/I2CT51068.2021.9418203.
- [5] R. Zeng, N. Li, X. Zhou and Y. Ma, "Building A Zero-trust Security Protection System in The Environment of The Power Internet of Things," in Proceedings of the 2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT), Shanghai, China, 2021, pp. 557-560. doi: 10.1109/AINIT54228.2021.00114.
- [6] Microsoft Security, "Zero Trust Model - Modern Security Architecture," [Online]. Available: <https://www.microsoft.com/en-us/security/business/zero-trust>.
- [7] U. B. Chaudhry and A. K. M. Hydros, "Zero-trust-based security model against data breaches in the banking sector: A blockchain consensus algorithm," IET Blockchain, Mar. 2023, doi: 10.1049/ble2.12028.
- [8] M. Shore, S. Zeadally, and A. Keshariya, "Zero trust: the what, how, why, and when," Computer, vol. 54, no. 11, pp. 26-35, 2021.
- [9] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture (No. NIST Special Publication (SP) 800-207)," National Institute of Standards and Technology, 2020.
- [10] B. Chen, S. Qiao, J. Zhao, D. Liu, X. Shi, M. Lyu, H. Chen, H. Lu, and Y. Zhai, "A security awareness and protection system for 5G smart healthcare based on zero-trust architecture," IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10248-10263, 2020.
- [11] D. D'Silva and D. D. Ambawade, "Building a zero trust architecture using Kubernetes," in 2021 6th International Conference for Convergence in Technology (I2CT), April 2021, pp. 1-9.
- [12] N. Papakonstantinou, D. L. Van Bossuyt, J. Linnosmaa, B. Hale, and B. O'Halloran, "A zero trust hybrid security and safety risk analysis method," Journal of Computing and Information Science in Engineering, vol. 21, no. 5, 2021.