# Short-Lived Certificate in Zero Trust Model

Ayushi Shrivastava
*Department of Computer Science*
*University of Oregon*
Eugene OR, USA
ayushis@uoregon.edu

Frimpong Osei
*Department of Computer Science*
*University of Oregon*
Eugene OR, USA
fosei@uoregon.edu

Kenneth Nnadi
*Department of Computer Science*
*University of Oregon*
Eugene OR, USA
knnadi@uoregon.edu

***Abstract*—This research integrates short-lived certificates into the zero-trust security model to enhance security measures and address vulnerabilities in traditional authentication methods. By implementing short-lived certificates, a continuous re-authentication process is enforced, significantly reducing the risk of unauthorized access over extended periods. This approach offers notable advantages by limiting the time-frame for potential misuse in case of compromised certificates. The study thoroughly examines the technical aspects of managing short-lived certificates, covering generation, secure distribution, and efficient validation processes. The findings emphasize the significance of these technical intricacies in establishing a robust and proactive authentication approach within the zero-trust framework with the concept of never trust always verify. The adoption of short-lived certificates contributes to creating a resilient security environment, safeguarding critical information by leveraging on the short lifespan of the certificate. This research provides valuable insights into security practices, highlighting the importance of continuous verification as a fundamental aspect of the zero-trust paradigm.**

***Index Terms*—Short-lived certificates, Zero-trust security, Continuous Re-authentication, Vulnerability mitigation, Certificate management, Secure distribution, Privacy, Confidentiality,Data integrity,Security compliance's.**

## I. Introduction

The motivation behind this project is to investigate the integration of short-lived certificates into the emerging zero-trust security model. Traditional security models, including token-based authentication and password-based authentication, exhibit inherent limitations that render them susceptible to exploitation by malicious actors. For instance, OTPs can be intercepted or compromised, leading to unauthorized access to critical systems and sensitive information. To address these vulnerabilities and enhance security measures, this project proposes the implementation of short-lived certificates within the novel zero-trust security model.

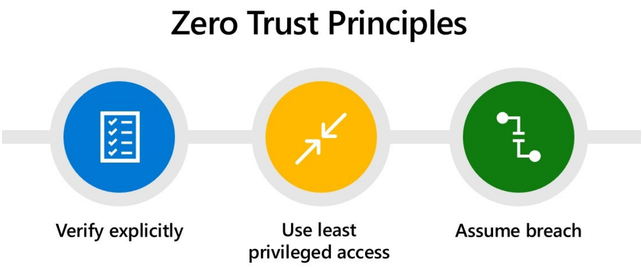


Fig. 1. Zero-Trust Principle

The zero-trust model embodies the fundamental principle of ”Never Trust, Always Verify,” emphasizing the continuous verification of users and devices prior to granting authorisation. By enforcing regular re-authentication, short-lived certificates reduce the risk of unauthorized access over extended periods, fortifying the overall security posture. Additionally, short-lived certificates offer a notable advantage over their long-lived counterparts by shortening the validity period. This shorter lifespan significantly limits the window of opportunity for threat actors to exploit stolen or compromised certificates, bolstering overall security.

The integration of the Zero Trust and Short-lived certificate authentication security models presents a compelling and innovative approach to achieving enhanced security measures. By capitalizing on the continuous verification and validation of user access to protected devices or services, this conceptualization offers a robust solution for mitigating the risks associated with long-lived certificates and unauthorized network presence. Short-lived certificates, with their shorter lifespans, provide a viable alternative to traditional certificate-based authentication, reducing the window of vulnerability for potential attacks.

Through the implementation of this method, users are granted access to a server only within a session created after successful authorization through the server's certificate validation process. This integration not only strengthens security measures but also proactively addresses the risk of unauthorized access and potential data breaches. To illustrate the practical application of this concept, consider a banking system where users request a short-lived certificate from a central banking certificate issuer. This certificate, similar to a one-time password (OTP), remains valid for a very short period of time. Once issued, the client utilizes the certificate for authentication, eliminating the need for additional security measures. The certificate's validity and authenticity are verified by the server, ensuring it originates from the specific certificate issuer and corresponds to a registered user or client attribute within the bank's system.

The focus of our research lies in exploring the effectiveness and implementation of short-lived certificate authentication within a Zero-Trust framework. By investigating this integration, we aim to provide valuable insights into the practical application of this security model and its potential to enhance the protection of sensitive information, safeguard against unauthorized access, and maintain the integrity of data

## II. Related Work

In recent years, the use of short-lived certificates and certificate-based authentication has gained significant attention as a promising approach to enhancing security in various network infrastructures. This literature review provides an overview of the existing research in this field, focusing on the potential benefits and advancements in security frameworks.

One notable research study conducted by Hsu and Seymour (1997) explored the application of short-lived certificates in an intranet security framework. The study aimed to strengthen security within intranet environments by implementing a system where certificates have a limited lifespan. The authors proposed a framework that integrated short-lived certificates for authentication and access control purposes. This research contributes to the field by providing insights into the practical implementation of short-lived certificates to mitigate risks associated with long-lived certificates in intranet systems.

Moreover, Sciancalepore et al. (2015) introduced a key management protocol with implicit certificates for Internet of Things (IoT) systems. The protocol addressed the challenge of secure key management in resource constrained IoT environments. By utilizing lightweight implicit certificates, the protocol aimed to reduce computational, and storage overhead associated with traditional Public Key Infrastructures (PKIs). This research contributes to the field of IoT security by providing a tailored key management solution that is practical and effective in real-world IoT deployments.

In the domain of vehicular ad-hoc networks (VANETs), Farooq et al. (2016) conducted research on the implementation of certificate-based security mechanisms using the IEC 61850 and IEEE WAVE standards. The study explored the integration of certificates as a security measure to protect communication and data exchange within VANETs. By leveraging certificates for authentication and secure communication between vehicles and infrastructure, the authors aimed to establish a robust security architecture. This research contributes to the field by providing insights into the practical application of certificate-based security mechanisms in VANETs.

Furthermore, the concept of zero trust architecture is discussed in the NIST Special Publication 800 (2020) by Stafford. The publication provides an overview and guidelines for implementing a zero-trust approach to cybersecurity. It emphasizes the importance of continuously verifying the identity and trustworthiness of users and devices, challenging the traditional notion of implicit trust. The document highlights various principles and components of a zero-trust architecture, such as strong authentication, least privilege access, and continuous monitoring. Stafford's work contributes to the field by providing insights and recommendations for organizations looking to adopt a zero-trust security paradigm.

In the context of next-generation automobiles, Kondaveety et al. (2022) presented a research study on a zero-trust architecture specifically designed to address the security challenges in modern automotive systems. The study emphasized continuous verification and authentication of all entities within the automotive network to enhance security and mitigate potential cyber threats. By adopting a zero-trust approach, the authors aimed to improve the security posture of automobiles. This work contributes to the literature by providing a comprehensive understanding of the application of zero trust principles in the context of automotive cybersecurity.

In conclusion, this literature review has provided an overview of the existing research on Zero trust and certificate-based authentication. The reviewed studies highlight the potential benefits of these security measures and their application in various contexts, including intranet environments, automotive systems, VANETs, and IoT deployments. Thus, our motivation is to integrate these two security architectures, short-lived certificate authentication in the zero trust model, for more robust authentication of clients accessing protected resources on a server.

## III. Why Short-Lived Certificates

Traditional models, including SSL (Secure Socket Layer) and TLS (Transport Layer Security), have long been recognized as essential components for securing network communications. However, it is crucial to acknowledge that these traditional models are not infallible and have inherent vulnerabilities. The following statistics shed light on the extent of these vulnerabilities and the need for alternative security measures:

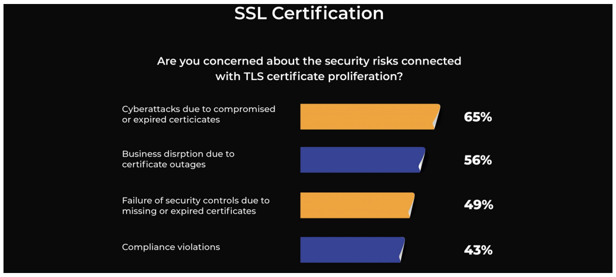


Fig. 2. Statistics showcasing why SSL/TLS are vulnerable

According to recent studies, a significant percentage of data breaches occur due to compromised SSL/TLS certificates, resulting in unauthorized access to sensitive information. The average lifespan of a compromised SSL/TLS certificate is approximately two years, during which attackers can exploit the compromised certificate to gain unauthorized access and perpetrate malicious activities. An average time to detect and remediate a compromised certificate is long, leaving a significant window of opportunity for attackers to exploit the compromised credentials. Given these statistics and the growing sophistication of cyber threats, there is a need to explore alternative security measures that can provide enhanced protection and mitigate the risks associated with long-lived certificates. Short-lived certificates emerge as a promising solution, offering reduced vulnerability exposure and improving the overall security posture of network communications.

In **fig 1**, the statistics show that 65% of cyber-attacks are due to compromised or expired certificates.Additionally, 56% of cyber-attacks are attributed to certificate outages.Furthermore, the failure of security controls due to expired certificates accounts for approximately 49% of cyber-attacks.Finally, compliance violations are responsible for about 43% of cyber-attacks.

### Benefits of Short-Lived Certificates:

- **Reduced Exposure to Risk:** By implementing short-lived certificates, the exposure to risk is significantly reduced. Since these certificates have shorter lifespans, even if a certificate is compromised, the window of opportunity for misuse is limited. This helps prevent unauthorized access and mitigates the potential impact of a compromised certificate.
- **Faster Detection and Response:** Short-lived certificates facilitate faster detection and response to security incidents. With shorter certificate lifetimes, anomalies and security breaches can be identified more quickly. This enables organizations to promptly respond, investigate, and mitigate potential threats, minimizing the potential damage caused by com-

promised certificates.

- **Improved Key Management:** Short-lived certificates contribute to improved key management practices. Automated renewal and rotation of certificates are integral to short-lived certificate implementations. This reduces the burden of manual certificate management and ensures that certificates are regularly updated and refreshed. By automating these processes, organizations can enhance their overall security posture and minimize the risk of using outdated or compromised certificates.

## IV. Zero Trust Operational Model

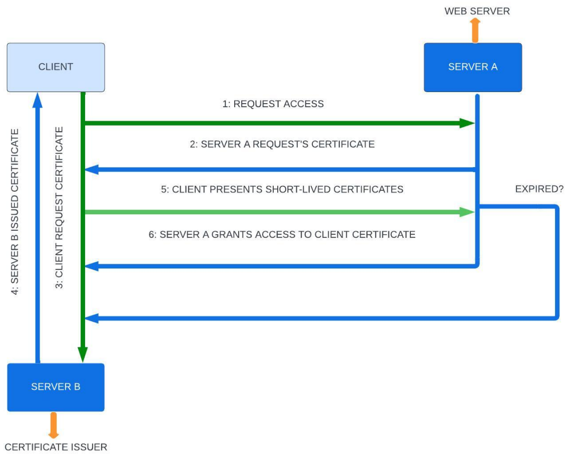

WEB SERVER
CLIENT
SERVER A
1: REQUEST ACCESS
2: SERVER A REQUEST'S CERTIFICATE
5: CLIENT PRESENTS SHORT-LIVED CERTIFICATES
EXPIRED?
6: SERVER A GRANTS ACCESS TO CLIENT CERTIFICATE
4: SERVER B ISSUED CERTIFICATE
3: CLIENT REQUEST CERTIFICATE
SERVER B
CERTIFICATE ISSUER

Fig. 3. Zero-Trust Operational Model

### A. Design

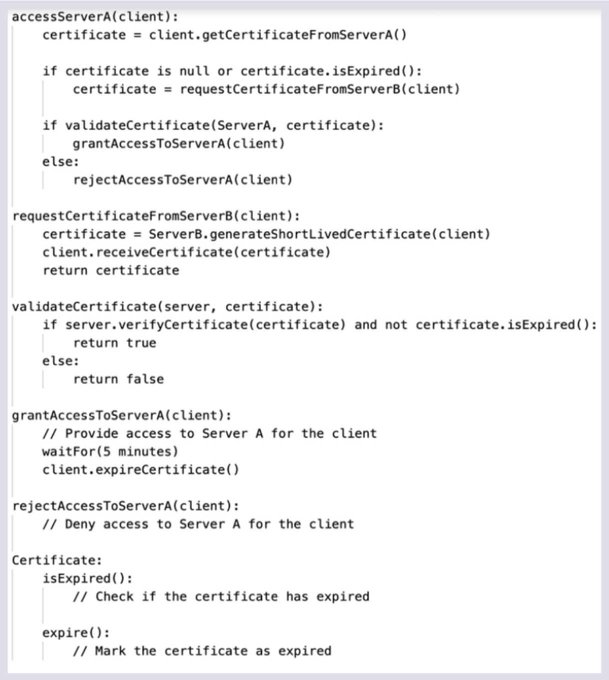
In our model above, the process of authentication and access involves the interaction between the client (User), Server A (Protected Web-Server), and Server B (Certificate Issuance server). **Here is a step-by-step explanation of the workflow:**

The client initiates a request to access Server A (either web server, email server or file server etc.) Server A, as part of the zero-trust model, requires the client to present a certificate for authentication. Since the client doesn't have a certificate, it reaches out to Server B (Certificate Issuance Server) to request one. Server B, acting as a certificate authority, verifies the identity of the client and generates a short- lived certificate for the client. The short-lived certificate is securely transferred from Server B to the client's machine.

The client, now in possession of the short-lived certificate, presents it to Server A as proof of its identity. Server A verifies the authenticity and validity of the short-lived certificate. If the certificate is successfully validated, Server A grants access to the client. If the client exits Server A and wishes to log back in after more than 5 minutes (the specified validity duration of the short-lived certificate), the client will need to repeat the entire process again, starting from requesting a new certificate from Server B.

This workflow ensures the client's continuous authentication based on zero trust and authorization by short- lived certificates. By requiring the client to go through the authentication process each time, the model maintains the principles of the zero-trust security model, where trust is not assumed, and constant verification is necessary.

### B. Algorithm



```
accessServerA(client):
    certificate = client.getCertificateFromServerA()

    if certificate is null or certificate.isExpired():
        certificate = requestCertificateFromServerB(client)

    if validateCertificate(ServerA, certificate):
        grantAccessToServerA(client)
    else:
        rejectAccessToServerA(client)

requestCertificateFromServerB(client):
    certificate = ServerB.generateShortLivedCertificate(client)
    client.receiveCertificate(certificate)
    return certificate

validateCertificate(server, certificate):
    if server.verifyCertificate(certificate) and not certificate.isExpired():
        return true
    else:
        return false

grantAccessToServerA(client):
    // Provide access to Server A for the client
    waitFor(5 minutes)
    client.expireCertificate()

rejectAccessToServerA(client):
    // Deny access to Server A for the client

Certificate:
    isExpired():
        // Check if the certificate has expired

    expire():
        // Mark the certificate as expired
```

Fig. 4. Working of our model using Pseudo-code

### C. Implementation

**1. Deployment of Servers on AWS EC2 Instance:** Two servers were provisioned on the Amazon Web Services (AWS) EC2 platform to establish

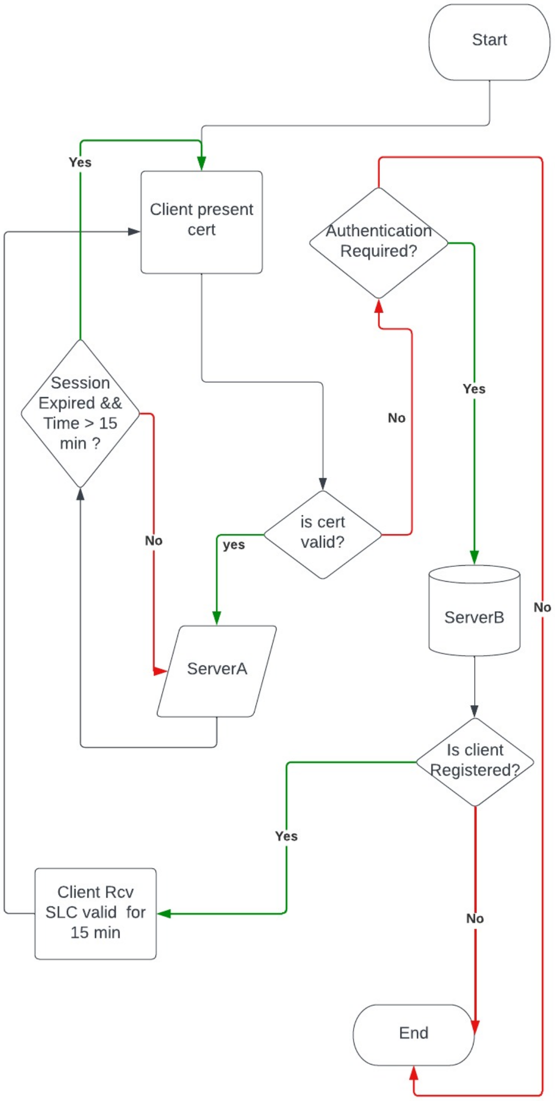


Fig. 5. Flowchart of Zero Trust Operational Model

the necessary infrastructure for our research. Server A, functioning as an NGINX web server, and Server B, designated as the Certificate Authority Issuance Server, were deployed to facilitate the authentication process evaluation and analysis.

**2. Configuration of Server A (NGINX Web Server):** The NGINX web server was meticulously configured on Server A to ensure optimal performance and accurate testing of our authentication model. The server's settings and parameters were fine-tuned to align with the specific requirements of our research objectives.

**3. Setup of Certificate Authority Issuance Server (Server B):** Server B, designed as the Certificate Authority Issuance Server, underwent a comprehensive setup process to enable the issuance of certificates to registered clients. The configuration involved the establishment and signing of a root certificate, followed by the creation and signing of an intermediate or sub-certificate by the root-CA. The sub-CA or intermediate certificate, serving as the trust anchor, was utilized to sign both the server certificate employed in the configuration of Server B and the client certificate securely transmitted to clients for authentication purposes. It is important to note that the client certificate possesses a restricted lifespan of 15 minutes, after which it expires. Subsequent connection attempts to Server A utilizing an expired client certificate will be rejected as part of the implemented security measures.

**4. Testing with a user on AWS EC2 instance:** During the testing phase of our model, the client initiated a certificate signing request (CSR) by employing its private key. Subsequently, the client's CSR was signed by the sub-certificate authority, resulting in the generation of a short-lived certificate with the fully qualified domain name of the protected web-server and the clients credentials. This certificate was securely transferred to the client for immediate usage.To establish a trusted connection, the root certificate of the Certificate Authority (CA) was also securely transmitted to the client. This root-CA certificate was incorporated into the client's operating system trusted certificates and updated. The process of updating the trusted root-CA is only done once. This step was crucial to ensure that the operating system recognizes and trusts our CA. Without this trust, establishing a secure connection would not be feasible. Similarly, in Server A, the root-CA certificate of Server B was securely transferred and installed. This ensured that the operating system on Server A recognized and trusted our CA. Server B utilized the certificate chain of trust validation mechanism to authenticate and validate the client certificate, ensuring that it originated from our trusted CA and also checks the client's credential matches with the registered clients in the server B. This validation process provides an additional layer of security and verifies the authenticity of the client certificate before granting access to the requested resources.

## V. Results

Our model embodies a robust Zero Trust authentication and access control architecture designed to ensure high-level security. It leverages a Public Key Management Infrastructure (PKMI) to issue short-lived certificates to clients seeking access to our web server. These certificates are granted for a limited duration and undergo rigorous authentication and expiration checks. Clients presenting valid and non-expired certificates are granted secure access to our protected resources. This approach ensures a strong security posture while simplifying the user experience. In our testing phase, we focused on a single client connecting to the protected web server hosted on Nginx. The model successfully validated the client based on their credentials and the canonical name of the certificate generated by our Certificate Authority (Server B). This demonstrates that short-lived certificates can be seamlessly integrated into a Zero Trust model, consistently validating clients with valid certificates originating from a trusted Certificate Authority. One significant security implication of this architecture is the decentralized and distributed nature of the web server's security. By separating the configurations and services across different servers, it helps to avoid a single point of failure. This architecture also safeguards against potential risks associated with compromised certificates, as the short lifespan of the certificates limits the advantage that threat actors could gain from such compromises.

## VI. Lessons Learned

During the course of our study and the implementation of the zero-trust model with short-lived certificates, we encountered several limitations that influenced our approach and the scope of the project. It is important to address these limitations to provide a comprehensive overview of our work and its implications. We have identified the following limitations and the corresponding adjustments made to overcome them:

**Deployment Infrastructure**: Initially, we planned to deploy our servers on virtual machines (VMs). However, we recognized that this infrastructure might not offer the necessary robustness and scalability for a distributed implementation. To address this limitation, we made the strategic decision to transition to a cloud-based environment, which provided enhanced flexibility and accessibility, enabling us to meet the requirements of our project effectively.

**Practicality of Certificate Request Trigger**: One aspect we intended to explore was the possibility of triggering the certificate request process through a login page, where users could access their accounts by providing the correct password. However, we realized that integrating a login page with a database to store login fields would introduce trust assumptions that contradicted the principles of the zero-trust model. This deviation from the core principle of ”Never Trust, Always Verify” raised concerns about the integrity of our implementation. Consequently, we decided to abandon the idea of a login page and instead focused on developing a command-line interface (CLI) implementation. This adjustment ensured that our project remained aligned with the principles of the zero-trust model, without compromising security.

These limitations necessitated adjustments to our implementation strategy. While transitioning to a cloud-based infrastructure enhanced the overall robustness of our system, the shift from a login page to a CLI interface narrowed the scope of our study. It is vital to acknowledge these limitations and their impact on the direction and outcomes of our project.

Despite these limitations and adjustments, our study remains focused on implementing the zero-trust model with short-lived certificates and addresses the key objectives and deliverable outlined in our project plan. We strive to present a practical and effective solution for enhancing security in online transactions, staying true to the principles of the zero-trust model. By highlighting these limitations and our efforts to mitigate them, we contribute to the transparency and integrity of our research.

## VII. Discussion

Integrating short-lived certificates into the zero-trust security model presents several complex and unresolved issues that require further exploration and consideration. Some of these issues include:

**Navigating Technical Barriers:** Integrating short-lived certificates into existing authentication systems can pose technical challenges. Establishing a robust infrastructure for generating, distributing, and managing short-lived certificates requires careful planning and coordination. The implementation process must consider scalability, certificate revocation mechanisms, and secure distribution channels.

**Certificate Lifecycle Management:** Managing the life-cycle of short-lived certificates involves regular generation, distribution, and revocation. The efficient handling of these certificates requires automated processes and robust certificate management systems. Resolving issues related to certificate renewal, and expiration is crucial to ensure continuous and secure authentication.

**Interoperability and Compatibility:** Integrating short-lived certificates into different systems and platforms may encounter compatibility issues. Achieving interoperability between diverse applications, devices, and network environments can be challenging. Standardization efforts and compatibility testing are necessary to address these issues and ensure seamless integration across various platforms.

**Key Management and Security:** Short-lived certificates rely on encryption keys for secure authentication. Proper key management practices, including key generation, storage, and protection, are essential to prevent unauthorized access to the certificates and ensure the integrity of the authentication process. Effectively tackling key management challenges and upholding robust security measures are of paramount importance for ensuring the seamless integration and success of the solution.

**Regulatory and Compliance Considerations:** Organizations operating in regulated industries, such as finance, healthcare, or government, need to comply with specific security and privacy regulations. Introducing short-lived certificates may require organizations to reassess their compliance measures and ensure that the integration aligns with regulatory requirements.

**Performance and Scalability:** Implementing short-lived certificates at large scale may have implications on system performance and scalability. The generation, distribution, and validation processes need to be optimized to handle large numbers of certificates and authentication requests efficiently. Resolving performance bottlenecks and ensuring smooth operation under high loads is essential for successful deployment.

**Cost and Resource Implications:** Integrating short-lived certificates may involve additional costs and resource requirements. Organizations need to evaluate the financial implications of implementing and maintaining the necessary infrastructure, tools, and processes. Balancing the costs with the anticipated security benefits is a crucial consideration.

Addressing these complicated and unresolved issues requires a multidisciplinary approach involving experts in security, cryptography, system architecture, and user experience. Further research, collaboration, and experimentation are needed to develop best practices, standards, and guidelines for the successful integration of short-lived certificates into the zero-trust security model.

Regardless of the mentioned complications our model has various advantages and capabilities as well such as:

**Enhanced Security:** Our model incorporates the use of short-lived certificates, which adds an extra layer of security compared to traditional long-lived certificates. Short-lived certificates reduce the window of opportunity for attackers to exploit compromised or stolen certificates. By continuously generating and renewing certificates within short duration's, we minimize the potential risks associated with certificate-based authentication.

**Implementation Simplicity:** Our model focuses on a command-line interface (CLI) implementation, which simplifies the deployment and integration process. Unlike systems that require complex login pages and database setups, our CLI implementation reduces complexity and avoids the introduction of additional trust assumptions. This simplicity contributes to easier adoption and integration into existing systems, making it more accessible for organizations across different sectors.

**Zero-Trust Principles Adherence:** Our model strictly adheres to the principles of the zero-trust model, particularly the ”Never Trust, Always Verify” principle. By mandating continuous authentication, authorization, and validation of users both inside and outside the organization’s network, our model establishes a robust security posture. This approach eliminates the reliance on implicit trust assumptions and ensures that access to resources is based on verified and authenticated user identities.

**Focused Scope and Objectives:** Our model specifically addresses the vulnerabilities and risks associated with traditional security models, particularly in sectors like banking, health, education, and more. We concentrate on the use of short-lived certificates and their management, providing a targeted solution to enhance security in online transactions. This focused approach allows us to address specific pain points and deliver a more effective solution.

**Continuous Validation:** Our model emphasizes continuous validation of user credentials and certificates throughout the active session. By constantly verifying the authenticity and validity of certificates, we ensure that access to resources remains secure, even in dynamic environments. This continuous validation mechanism provides an additional layer of protection against unauthorized access and potential security breaches.

**Adaptability and Scalability:** Our model is designed to be adaptable and scalable, allowing for integration into existing systems and infrastructure. It can be applied across different sectors, accommodating various organizational needs and requirements. This adaptability and scalability make our model suitable for organizations of different sizes, from small businesses to large enterprises.

By incorporating short-lived certificates, adhering to zero-trust principles, maintaining implementation simplicity, and providing continuous validation, our model offers a more robust and secure approach to safeguarding systems. It addresses the limitations of traditional security models and provides practical solutions for sectors like banking, healthcare, education, and more.

## VIII. Future Work

Our implementation showcased the feasibility of integrating short-lived certificates into the Zero Trust model. However, an area that warrants further exploration is the automation of the certificate request and issuance process for clients. This would involve developing a sophisticated client software that facilitates seamless certificate request and presentation to the intended server. Future research could focus on creating and integrating such software, connecting it directly to the certificate authority and servers. This development holds immense potential in streamlining and enhancing certificate management within the Zero Trust architecture, making it an exciting avenue for further exploration.

## IX. Conclusion

In conclusion, our project has successfully integrated short-lived certificates into the zero-trust security model, yielding continuous verification and a substantial reduction in the risk of unauthorized access. Through extensive research and meticulous implementation, we have enhanced security measures, mitigated vulnerabilities, and established a robust solution to safeguard sensitive information and systems from potential cyber threats. By embracing the concept of short-lived certificates and upholding the fundamental principle of ”Never Trust, Always Verify,” we have established a solid and dependable framework for secure authentication within the zero-trust paradigm.

## References

[1] Hsu, Yung-Kao, and Stephen Seymour. ”Intranet security framework based on short-lived certificates.” Proceedings of IEEE 6th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises. IEEE, 1997.

[2] Iță, C. R., Constantinescu, R. C., Vlădescu, A., Alexandrescu, B. (2023, March). Security in remote access, based on zero trust model concepts and SSH authentication with signed certificates. In Advanced Topics in Optoelectronics, Microelectronics, and Nanotechnologies XI (Vol. 12493, pp. 684-691). SPIE.

[3] Jakkal, V. (2021, June 30). The critical role of Zero Trust in securing our world. Microsoft. Retrieved from https://www.microsoft.com/en-us/security/blog/2021/06/30/the-critical-role-of-zero-trust-in-securing-our-world/

[4] Kondaveety, Vijaya Bhaskar, Hemraj Lamkuche, and Suneel Prasad. ”A zero trust architecture for next generation automobiles.” AIP Conference Proceedings. Vol. 2519. No. 1. AIP Publishing LLC, 2022.

[5] Radić, D. (2023). SSL Stats for Secure Browsing in 2023. SerpWatch. Retrieved from https://serpwatch.io/blog/ssl-stats/

[6] S. Sciancalepore, A. Capossele, G. Piro, G. Boggia and G. Bianchi, ”Key management protocol with implicit certificates for IoT systems”, Proc. Workshop IoT challenges Mobile Ind. Syst., pp. 37-42, May 2015.

[7] S. M. Farooq, S. M. Hussain, S. Kiran and T. S. Ustun, ”Certificate based security mechanisms in vehicular adhoc networks based on IEC 61850 and IEEE WAVE standards”, Electronics, vol. 8, no. 1, pp. 96, 2016.

[8] Stafford, V. A. ”Zero trust architecture.” NIST Special Publication 800 (2020): 207.

[9] Zhong, Y., Zhou, M., Li, J., Chen, J., Liu, Y., Zhao, Y., Hu, M. (2021). Distributed blockchain-based authentication and authorization protocol for smart grid. Wireless Communications and Mobile Computing, 2021, 1-15.

## Appendix: Software Description

In this appendix, we provide a concise description of the software that was developed or used during the implementation of our research. These software tools played a crucial role in designing and implementing our public key infrastructure (PKI), ensuring secure transmission of keys and certificates, and facilitating the deployment of our research findings.

### *OpenSSL*

OpenSSL served as a fundamental tool in our research, enabling us to design and manage our public key infrastructure effectively. We utilized OpenSSL commands to generate and configure various types of certificates, including root certificates, subordinate certificates, client certificates, and server certificates. By leveraging the robust cryptographic capabilities of OpenSSL, we ensured the integrity and security of our PKI.

### *Secure Copy (SCP)*

To maintain the confidentiality and integrity of our keys and certificates during transmission, we relied on the Secure Copy (SCP) protocol. SCP, which utilizes the SSH (Secure Shell) protocol's public key and private key encryption, provided a secure file transfer mechanism. Through SCP, we securely transferred our keys and certificates between different systems, safeguarding them against unauthorized access or tampering.

### *Nginx Web Server*

As part of our implementation, we used Nginx web server (Server A) to host our protected web server. Nginx, known for its high performance and scalability, allowed us to serve web content securely. We leveraged Nginx's built-in SSL/TLS support to enable encrypted communication between clients and the web server, enhancing the overall security of our system.

By employing OpenSSL, SCP, and Nginx, we established a comprehensive software stack that supported the design and implementation of our research. These software tools provided the necessary functionality, security measures, and deployment capabilities to ensure the success of our project.

### *Additional Tools and Libraries*

In addition to the aforementioned software, we also made use of various other tools and libraries to support different aspects of our research. These included cryptographic libraries for key generation and encryption operations, scripting languages for automating tasks, and monitoring tools to ensure the availability and performance of our system.

It is worth noting that the software and tools used in our implementation were carefully selected based on their compatibility, reliability, and security features, enabling us to deliver a robust and secure solution.