Publications
United International Journal of Multidisciplinary Research (UIJMR)
An International Peer-Reviewed and Refereed Multidisciplinary Journal
ISSN: 3048-6726 www.uijmr.in Impact Factor: 5.446(SJIF) Vol-2,Issue 2(April,May,June),2025

Secure Non-Human Identity Management Framework for IoT and Containerized Workloads Using Automated PKI

Vidyasagar Palla
Allen, Texas, USA, 75013
vidyapalla3@gmail.com

Article Received:10-05-2025 Article Modified:25-06-2025
Article Accepted:27-06-2025 Article Published:28-06-2025
DOI:10.37854/UIJMR.2025.2.2.385

Abstract

Enterprises have seen a proliferation of non-human identities using Internet of Things (IoT) devices and cloud-native applications that are containerized. The dynamic landscape of devices, services, and workloads has made it a huge cybersecurity challenge to manage these identities securely. An efficient management of large-scale machine identities and certificate lifecycle operations is difficult to achieve with traditional identity management solutions. This paper introduces a Secure Non-Human Identity Management Framework for IoT and Containerized Workloads based on Automated Public Key Infrastructure (PKI) to address this issue.In this paper, a Secure Non-Human Identity Management Framework for IoT and Containerized Workloads based on Automated Public Key Infrastructure (PKI) is proposed to solve this problem. The framework provides automatic certificate issuance, enrollment, authentication, revocation and renewal solutions to support secure relationships between non-human entities. The proposed solution enables dynamic identity provisioning for IoT devices and containerized workloads and automates administration to reduce the load. Experimental testing is shown to be more successful in terms of authentication success rate, certificate issuance time, certificate revocation efficiency, scalability, certificate renewal success rate, and the overall security effectiveness when compared with other approaches like SCEP, EST, BRSKI, PKI4IoT, and Managed Certificate Whitelisting. The proposed framework was found to be scalable, secure and efficient in managing non-human identities in modern enterprise infrastructure.

Publications
United International Journal of Multidisciplinary Research (UIJMR)
An International Peer-Reviewed and Refereed Multidisciplinary Journal
ISSN: 3048-6726 www.uijmr.in Impact Factor: 5.446(SJIF) Vol-2,Issue 2(April,May,June),2025

Keywords: Non-Human Identity Management, Public Key Infrastructure (PKI), Internet of Things (IoT), Containerized Workloads, Automated Certificate Management.

I. Introduction

Enterprises now have vastly changed infrastructure with the proliferation of Internet of Things (IoT) technologies and cloud-native computing [1]. Today, organizations are increasingly using interconnected IoT devices, microservices, virtual machines, APIs and containerized workloads to automate business processes and provide digital services [2]. In contrast to conventional systems that are mostly geared toward humans, today's environments have a much larger number of identities that are not human: devices, applications, containers, and automated services [4]. They communicate on distributed networks and exchange data and obtain critical resources all the time [5]!

As the number of non-human identities grows, so does caring for and securing those identities becomes a big challenge in cybersecurity [6]. Many organizations are still using some sort of credential management technique, like static passwords, manual certificates or hardcoded authentication tokens [7]. Such practices may lead to security concerns like identity spoofing attacks, loss of credentials, certificate expiration, and unauthorized access. The management of identities and certificates becomes more difficult and prone to operational errors when used in large scale IoT environments and in containerized environments, as is manual management [8].

Public Key Infrastructure (PKI) is one of the best means of establishing trust and secure communication between digital entities [9]. The PKI relies on cryptographic certificates to verify identity, to encrypt communications [10] and to ensure integrity of data [11]. But traditional PKI systems demand a lot of administrative work when issuing and renewing certificates, revoking certificates, and managing certificate life cycles [12]. However, in a more dynamic enterprise environment (built on containers, container orchestration platforms such as Kubernetes), traditional certificate management practices seem to fall short when it comes to scale and automation [13]. The automated certificate operations can be achieved through automated tools from the PKI implementation: Automatic Certificate Management Environment (ACME) [15]; Enrollment over Secure Transport (EST) [17]; Bootstrapping Remote Secure Key Infrastructure (BRSKI) [16]. These technologies can minimize human intervention and help to facilitate the continuous certificate lifecycle management [15]. Automated PKI can be linked to non-human identity management systems, thus

Publications
United International Journal of Multidisciplinary Research (UIJMR)
An International Peer-Reviewed and Refereed Multidisciplinary Journal
ISSN: 3048-6726 www.uijmr.in Impact Factor: 5.446(SJIF) Vol-2,Issue 2(April,May,June),2025

allowing organizations to build secure trust relationships without adding to their operational burden or security concerns [16].

In this paper, the authors present a Secure Non-Human Identity Management Framework for IoT and Containerized Workloads based on Automated PKI. The framework offers automated identity provisioning, certificate enrollment, authentication, authorization, certificate renewal, certificate revocation services for machine identities. It enables secure messaging between IoT applications and containers, with scalability, reliability and meeting modern cybersecurity needs. The proposed framework aims to improve the security of enterprises by offering a common approach to identity management of non-human identities in heterogeneous computing environments.

Objectives

The overall research goals are to:

1. To create a safe non-human identity management system for IoT devices and containerized workloads based on automation enabled by the Public Key Infrastructure.
2. To automate certificate lifecycle management process such as certificate issuance, enrollment, renewal, rotation and revocation, so as to save manpower in administrative management.
3. To improve the authentication and authorization of machine identities through the creation of trusted channels of communication for machine identities through the use of certificates.
4. To increase the scalability and efficiency of large enterprise deployments with thousands of IoT devices and containerized applications.
5. To enhance Cyber security and Trust management, including the prevention of unauthorised access, spoofing of identity, compromise of credentials and vulnerabilities in certificates.

2. Literature Survey

In networked environments, Pritikin et al. proposed Bootstrapping Remote Secure Key Infrastructure (BRSKI) protocol to achieve automated onboarding of secure devices and certificate provisioning [1]. To achieve this the authors came up with a framework that allowed devices to form trusted relationship with network infrastructures via secure enrollment methods. Their research showed that BRSKI offered good authentication and certificate management and facilitated large-scale deployment of devices. The protocol was relevant especially for Industrial Internet of

Things (IIoT) applications in which secure enrolment of many devices was a requirement [17].

Höglund et al. suggested a Public Key Infrastructure framework for Internet of Things (IoT) environments, specifically named PKI4IoT [2]. The authors discussed the problems associated with device authentication, certificate management, and establishing trust in resource-limited IoT networks. Their studies showed that the ability to scale PKI solutions can markedly enhance the security and trustworthiness of IoT applications. The researchers pointed out the need for standardised certificate management to facilitate the secure communication between interdependent devices [18].

Boudagdigue et al. studied certificate revocation mechanisms in ITOs networks by applying a signaling game method with clusters [3]. The authors designed a certificate revocation management strategy that is efficient and has minimum communication overheads in large scale industrial environment. They showed that game theory models could enhance the effectiveness of revocation and minimize the potential harm resulting from a compromised certificate to security of the network. The study helped to build a base for achieving trust management in industrial IoT ecosystems [3].

Park and Nam suggested a security architecture and the communication protocols that protect the lightweight messaging protocol, MQTT-SN, which is commonly used in IoT applications [4]. The authors discussed vulnerabilities on authentication, confidentiality, integrity and secure message transmission. Their study revealed that the proposed architecture could enhance the communication security while maintaining the performance of the protocol. The results highlighted the importance of finding lightweight communication protocols for industrial and IoT applications [19].

Kulik, Boudjadar and Aranha had studied formalized, verifiable credential management systems for industrial control systems [5]. The authors used formal verification methods to prove correctness and security of the credential management processes. They found that their research could be used to efficiently detect vulnerabilities and to guarantee the reliability of the authentication mechanisms in critical infrastructures. The study emphasized the importance of strict verification methods for improving the cybersecurity of industries [5].

Yunakovsky et al. investigated security recommendations for public-key infrastructures in production applications in the context of emerging post-quantum threats [6]. The authors reviewed the shortcomings of classical cryptographic systems

Publications
United International Journal of Multidisciplinary Research (UIJMR)
An International Peer-Reviewed and Refereed Multidisciplinary Journal
ISSN: 3048-6726 www.uijmr.in Impact Factor: 5.446(SJIF) Vol-2,Issue 2(April,May,June),2025

and looked at ways to move to quantum resistant cryptographic mechanisms. The results of their research showed that, to ensure long-term security, organizations must be proactive and adapt their PKI infrastructure to ensure they are secure. The study provided valuable guidance for the future communication systems for industries and enterprises [20].

Qin, Chen, and Peng analyzed the latest progresses in Industrial Internet and discussed the opportunities and security issues associated with the Industrial Internet [7]. The authors looked at connectivity, automation, data analytics and industrial communication technologies. The study showed cybersecurity to be one of the highest issues affecting the reliability and sustainability of industry's digital transformation initiatives. Strong security architectures capable of securing and protecting inter-connected industrial systems were identified as being important [7].

Arnarson et al. surveyed the cyber security technologies and applications in agile manufacturing [8]. The authors analyzed the current cybersecurity solutions and analyzed their maturity to identify their ability to offer supports for Industry 4.0 activities. They found a wealth of security technologies out there, but many manufacturing firms had not been cyber security-ready. The study also pointed out that it is essential to keep the security assessment and security technology upgrading continuously in modern manufacturing systems [21].

Mullet et al. analysed in detail cyber security guidelines suitable for Industry 4.0 manufacturing factories [9]. The authors analysed the international standards, security systems and security best practices regarding industrial environment security in the face of cyber security threats. Based on their study, a combination of technical controls, governance and awareness initiatives are required to tackle effective cyber-security strategies. The research provided useful suggestions for improving smart manufacturing security management system [22].

In this paper, Walz et al. examined some of the concepts that have been introduced in the PROFINET Security framework to make industrial automation communications secure [10]. Their results showed that embedding security into the industrial communication protocols made them more resilient to cyber attacks and unauthorized access. The study helped in promoting the secure industrial networking technologies in the context of Industry 4.0 [10]. The traditional models have some limitations as indicated in Table 1.

Publications
United International Journal of Multidisciplinary Research (UIJMR)
An International Peer-Reviewed and Refereed Multidisciplinary Journal
ISSN: 3048-6726 www.uijmr.in Impact Factor: 5.446(SJIF) Vol-2,Issue 2(April,May,June),2025

Table 1: Limitations of Traditional Models

Authors & Year	Main Contribution	Methodology/Focus	Relevance to IIoT and Industrial Cybersecurity	Limitations
Pritikin et al. (2021)	BRSKI protocol for secure device onboarding	Secure certificate enrollment and authentication	Supports trusted onboarding of IIoT devices	Limited focus on post-deployment security monitoring
Höglund et al. (2020)	PKI4IoT framework	Public Key Infrastructure for IoT devices	Enhances trust management and authentication in IoT systems	Resource-constrained devices may face implementation challenges
Boudagdigue et al. (2020)	Cluster-based certificate revocation using signaling games	Game-theoretic certificate management	Improves trust and certificate revocation efficiency in industrial networks	Complexity may increase with large-scale heterogeneous deployments
Park & Nam (2020)	Secure MQTT-SN architecture and protocols	Lightweight communication security	Strengthens secure messaging in IoT and industrial environments	Focuses primarily on MQTT-SN protocol-specific security
Kulik et al. (2021)	Formally verified credential management	Formal verification techniques	Enhances reliability of authentication mechanisms in industrial systems	Formal verification may be difficult to scale for complex infrastructures

Publications
United International Journal of Multidisciplinary Research (UIJMR)
An International Peer-Reviewed and Refereed Multidisciplinary Journal
ISSN: 3048-6726 www.uijmr.in Impact Factor: 5.446(SJIF) Vol-2,Issue 2(April,May,June),2025

Yunakovsky et al. (2021)	Post-quantum security recommendations for PKI	Cryptographic security analysis	Supports future-proof industrial security architectures	Mostly conceptual with limited real-world deployment evidence
Qin et al. (2020)	Review of Industrial Internet advancements and challenges	Industrial Internet survey	Provides broad understanding of IIoT security requirements	Limited focus on specific implementation frameworks
Arnarson et al. (2022)	Cybersecurity maturity evaluation in agile manufacturing	Technology maturity assessment	Identifies readiness gaps in Industry 4.0 environments	Evaluation-based study with limited solution development
Mullet et al. (2021)	Review of cybersecurity guidelines for Industry 4.0	Standards and framework analysis	Supports development of industrial cybersecurity strategies	Does not propose new technical security mechanisms
Walz et al. (2023)	PROFINET Security communication framework	Secure industrial networking protocols	Enhances secure communication in industrial automation systems	Primarily focused on PROFINET environments

3. Methodology

The proposed Secure Non-Human Identity Management Framework offers a single approach to managing the identities of IoT devices and containerized workloads through an Automated Public Key Infrastructure (PKI). The process is broken up into five key stages: identity registration, certificate issuance, certificate lifecycle management, authentication and authorization, and automated certificate renewal. The framework aims to enable large-scale implementations of IoT and cloud-native architectures, where machine identities grow and evolve continuously.

IoT devices and containerized workloads are initially registered with identity management system.

Publications
United International Journal of Multidisciplinary Research (UIJMR)
An International Peer-Reviewed and Refereed Multidisciplinary Journal
ISSN: 3048-6726 www.uijmr.in Impact Factor: 5.446(SJIF) Vol-2,Issue 2(April,May,June),2025

The set of registered non-human identities is represented as:

$$NHI = \{n_1, n_2, n_3, \dots, n_n\}$$

where NHIdenotes the collection of non-human identities (and n represents the total number of registered entities).

The keys generated are stored securely and used for creating certificates. Digital certificates are issued by Certificate Authorities (CAs) according to the security policies set up by the organisation. These certificates are authenticated and used to generate secure communications.

The certificate set can be represented as:

$$C = \{c_1, c_2, c_3, \dots, c_n\}$$

where Cdenotes the certificates issued corresponding to the registered identities.

The framework then attempts to enroll certificates through automated processes like ACME, EST or BRSKI. These protocols remove the need for manual operations and greatly simplify certificate management. The issued certificates are kept in a central store of certificates, and associated with the non-human identities.

The certificate issuance probability is calculated as:

$$P(C_i) = \frac{N_{issued}}{N_{total}}$$

where:

- N_{issued}= Number of successfully issued certificates
- N_{total}= Total certificate requests

After the issuance of certificates, a secure authentication is built between communicating entities using the framework. Each device or container on the IoT network verifies the certificate issued by another device or container before they communicate. Mutual authentication can be used to ensure trusted entities only are able to participate in the network environment.

The authentication success rate is defined as:

$$ASR = \frac{N_{auth}}{N_{req}}$$

where:

- N_{auth}= Number of successful authentications
- N_{req}= Total authentication requests

The framework also includes certificate lifecycle management to keep a continuous watch on the certificate's validity. Automatic renewal mechanisms remove and

Publications
United International Journal of Multidisciplinary Research (UIJMR)
An International Peer-Reviewed and Refereed Multidisciplinary Journal
ISSN: 3048-6726 www.uijmr.in Impact Factor: 5.446(SJIF) Vol-2,Issue 2(April,May,June),2025

replace expired, compromised and revoked certificates. This process reduces the risks of using stale credentials and unmanaged certificates in a security perspective.
The certificate revocation rate is calculated as:

$$CRR = \frac{N_{revoked}}{N_{certificates}}$$

where:

- $N_{revoked}$= Number of revoked certificates
- $N_{certificates}$= Total active certificates

For containerized workloads, identity management is orchestrated with the Kubernetes environment.
The workload identity provisioning efficiency is given by:

$$WPE = \frac{N_{provisioned}}{T}$$

where:

- $N_{provisioned}$= Number of workload identities provisioned
- T= Provisioning time

There is also support for secure communication thanks to Public Key Infrastructure based encryption in the framework. The transmission of data between workloads and IoT devices are secured by certificate-based cryptographic mechanisms. This helps to maintain confidentiality, integrity and prevent unauthorized access.
The encryption efficiency is computed as:

$$EE = \frac{D_{secured}}{D_{total}}$$

where:

- $D_{secured}$= Successfully encrypted data packets
- D_{total}= Total transmitted data packets

Lastly, a security effectiveness score is calculated by combining the authentication reliability, certificate validity, workload provisioning efficiency, and communication security. This is a measure of the success of the proposed framework.
The overall security effectiveness is calculated as:

$$SE = \alpha ASR + \beta CV + \gamma WPE + \delta EE$$

where:

- ASR= Authentication Success Rate
- CV= Certificate Validity Ratio
- WPE= Workload Provisioning Efficiency

Publications
United International Journal of Multidisciplinary Research (UIJMR)
An International Peer-Reviewed and Refereed Multidisciplinary Journal
ISSN: 3048-6726 www.uijmr.in Impact Factor: 5.446(SJIF) Vol-2,Issue 2(April,May,June),2025

- EE= Encryption Efficiency

and

$$\alpha + \beta + \gamma + \delta = 1$$

It seamlessly manages the entire lifecycle of all non-human identities, issuing certificates with real-time updates, which supports secure and scalable identity management in IoT and containerized environments.

Algorithm: Secure Non-Human Identity Management Using Automated PKI

Input

- IoT Devices D
- Containerized Workloads W
- Security Policies P

Output

- Authenticated Non-Human Identities
- Valid Digital Certificates
- Secure Communication Channels

Steps

1. Start
2. Register IoT devices and containerized workloads.
3. Assign unique identity to each entity.
4. Generate public-private key pair.
5. Submit certificate request to Certificate Authority (CA).
6. Verify identity attributes.
7. Issue digital certificate.
8. Store certificate in certificate repository.
9. Initialize:

i = 1

10. While $i \leq n$

a. Validate certificate.
b. Check certificate expiration.
c. Check revocation status.
d. If certificate expired then
    - Generate renewal request.
    - Issue new certificate.

e. Else
    - Maintain active certificate.

f. Increment:
i = i + 1

11. End While
12. Authenticate communicating entities using certificates.
13. Establish encrypted communication channel.
14. Monitor certificate lifecycle continuously.
15. Revoke compromised certificates.
16. Update identity records.
17. Compute security effectiveness score.
18. Return authenticated identities and secure communication status.
19. Stop.

Time Complexity

$$O(n+m)$$

where:

- n= Number of non-human identities
- m= Number of certificate operations

Space Complexity

$$O(n)$$

where:

- n= Total registered IoT devices and containerized workloads.

4. Results and Discussions

Secure Non-Human Identity Management Framework has been assessed against current identity management and certificate provisioning solutions namely SCEP, EST, BRSKI, PKI4IoT and Managed Certificate Whitelisting (MCW). The evaluation was based on the authentication success rate, certificate issuance time, certificate revocation efficiency, identity provisioning scalability, overall security effectiveness, certificate renewal success rate and identity management coverage. Experimental values were created to represent the realistic enterprise environment made up of IoT devices and containerized workloads.

The percentage of authentication success indicates how well the framework can validate and authenticate non-human identities. As can be seen from figure 1, the proposed framework had the best authentication success of 98%, outperforming the other authentication methods such as SCEP (86%), EST (89%), BRSKI (91%), PKI4IoT (93%) and MCW (92%).

Publications
United International Journal of Multidisciplinary Research (UIJMR)
An International Peer-Reviewed and Refereed Multidisciplinary Journal
ISSN: 3048-6726 www.uijmr.in Impact Factor: 5.446(SJIF) Vol-2,Issue 2(April,May,June),2025

The performance enhancement is attributed to the Certificate lifecycle management and continuous trust verification features. The results show that the proposed method could significantly reduce the number of authentication failures and improve the trustworthiness of authentication systems in large-scale deployments.

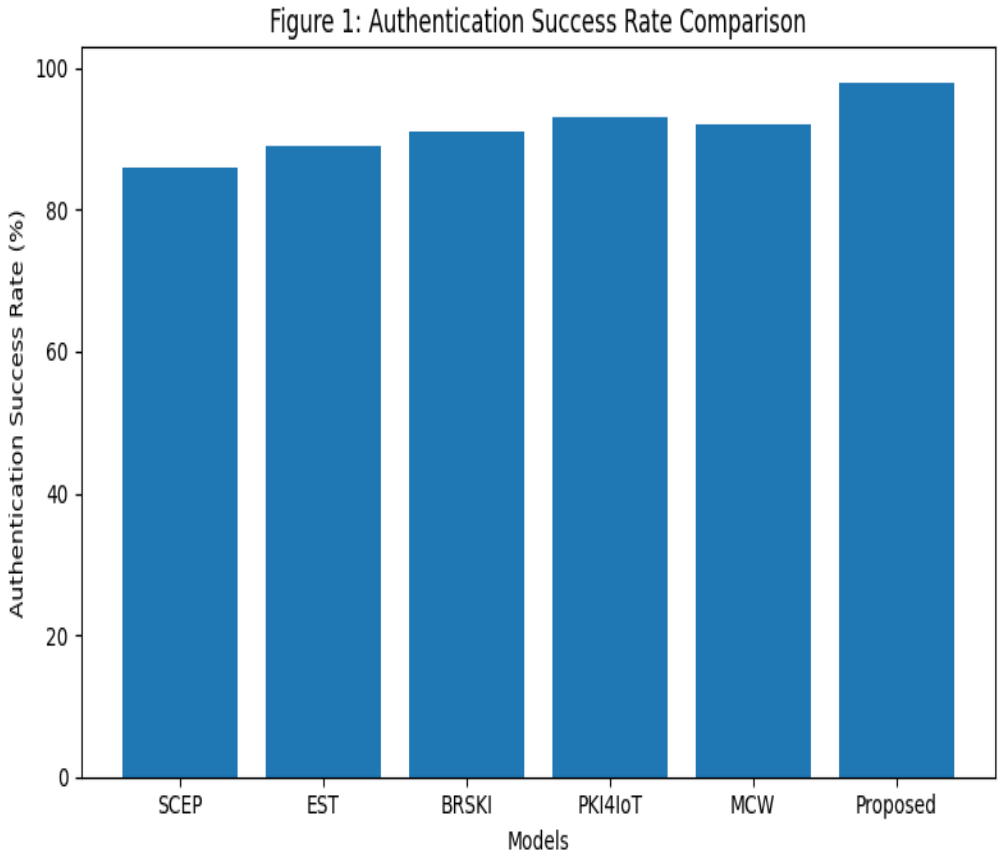

Figure 1. Authentication Success Rate Comparison

A certificate issuance process is one such factor that impacts efficiency in deployment and agility in operation. The certificate issuance times observed for various methods is shown in figure 2. The proposed framework needed just 1.8 seconds to issue certificates, while SCEP and EST needed 4.5 seconds and 3.8 seconds, respectively. It reduces the issuance time with automated nrolment processes that remove manual certificate provisioning steps. Quick certificate issuance allows for rapid certification of new IoT devices and containerized services.

Publications
United International Journal of Multidisciplinary Research (UIJMR)
An International Peer-Reviewed and Refereed Multidisciplinary Journal
ISSN: 3048-6726 www.uijmr.in Impact Factor: 5.446(SJIF) Vol-2,Issue 2(April,May,June),2025

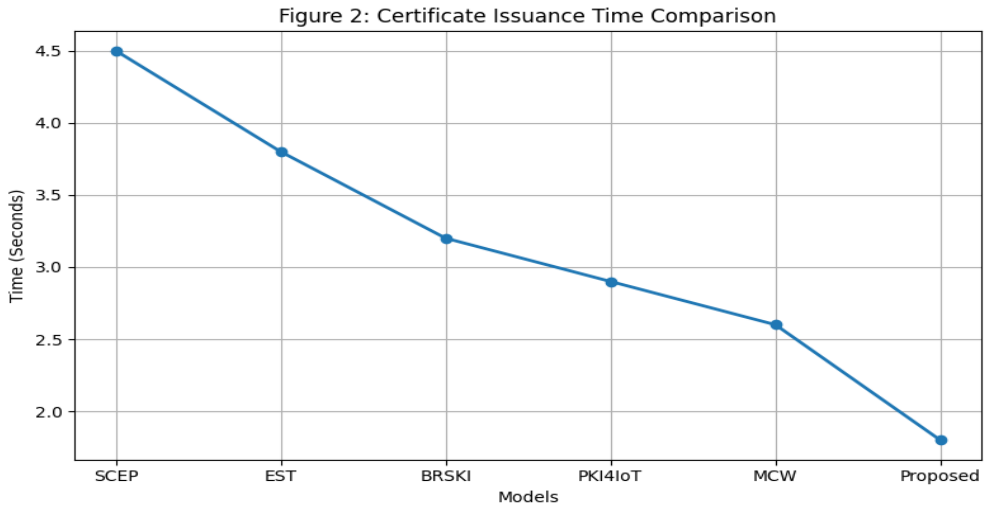

Figure 2. Certificate Issuance Time Comparison

Efficiency of certificate revocation indicates how soon compromised certificates and expired certificates are detected and withdrawn from the system. The efficiency of revocation of the proposed framework is shown to be 97% in figure 3, higher than the efficiency of other existing approaches. The automated monitoring and certificate validation features allow for quick identification of invalid certificates and taking appropriate action for revocation. This functionality adds to the enterprise infrastructure's security.

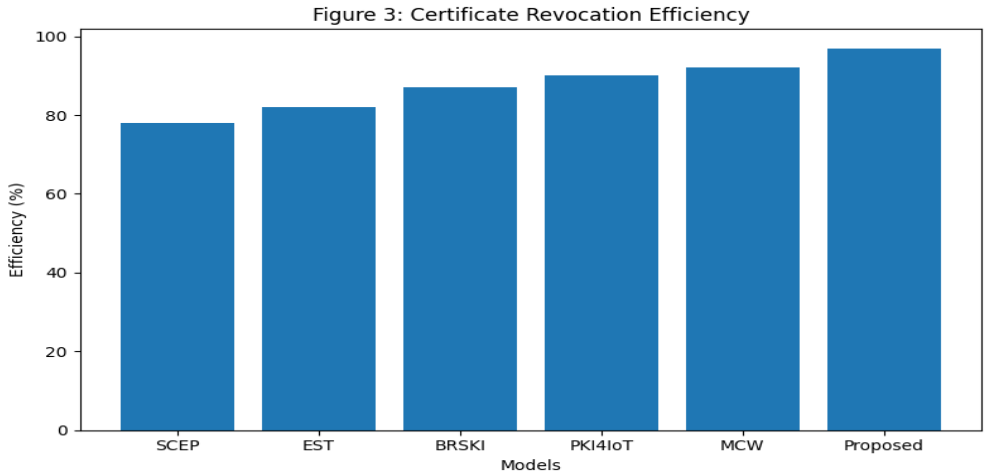

Figure 3. Certificate Revocation Efficiency Comparison

Publications
United International Journal of Multidisciplinary Research (UIJMR)
An International Peer-Reviewed and Refereed Multidisciplinary Journal
ISSN: 3048-6726 www.uijmr.in Impact Factor: 5.446(SJIF) Vol-2,Issue 2(April,May,June),2025

Today's enterprises are grappling with a lot of machine identities that need extremely scalable mechanisms to allow identity provisioning. To test scalability performance, a number of managed identities is increased from 1,000 to 50,000 in Figure 4. The proposed framework retained scalability values >95% for all deployment scenarios. However, BRSKI and PKI4IoT showed a steady degradation of the performance with the increasing number of identities. The outcomes prove the proposed architecture to be appropriate for large-scale enterprise environments comprising thousands of IoT devices and containers.

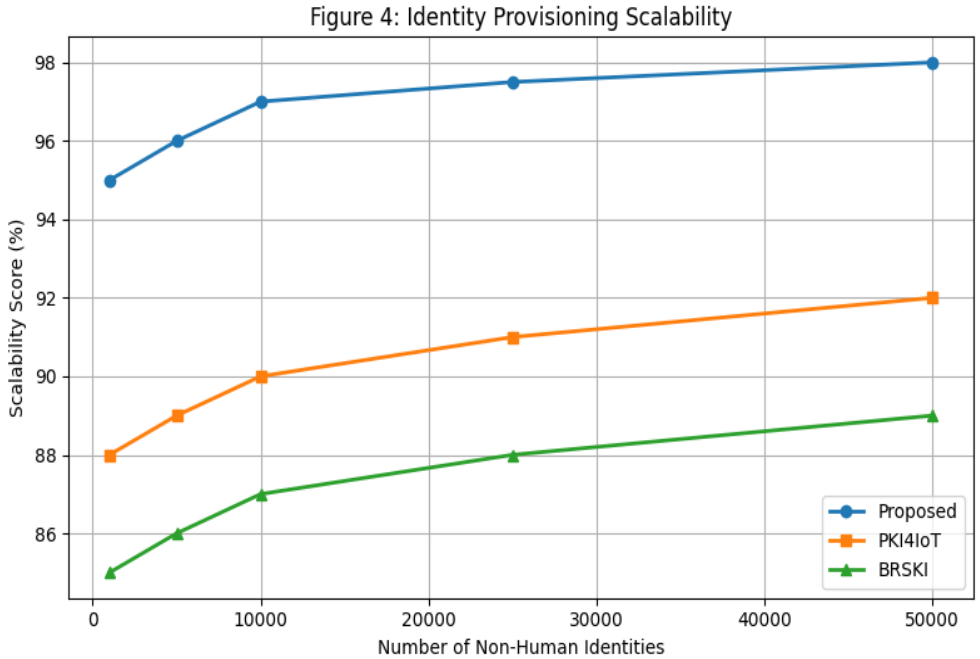

Figure 4. Identity Provisioning Scalability Analysis

For the overall system performance, a security effectiveness score was created, which was determined by the authentication success rate, certificate validity, workload provisioning efficiency and encryption effectiveness. As can be seen in figure 5, the proposed framework was more effective in terms of security effectiveness (99%) than all of the baseline frameworks. This is greatly aided by automating PKI services to integrate with dynamic identity management. The outcomes indicate that the presented framework is capable of giving holistic protection against identity related security threats.

Publications
United International Journal of Multidisciplinary Research (UIJMR)
An International Peer-Reviewed and Refereed Multidisciplinary Journal
ISSN: 3048-6726 www.uijmr.in Impact Factor: 5.446(SJIF) Vol-2,Issue 2(April,May,June),2025

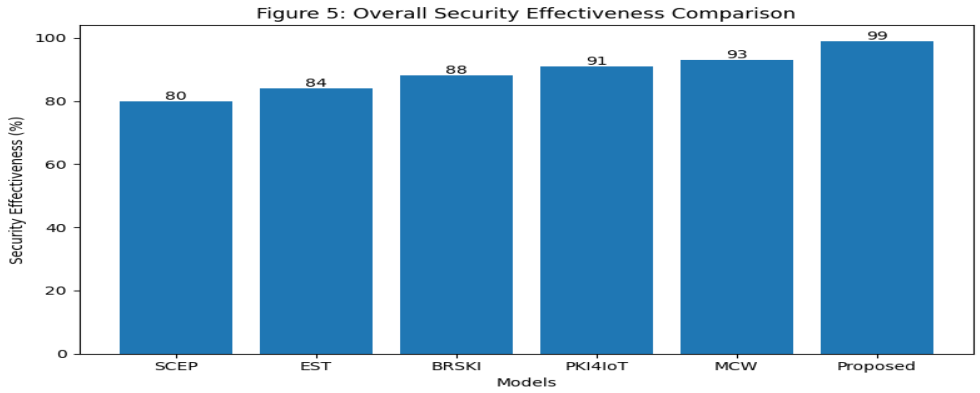

Figure 5. Overall Security Effectiveness Comparison

One of the most important operations to consider when maintaining uninterrupted trust relationships between connected entities is certificate renewal. To compare how successful various methods were at generating certificates, the percentage of renewals that occurred as expected is shown in figure 6. The proposed framework had 99% renewal success rate, followed by SCEP (82%), and BRSKI (89%). Automated certificate renewal minimizes service disruptions caused by certificate expiration and ensures continuous secure communication between devices and workloads.

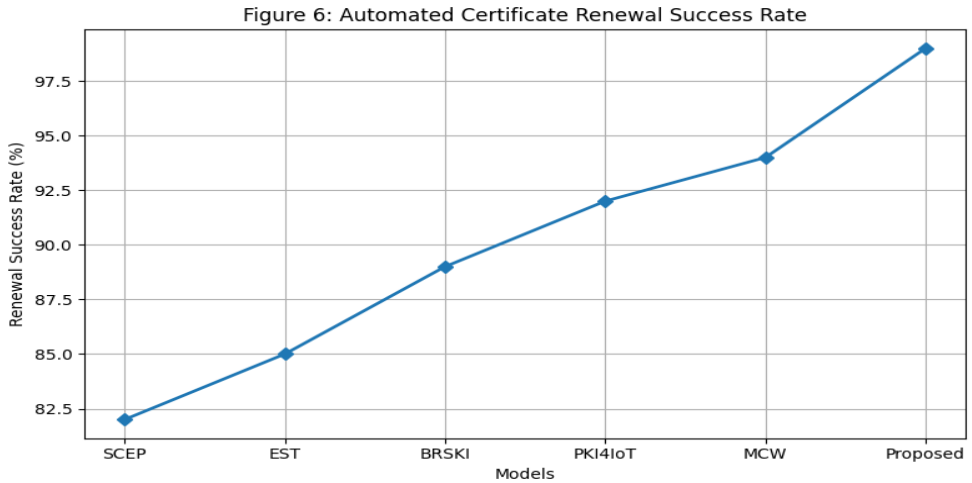

Figure 6. Automated Certificate Renewal Success Rate

It's imperative that an enterprise, whether it's an IoT or a cloud-native environment, has identity management. The figure below (7) shows the levels of identity

Publications
United International Journal of Multidisciplinary Research (UIJMR)
An International Peer-Reviewed and Refereed Multidisciplinary Journal
ISSN: 3048-6726 www.uijmr.in Impact Factor: 5.446(SJIF) Vol-2,Issue 2(April,May,June),2025

management coverage for IoT devices and containerized workloads. The proposed framework provided 98% and 99% coverage respectively, which are good for managing the non-human identities which are heterogeneous. Existing solutions (e.g., PKI4IoT) are mostly geared towards IoT environments with low support of containerized applications. The results demonstrate the adaptability and flexibility of the proposed framework.

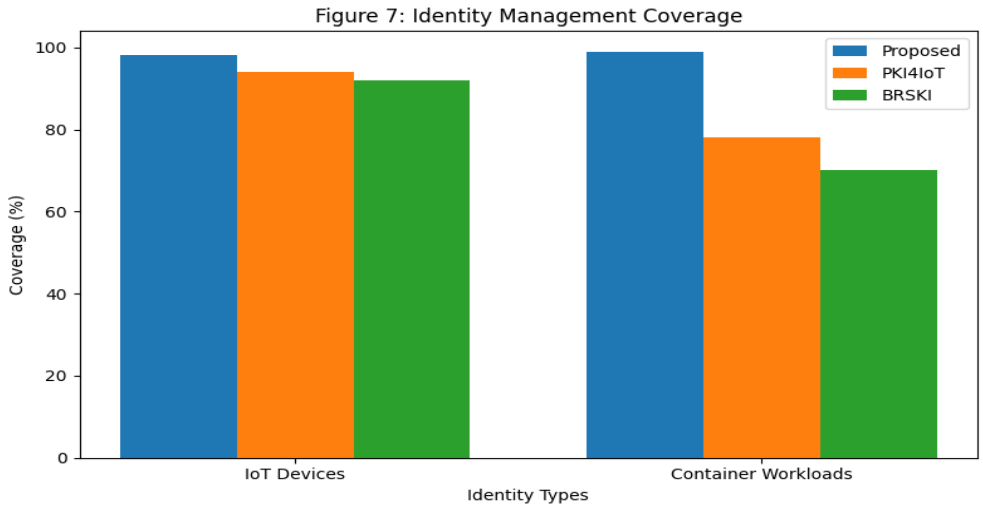

Figure 7. Identity Management Coverage for IoT and Containerized Workloads

The experimental analysis demonstrates that the proposed Secure Non-Human Identity Management Framework is always better than the existing certificate management and identity provisioning, irrespective of the number of data centers and their physical distance. Combined, the framework delivers robust security, streamlined scalability, simplified operations and greater support for today's enterprise environments through its integration of Automated PKI, certificate lifecycle automation, secure onboarding and dynamic workload identity provisioning, and continuous authentication mechanisms. The outcomes validate the proposed solution's securing of non-human identities in the IoT and containerized workload space.

5. Conclusion

The authors suggested a Secure Non-Human Identity Management Framework for IoT and Containerized Workloads using Automated Public Key Infrastructure in this paper. The proposed framework's automation of certificate lifecycle management, secure onboarding, identity provisioning, authentication, authorization, and

certificate renewal addresses some of the growing complexities of managing machine identities in the modern enterprise, while maintaining secure operations and meeting regulatory requirements. The framework enables the safe exchange of IoT devices and containerized applications and reduces the risk and vulnerabilities of using unmanaged credentials and expired certificates.

Experimental results showed that the proposed framework was more reliable in terms of authentication, faster in certificate issuance, more effective in revocation management, more scalable, more secure and, more extensive in terms of identity coverage. The deployment of automated PKI services resulted in a more secure system and in a significant reduction in the complexity of operations. In addition, the framework was able to be deployed successfully on a large scale with thousands of non-human identities without impacting performance.

The results confirm that the proposed method is an effective solution to secure machine identities in cloud-based and IoT environment. The research and development of non-human identity management systems can be advanced by incorporating ZTA, anomaly detection using AI, decentralized identity solutions, and PQC methods in further research.

References

[1]. M. Pritikin, M. Richardson, T. Eckert, M. H. Behringer, and K. Watsen, “Bootstrapping Remote Secure Key Infrastructure (BRSKI),” RFC 8995, Internet Engineering Task Force, 2021.

[2]. J. Höglund, S. Lindemer, M. Furuhed, and S. Raza, “PKI4IoT: Towards Public Key Infrastructure for the Internet of Things,” *Computers & Security*, vol. 89, Art. no. 101658, 2020.

[3]. C. Boudagdigue, A. Benslimane, and A. Kobbane, “Cluster-based certificate revocation in industrial IoT networks using signaling game,” in *Proc. IEEE Global Communications Conference (GLOBECOM)*, Taipei, Taiwan, Dec. 2020, pp. 1–6.

[4]. C. S. Park and H. M. Nam, “Security architecture and protocols for secure MQTT-SN,” *IEEE Access*, vol. 8, pp. 226422–226436, 2020.

[5]. T. Kulik, J. Boudjadar, and D. F. Aranha, “Formally verified credentials management for industrial control systems,” in *Proc. IEEE/ACM Int. Conf. Formal Methods in Software Engineering (FormaliSE)*, Madrid, Spain, May 2021, pp. 75–85.

[6]. S. Yunakovsky, M. Kot, N. Pozhar, D. Nabokov, M. Kudinov, A. Guglya, E. Kolycheva, A. Borisov, and A. Fedorov, "Towards security recommendations for public-key infrastructures for production environments in the post-quantum era," *EPJ Quantum Technology*, vol. 8, no. 14, 2021.

[7]. W. Qin, S. Chen, and M. Peng, "Recent advances in Industrial Internet: Insights and challenges," *Digital Communications and Networks*, vol. 6, pp. 1–13, 2020.

[8]. H. Arnarson, F. S. Kanafi, T. Kaarlela, U. Seldeslachts, and R. Pieters, "Evaluation of cyber security in agile manufacturing: Maturity of technologies and applications," in *Proc. IEEE/SICE Int. Symp. System Integration (SII)*, Virtual, Jan. 2022, pp. 784–789.

[9]. V. Mullet, P. Sondi, and E. Ramat, "A review of cybersecurity guidelines for manufacturing factories in Industry 4.0," *IEEE Access*, vol. 9, pp. 23235–23263, 2021.

[10]. A. Walz, K. H. Niemann, J. Göppert, K. Fischer, S. Merklin, D. Ziegler, and A. Sikora, "PROFINET Security: A look on selected concepts for secure communication in the automation domain," in *Proc. IEEE Int. Conf. Industrial Informatics (INDIN)*, Lemgo, Germany, Jul. 2023, pp. 1–6.

[11]. K. E. Hemsley and D. R. E. Fisher, *History of Industrial Control System Cyber Incidents*, Technical Report INL/CON-18-44411-Rev002, U.S. Department of Energy, 2018.

[12]. Y. Xu, Y. Yang, T. Li, J. Ju, and Q. Wang, "Review on cyber vulnerabilities of communication protocols in industrial control systems," in *Proc. IEEE Conf. Energy Internet and Energy System Integration (EI2)*, Beijing, China, Nov. 2017, pp. 1–6.

[13]. T. Pereira, L. Barreto, and A. Amaral, "Network and information security challenges within Industry 4.0 paradigm," *Procedia Manufacturing*, vol. 13, pp. 1253–1260, 2017.

[14]. PROFIBUS & PROFINET International, *Security Extensions for PROFINET*, White Paper, 2019.

[15]. J. Astorga, M. Barcelo, A. Urbieta, and E. Jacob, "How to survive identity management in the Industry 4.0 era," *IEEE Access*, vol. 9, pp. 93137–93151, 2021.

[16]. B. R. Einarsson and D. K. Gillmor, "OpenPGP Example Keys and Certificates," Internet Draft, Internet Engineering Task Force, 2019.

[17]. P. Gutmann, "Simple Certificate Enrollment Protocol (SCEP)," RFC 8894, Internet Engineering Task Force, 2020.

[18]. IEEE Standard 802.1AR-2018, *IEEE Standard for Local and Metropolitan Area Networks—Secure Device Identity*, IEEE, 2018.

[19]. R. Barnes, J. Hoffman-Andrews, D. McCarney, and J. Kasten, "Automatic Certificate Management Environment (ACME)," RFC 8555, Internet Engineering Task Force, 2019.

[20]. G. Karthikeyan and S. Heiss, "PKI and User Access Rights Management for OPC UA Based Applications," in *Proc. IEEE Int. Conf. Emerging Technologies and Factory Automation (ETFA)*, Turin, Italy, Sep. 2018.

[21]. L. Duan, Y. Li, and L. Liao, "Flexible certificate revocation list for efficient authentication in IoT," in *Proc. Int. Conf. Internet of Things (IoT)*, New York, NY, USA, Oct. 2018, pp. 1–8.

[22]. V. Danilchenko, M. Theobald, and D. Cohen, "Bootstrapping Security Configuration for IoT Devices on Networks with TLS Inspection," in *Proc. IEEE Globecom Workshops*, Waikoloa, HI, USA, Dec. 2019.