MJoSHT
Malaysian Journal of Science, Health & Technology
[mjosht.usim.edu.my]

Article

Analysis of Trust Models in Public Key Infrastructure: A Systematic Literature Review of Interoperability Challenges

R.Radzali[1,3], A.H. Azni[2,3], Farida Hazwani Mohd Ridzuan[2,3], Nur Hafiza Zakaria[2,3] and Tasnuva Ali[4]

[1]Faculty of Computer Science and Information Computing Technology, New Era University College, Blok B&C, Lot 5, Seksyen 10, Jalan Bukit, 43000 Kajang, Selangor, Malaysia.

[2]CyberSecurity and System Research Unit, Faculty of Science and Technology, Universiti Sains Islam Malaysia, Nilai 71800, Negeri Sembilan, Malaysia.

[3]Faculty of Science and Technology, Universiti Sains Islam Malaysia, 71800, Nilai, Negeri Sembilan, Malaysia.

[4]Department of Electronics and Telecommunication Engineering, Daffodil International University Dhaka, Bangladesh.

Correspondence should be addressed to:
Azni Haslizan binti Ab Halim; ahazni@usim.edu.my

Article Info
Article history:
Received:22 November 2024
Accepted: 22 January 2025
Published: 20 February 2025

Academic Editor:
Azira Khalil

Malaysian Journal of Science, Health & Technology

MJoSHT2025, Volume 11, Issue No. 1
eISSN: 2601-0003

https://doi.org/10.33102/mjosht.v11i1.465

Abstract*— Public Key Infrastructure (PKI) guarantees secure communication and authentication in digital contexts. With the expansion of digital ecosystems, the ability of PKI systems to work together smoothly becomes increasingly important, allowing multiple trust models to be compatible. Nevertheless, several significant challenges must be overcome when merging different trust models. The current body of research does not thoroughly examine these difficulties in various PKI trust models. This study aims to conduct a comprehensive assessment and analysis of the difficulties related to PKI interoperability. The focus will be on trust models such as Cross Certification, Bridge CA, Hierarchical, Hybrid, Cross Recognition, and Certificate Trust Lists. This systematic literature review (SLR) uses the PRISMA technique to analyse trust models in PKI interoperability. The review focuses on peer-reviewed studies published between 2000 and 2024, ensuring transparency and rigor. Eligibility criteria included studies using quantitative methodologies and sourced from major academic databases. This systematic review identified critical challenges in the interoperability of PKI trust models, particularly in operational complexity, security, liability, and scalability. Trust models like Cross Certification, Bridge CA, and Hierarchical systems each present unique challenges when integrated into diverse digital ecosystems. Moreover, gaps in the current research suggest the need for more standardised, scalable solutions that can accommodate the growing complexity of digital infrastructures. Future research should focus on developing a universal model for PKI interoperability, with a particular emphasis on large-scale environments such as E-commerce and E-government systems.

***Keywords*— Key management System (KMS), Interoperability, Public Key Infrastructure (PKI), Comparative analysis**

I. INTRODUCTION

Public Key Infrastructure (PKI) is necessary for ensuring secure digital communications by offering authentication, confidentiality, and integrity using digital certificates. The fundamental elements of PKI encompass Certificate Authorities (CAs), key management, and revocation procedures, all of which are essential for upholding trust in digital transactions [1]. CAs have the responsibility of issuing and overseeing digital certificates, ensuring the accurate association of public keys with their corresponding businesses [2]. Adhering to effective key management techniques is crucial at every stage of a digital certificate's lifespan, including issuance, renewal, and revocation. This is necessary to maintain the security and dependability of PKI systems. PKI remains a fundamental aspect of cybersecurity, but continuous advancements and assessments are required to overcome its limitations and improve its efficiency in a digitalized society. As technology evolves, PKI must adapt and enhance its capabilities to ensure the security of digital transactions and communications. By addressing the challenges and limitations of PKI, organisations can better protect their sensitive information and maintain trust in their digital interactions. Organizations can enhance their cybersecurity defenses and establish a more secure digital ecosystem by staying updated with the latest advancements in PKI technology and adopting optimal strategies. Organizations must prioritize ongoing improvements and innovations in their PKI frameworks to effectively protect their data and stay ahead of cyber threats.

In many areas, especially e-government services and computational grids, interoperability in PKI is challenging because of legal, organizational, and technical differences that make it hard to work together smoothly[3]. The shift to e-signatures using Digital Signature Certificates (DSC) is crucial for authenticity, access control, and data integrity in digital transactions. PKI is widely adopted for secure web applications, ensuring reliable electronic interactions [4]. Additionally, achieving interoperability is further complicated by varying legal frameworks and organizational policies across different countries [5]. This makes it more complicated to maintain trust and rely on certificates. Although these studies emphasise the urgent difficulties in achieving interoperability, they also indicate that creative solutions, such as middleware and trust brokers, could facilitate the integration of PKI in various situations.

Recent studies have emphasised the urgent requirement for a systematic review of these difficulties, pointing out that current solutions frequently fall short of tackling the complete range of problems that arise in PKI interoperability[6][7][8]. With the increasing need for safe and scalable digital infrastructures, it is crucial to create stronger and more flexible PKI models that can effectively address these difficulties while upholding high standards of security and trust[9].

This study aims to fill this void by doing a thorough and systematic review of the existing literature and analysing the difficulties related to PKI interoperability among various trust models. The purpose of this analysis is to identify important problems and suggest possible solutions that can improve the ability of PKI systems to work together, ensure security, and handle increasing demands.

In this study, an in-depth study has been conducted on PKI interoperability. The contributions obtained from the research are listed as follows:

- Comprehensive Review and Synthesis: A systematic review of PKI trust models has been conducted, identifying key challenges, gaps, and future research directions in PKI interoperability.
- Practical Applications for E-Government and E-Commerce: The research offers best practices for implementing secure and scalable PKI systems in e-commerce and e-government applications.

According to the related papers that were reviewed, the relevance and necessity of this systematic review on PKI interoperability are substantiated by numerous critical studies. As in [10] the authors provide a comprehensive examination of hierarchical, mesh, bridge CA, hybrid, and trust list models, highlighting significant problems like scalability, certificate path validation, and cross-certification management. Similarly, The paper [11] examines different models, including subordinated hierarchy, cross-certified mesh, and bridge CA models, highlighting concerns regarding path construction, certification path validity, and scalability in extensive environments.

The reviewed studies justify the need for this comprehensive literature review by emphasizing the ongoing issues in PKI trust models, including operational complexity, scalability, and security vulnerabilities. Even though different models have been suggested, there are still some things that need to be done to create consistent compatible solutions that can be used successfully in many fields, such as e-government and e-commerce.

This article is organized in the following way. This systematic literature review (SLR) used PRISMA method, which is explained in Section II. In Section III, the results of the study on the current problems and challenges with the PKI compatibility trust model are given. Part IV shows the improvement needed. Finally, section V conclude the research work that was done for this study.

II. RESEARCH METHODOLOGY

This SLR study on the challenges related to the interoperability of Public Key infrastructure (PKI) across different trust models. In order to do this, the PRISMA was used as the systematic review method to identify relevant studies. Following the PRISMA guidelines for systematic reviews and meta-analyses was important for this review. These guidelines provide a structured way to find, choose, and evaluate relevant papers [12][13][14][15]. The review process in this study consists of four essential steps: identification, screening, eligibility, and inclusion, as depicted in Figure 1.

A. Search Strategy

The identification stage compiles a comprehensive and inclusive collection of relevant studies, multiple academic databases were employed. These databases were chosen based on their relevance to computer science, information security, and network engineering. The main databases used are IEEE Xplore, ACM Digital Library, Scopus, Web of Science, Google Scholar, SpringerLink and ScienceDirect databases as shown in Figure 2. A broad search approach was implemented, including a keywords-based strategy. “PKI” AND “interoperability” AND “Trust models" were all part of the search term.

Initially, 1,365 articles published between 2000 and 2024 were retrieved from academic databases. Since E-commerce and digital security saw major advancements throughout this time, it was decided to concentrate on research that was published between 2000 and 2024. The early 2000s saw the widespread use of e-commerce platforms, leading to the need for robust security infrastructures like PKI to ensure the authenticity and confidentiality of web-based interactions. The rise of e-commerce giants like Amazon, eBay, and Alibaba further expanded their global reach. The popularity of e-government systems also highlighted the need for scalable and interoperable PKI solutions for secure cross-domain communications. 2000-2024 was chosen as a significant year for PKI interoperability improvements in digital ecosystems[16].

Following the identification of relevant papers, a screening method was employed to eliminate publications that did not directly address PKI trust models or interoperability challenges, as well as duplicate papers. Initially, the titles and abstracts of the retrieved publications were screened based on predefined inclusion and exclusion selection criteria listed in Table I. The inclusion requirements necessitated peer-reviewed journal publications, conference papers, or technical reports published in English that addressed PKI interoperability, trust models, and related issues. A total of 440 articles were filtered during the screening process.

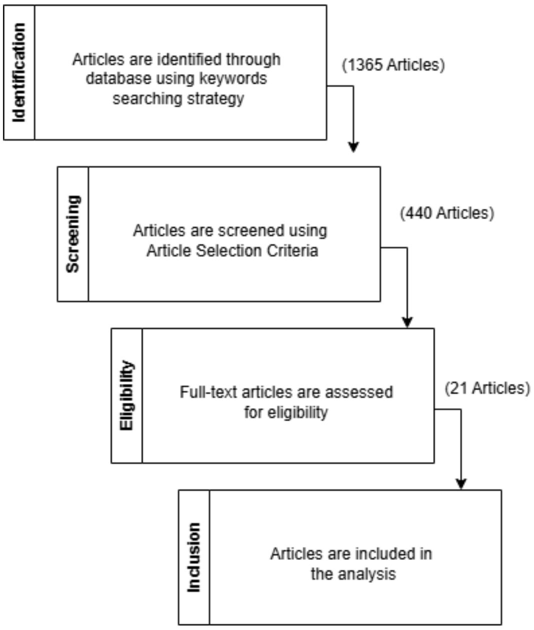
Identification
Articles are identified through database using keywords searching strategy
(1365 Articles)
Screening
Articles are screened using Article Selection Criteria
(440 Articles)
Eligibility
Full-text articles are assessed for eligibility
(21 Articles)
Inclusion
Articles are included in the analysis

Figure 1. Flowchart of research process

After the screening stage, the eligibility assessment ensured that the selected studies adhered to the criteria for relevance and quality. The focus was on studies that directly addressed PKI interoperability, particularly in relation to different trust models. Studies that primarily discussed cryptographic algorithms or unrelated security mechanisms were excluded, as they did not contribute to the understanding of PKI trust models. After applying these eligibility criteria, a total of 21 articles from the initial 440 publications were selected for the final review, providing comprehensive insights into the challenges and solutions related to PKI interoperability and trust models.

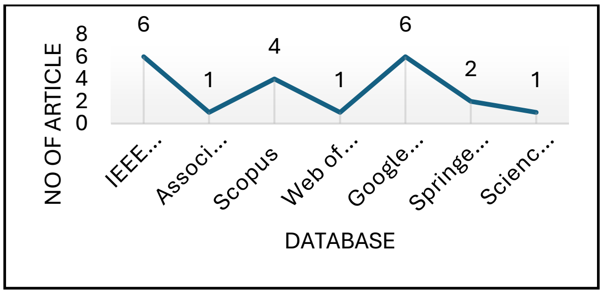

Figure 2. Resources database

TABLE I. INCLUSION AND EXCLUSION CRITERIA

Criteria	Inclusion	Exclusion
Language	Articles published in English to ensure accessibility and understanding.	Articles published in languages other than English.
Types of articles	Peer-reviewed journal articles, conference proceedings, or technical reports.	Non-peer-reviewed publications, reports, or grey literature. (e.g., PowerPoint slides, thesis, and patent).
Domain	Focuses specifically on PKI interoperability challenges or comparisons of trust models.	Outside the scope of PKI or does not focus on interoperability challenges or trust models.
Relevance to Tech Field	Study is related to technology, particularly cryptography, PKI systems, and network security.	The study is unrelated to technology and focuses on other fields (e.g., law, biology, or social sciences).

The inclusion process concluded by gathering all the assessed articles to be included in the final analysis of PKI interoperability challenges. The articles that met the quality criteria were included in the final review and analysis. A narrative synthesis approach was employed, focusing on thematic analysis to identify common challenges and solutions across the various PKI trust models. This synthesis involved a detailed examination and comparison of the findings from the included studies to develop a comprehensive understanding of the obstacles and opportunities related to PKI interoperability.

B. Research questions

The following questions were established for this SLR to comprehend the issue of PKI interoperability and its challenges, as well as to emphasise the various criteria associated with this issue:

- RQ1: What are the primary challenges associated with the interoperability of different PKI trust models?

  This question seeks to identify and categorise the major obstacles that hinder effective interoperability among various PKI trust models.
- RQ1.1: What are the gaps in the current literature on PKI and which areas require further research?

  This sub-question identifies the gaps in the existing research and highlights areas where further investigation is needed
- RQ2: How can PKI systems be implemented in a secure and scalable manner for large-scale applications, such as e-government and e-commerce?

  This question delves into the identification of future research areas, emphasizing the need to further explore and address unresolved issues in PKI trust models for enhanced interoperability.

III. RESULT AND DISCUSSION

This study examined 21 articles on PKI interoperability and trust models. The comprehensive analysis of different trust models showcases the thoroughness of the study which answered RQ1 and RQ2 above. The study shows that different

PKI trust models, such as cross/mesh certification, bridge CA, hierarchical, hybrid, cross-recognition, and certificate trust lists, present numerous challenges, including security risks and scalability issues, which have not been fully explored in technical literature.

A. Trust Models in PKI Systems: Benefits and Challenges (RQ1)

Table II presents a comparison of multiple trust models in PKI interoperability models, showing a range of advantages and disadvantages to answer RQ1. The Mesh/Cross Trust Model combines elements of cross-signing and distributed models to form a decentralized trust framework that enables several Certificate Authorities (CAs) to establish direct trust relationships across domains. This concept is especially effective in systems where central control is not possible, such as blockchain infrastructures and multi-domain PKIs.

The paper [17] highlights challenges in implementing a mesh trust model for PKI. These include computational complexity, scalability, security concerns, and the need for further optimization of certificate path processing. The paper also suggests integrating Trusted Computing technologies to mitigate vulnerabilities in traditional PKI systems. [18] highlight the challenges of creating a Cross-Platform PKI Model, where ensuring interoperability across various systems is complex due to differences in platform architectures and certificate management requirements.

[19] investigate the benefits and risks of cross-signing in PKIs. They point out that, although cross-signing improves interoperability by enabling certificates from various CAs to be accepted across domains, it also poses substantial security risks. Balancing interoperability with strong security measures is crucial, since a breach in one CA may affect the whole trust network. Then, [20] investigate cross-certification in a distributed setting, namely inside Hyperledger Fabric, a blockchain platform. Their results show that cross-signing may be successfully used in distributed systems, improving authentication across decentralized nodes. However, as the network grows, administering cross-signed certificates becomes more complicated, necessitating the use of advanced management tools. Similarly, [21] offers a Validation Authority (VA) as a means of managing and verifying cross-signed certificates. The VA serves as a central hub for ensuring that certificates from various CAs are trusted across numerous domains. This technique tackles interoperability difficulties by coordinating rules across multiple PKI infrastructures, resulting in a managed but decentralized trust system. Also, [5] proposes centralising digital certificate validation with a VA, simplifying interoperability and reducing complexity. This model improves security, reduces client-side burdens, and unifies digital certificate validation. This approach contrasts with traditional trust models like the Strict Hierarchy, which is rigid but secure, or the Cross Certification model, which increases complexity and scalability challenges due to the peer relationships between CAs. The Bridge CA model attempts to centralize trust but places heavy operational burdens on the bridge CA, while Certificate Trust Lists (CTLs) simplify trust management but are less scalable in larger networks [5].

In a larger regional perspective, [22] highlight the importance of cross-recognition and dispersed trust connections in Asia's PKI interoperability initiatives. It suggests policy alignment and distributed trust mechanisms to ensure smooth PKI operations across various domains and jurisdictions. The research highlights the administrative and coordinating tasks required in distributed trust frameworks, particularly for cross-border interoperability. Korean perspectives on global PKI interoperability highlight the challenges of building confidence across borders due to different legislative, legal, and technological frameworks. Cross Certification and Cross Recognition models face scalability issues, trust management issues, and challenges in maintaining consistent trust policies across domains. These limitations underscore the operational complexity of PKI interoperability and the need for a more comprehensive approach to security.

The Hierarchical Trust Model establishes trust from the top down, with a Root Certificate Authority (RCA) at the top of the hierarchy and trusted by all lower-level CAs. This model is commonly used, yet it may be firm and less adaptable in multi-domain settings. Traditional models, in the publication [23] allude to the hierarchical PKI model in which a RCA is the core trust anchor. Although safe, this architecture has major difficulties with regard to scalability, trust management complexity, and centralized responsibility on the Root CA. The study addresses these problems by means of the hybrid paradigm, which combines Identity-Based Cryptography (IBC) with conventional hierarchical PKI. While keeping the hierarchical trust chain for external contacts, the hybrid approach simplifies certificate administration and increases scalability by lowering the dependency on certificates for internal communication. Hybrid PKI Models, identifying the challenge of balancing flexibility with security. While hybrid models provide resilience and scalability, they introduce operational complexity in managing trust chains and ensuring policy consistency across domains. Meanwhile, [24] investigate the hybridization of hierarchical models, focusing on hybrid designs in which a central authority retains control over trust connections. While hierarchical architectures provide great security, they may create bottlenecks in big, dynamic systems.

[25] presents RCA is responsible for certifying lower-tier authorities like Authorisation Authorities (AAs) and Enrolment Authorities (EAs), managing their certificates' lifecycle, including creation, renewal, expiration, and revocation. This can be complex, especially when cross-domain interoperability is involved. RCA certificates need to be exchanged and verified when national PKI systems need to work together, adding complexity. The cross-certification procedure adds complexity as each RCA must trust other RCAs and guarantee the authenticity of foreign PKI certificates. As the number of participating ITS stations and entities increases, scalability issues may arise in trust distribution and certificate verification.

[26] focus on the Bridge Certification Authority (BCA) model, where a single Bridge CA connects multiple PKI domains. The primary challenges here include single points of failure and centralized liability, as the entire network becomes vulnerable if the Bridge CA is compromised. Ensuring security and scalability in such interconnected environments remains a significant challenge. Similarly, [27] explore a modified Bridge CA model, focusing on establishing trust between multiple hierarchical systems. The challenge lies in balancing centralized control with inter-domain trust, as a breach in the bridge could affect the security of all connected domains.

[28] discusses two key trust models in PKI systems, hierarchical trust model and the bridge CA model. While this model is straightforward and widely used, it presents scalability issues as the network grows, with the reliance on a single RCA potentially becoming a bottleneck and creating centralization risks, particularly in large or multi-domain environments. Then, bridge CA model enhances interoperability between PKI domains but requires careful management to maintain efficiency, as managing trust relationships across multiple CAs becomes complex. Similarly, [29] and [30] also mentions that traditional centralized trust models such as hierarchical models or bridge model with a single Root CA are not sufficient for large-scale inter-domain networks. As the number of domains and CAs increases, managing trust relationships becomes more complex. This is particularly problematic in scenarios where cross-certification is necessary. PKI-based trust model described in this paper is designed to enhance scalability, interoperability, and flexibility in managing inter-domain trust relationships. It moves away from traditional hierarchical structures and toward a trust delegation model that better suits large, dynamic, and multi-domain PKI environments.

[31] presenting all trust models commonly used in PKI, highlighting their advantages and challenges. The Subordinated Hierarchical Model offers strong security with a root CA certifying subordinate CAs, simplifying trust paths and reducing the need for frequent root CA usage. However, the model faces challenges in managing the sensitive root CA keys, especially in large networks. The Mesh Model allows flexible trust relationships between CAs, which works well in smaller networks. However, as the network grows, it becomes increasingly complex and expensive to manage. The Bridge CA Model connects multiple CAs through a central bridge CA, combining the simplicity of hierarchical models with the flexibility of mesh models. Despite its advantages, it involves high operational costs and poses significant risks due to the sensitivity of the bridge CA's signing keys. For environments where cross-domain trust is needed, the Cross Recognition Model helps reduce technical interoperability challenges but requires more administrative work and is not ideal for high-trust environments. The Certificate Trust List (CTL) simplifies trust management by allowing vendors to decide which CAs to trust, but this leaves users without control and with potential legal risks. [31] suggest that the Loose Hierarchical Trust Model with crossover between sub-CAs is an effective solution for improving scalability, reducing traffic at the root CA, and enhancing the performance of Sudan’s national PKI. However, ongoing challenges include managing trust relationships during organizational changes and ensuring that the system remains secure and scalable over time.

Hybrid Trust Model combines aspects of different models to adapt to changing needs, but it increases complexity, making it harder to manage. Each of these models presents a unique balance of security, scalability, and complexity, depending on the specific requirements of the PKI environment. [24] and [32]both address challenges within Hybrid Trust Models, where trust management involves both hierarchical and non-hierarchical components.[24] note the complexity of maintaining trust relationships in such hybrid architectures, while [16] discuss the difficulties of interoperation between conventional PKI and ID-based infrastructures.[32] concludes that while traditional PKI typically refers to the Certificate-Based Trust Model or the Hierarchical Trust Model faces scalability and management issues, hybrid models offer promising solutions by leveraging the strengths of both PKI and ID-PKC systems. However, there remain challenges, particularly regarding system complexity, communication overhead, and ensuring secure key issuance. The authors call for future research to improve hybrid PKI models, reducing these overheads while maintaining robust security features.

[33] address PKI interoperability in Serbia, highlighting the difficulties in cross-recognition between different PKI systems. Maintaining consistent security policies and ensuring certificate validation across domains that operate under different standards poses significant challenges. [34] focus on CA models, particularly the challenges related to scalability and security management in web applications. As PKI systems scale, the management of certificates across domains becomes more complex and creating a single point of control and trust management like hierarchical model. Necessitating improvements in CA architectures. [35] discuss Inter-Domain Trust Models like cross-certification, bridge CA and hierarchical model, where the scalability of PKI systems introduces challenges in maintaining consistent security policies and certificate validation across multiple domains.

Lastly, [36] explore CA-CA interoperability, where different CAs form direct trust relationships without relying on a central authority. Challenges include policy conflicts, certificate validation, and revocation management, which become increasingly complex in environments where multiple CAs. This study discusses trusted CA certificate management, where mismanagement of certificates such as improper issuance or failure to revoke compromised certificates creates significant security risks. Managing certificates across multiple CAs adds to the difficulty of maintaining trust in large, distributed PKI environments such as Cross-Certification, Bridge CA, Cross-Recognition, hierarchical model and Certificate Trust Lists.

B. Secure and Scalable PKI Strategies for Large-Scale Applications (RQ2)

To address RQ2, this section identifies and describes key strategies for deploying secure and scalable PKI systems in large-scale applications such as E-government and E-commerce. Firstly, adopting collaborative trust models such as organisations, institutions, or domains to facilitate a shared trust model among multiple users while ensuring that each organisation maintains control over its own operations and security protocols. This supports scalability and flexibility, especially when managing trust relationships across different organizations or countries. For larger dynamic systems, decentralised PKI systems offer a scalable alternative to global E-commerce platforms by distributing trust and reducing reliance on centralised authorities. To achieve smooth interoperability, it's essential to maintain consistent trust policies and governance standards across all organisations, harmonizing certificate policies and validation procedures. Furthermore, implementing strong cryptographic standards and planning for the transition to post-quantum cryptography ensures long-term security and resilience. Finally, conducting ongoing security audits and ensuring compliance with regulatory frameworks help in the maintenance of trustworthiness and security across a variety of PKI systems.

By incorporating these best practices, E-government and E-commerce platforms can ensure secure, scalable, and efficient PKI interoperability across complex digital ecosystems. Future research should focus on developing these technologies in tandem with PKI to enhance infrastructure resilience and scalability in complex digital ecosystems.

TABLE II. PKI INTEROPERABILITY TRUST MODELS

Trust Model	Complexity	Security	Liability	Efficiency	Scalability Challenges
Cross/mesh Certification	High, due to cross-signing and certificate path processing. [17][18][22] [31]	Security risks increase with CA breaches across domains. [19][35]	Distributed, but breaches in one CA can affect the whole network. [19][20]	Moderate to efficient for smaller networks. [20]	Becomes complex as the network and cross-signing relationships grow. [17][20][22][25] [26][29][30][35] [36]
Bridge CA	Moderate to High, central trust authority adds operational complexity. [21]	Single point of failure creates centralized vulnerability. [21][31][35]	Bridge CA holds significant liability, making it vulnerable to compromise. [21]	Simplifies cross-domain interactions and trust management. [23]	Managing trust relationships between multiple domains can be challenging. [24][26][29][30] [35] [36]
Hierarchical	Low, as it is a centralized trust model with a Root CA. [19][23][34]	Strong security through a single Root CA. [19][31][35]	Root CA bears all liability for lower-level CAs. [19]	High efficiency in smaller, controlled networks. [19]	Centralization creates bottlenecks and scalability issues in multi-domain environments. [20][23][25] [31][35] [36]
Hybrid	High, due to mixing hierarchical and distributed components, [20][24][27] [32]	Offers flexibility and improved resilience, but security risks increase with multiple trust models. [20][27][31]	Shared liability between hierarchical and non-hierarchical CAs. [20][32]	Efficient, combining benefits of hierarchical and distributed models. [27]	Increased operational complexity as systems grow in size and scale. [20][23][26][24]
Cross Recognition Model	Need more administrative and management work. [18][22][31]	Balances interoperability with security, but domain breaches can spread across trust relationships. [18][24][33]	Liability is shared between CAs, but coordination is required. [18][33]	Efficient for interoperability across domains. [18][24]	High administrative effort, particularly across jurisdictions. [18][22][26][28] [36]
Certificate Trust Lists	Low, simplifies trust management through predefined CA lists. [5]	Security depends on the correct inclusion/exclusion of trusted CAs. [5][31]	Liability rests with the entities managing the trust lists. [31]	Highly efficient in smaller networks, but burdens clients with limited control. [26]	As the list grows, scalability becomes an issue; centralized control limits flexibility. [5][26][31][36]

B. Secure and Scalable PKI Strategies for Large-Scale Applications (RQ2)

To address RQ2, this section identifies and describes key strategies for deploying secure and scalable PKI systems in large-scale applications such as E-government and E-commerce. Firstly, adopting collaborative trust models such as organisations, institutions, or domains to facilitate a shared trust model among multiple users while ensuring that each organisation maintains control over its own operations and security protocols. This supports scalability and flexibility, especially when managing trust relationships across different organizations or countries. For larger dynamic systems, decentralised PKI systems offer a scalable alternative to global E-commerce platforms by distributing trust and reducing reliance on centralised authorities. To achieve smooth interoperability, it's essential to maintain consistent trust policies and governance standards across all organisations, harmonizing certificate policies and validation procedures. Furthermore, implementing strong cryptographic standards and planning for the transition to post-quantum cryptography ensures long-term security and resilience. Finally, conducting ongoing security audits and ensuring compliance with regulatory frameworks help in the maintenance of trustworthiness and security across a variety of PKI systems.

By incorporating these best practices, E-government and E-commerce platforms can ensure secure, scalable, and efficient PKI interoperability across complex digital ecosystems. Future research should focus on developing these technologies in tandem with PKI to enhance infrastructure resilience and scalability in complex digital ecosystems.

In implementing PKI interoperability, several key aspects must be considered to ensure success in E-commerce and E-government environments. Case studies of successful PKI interoperability implementations provide valuable insights. The eIDAS Regulation in the European Union aims to create a legal framework for electronic identification and trust services, promoting secure cross-border digital interactions and reducing digital transaction barriers, particularly in healthcare and public procurement sectors[37]. On the other hand, the Federal PKI Infrastructure (FPKI) in the United States is another example of a large-scale implementation of PKI interoperability. The FPKI facilitates secure electronic communications between federal agencies by ensuring the confidentiality, integrity, and authenticity of digital transactions. The system allows federal, state, and local governments to cross-certify, ensuring that certificates from different entities can be trusted. This framework has significantly improved the security and trustworthiness of digital communications within the US government[38].

Finally, successful implementation of PKI solutions necessitates effective user and organisational strategies. Engaging stakeholders early in the process results in a smoother implementation because all relevant parties understand the benefits and challenges of PKI. Training and awareness programs on PKI usage and certificate management help to increase adoption rates, while simplifying the integration of PKI systems into existing infrastructures can help organisations transition to interoperable PKI solutions. Incentives for adoption, such as improved security, regulatory compliance, and operational efficiency, can encourage organisations to implement PKI interoperability solutions.

IV. RECOMMENDATION

To address scalability issues, integrating PKI systems with cloud-based infrastructures offers a dynamic and efficient solution. Cloud-based PKI solutions are designed to handle large volumes of certificates, making them ideal for environments requiring quick and secure scaling. These systems enable automated certificate lifecycle management, such as issuance, renewal, and revocation, reducing administrative burden and lowering the risk of manual errors. Organisation can use cloud infrastructure to dynamically allocate resources as needed, ensuring that the PKI system remains robust even during times of high demand. Furthermore, cloud-based solutions provide global access, which is especially useful for systems that must accommodate users or entities from various locations. Importantly, cloud-based PKI solutions maintain high security standards by following industry best practices for encryption, access control, and regulatory compliance. This ensures that the system remains secure, reliable, and efficient as it grows in size.

This feature lets businesses easily change their resources based on demand without having to make big changes to their infrastructure. This gives businesses the freedom to handle changing workloads while keeping up performance and efficiency. With the added flexibility of crypto agility, the system can seamlessly adjust to different cryptographic protocols and algorithms, enhancing its adaptability. The versatility of the crypto agility further supports scalability, allowing it to expand with growing user without increasing complexity. By incorporating dynamic keys, the proposed research streamlines and enhances the efficiency and manageability of key management systems in large and dynamic environments, ensuring security, reliability, and scalability as the system evolves. In a word, merging PKI systems with cloud services provides both scalability and enhanced security, allowing organisations to manage certificates more effectively while ensuring that their systems are ready to handle increasing demand.

V. CONCLUSION

Across various PKI trust models, each has distinct strengths and challenges. Cross/Mesh Certification models offer flexibility in establishing trust between multiple CAs but suffer from operational complexity and security risks as the network scales. Bridge CA models are simpler to manage but face single points of failure and scalability issues due to their centralized nature. Hierarchical models provide strong security through a Root CA, but scaling across layers increases complexity. Hybrid models balance flexibility and security, though the management of trust lists becomes harder as the system grows. Cross-Recognition Models ease interoperability between domains but require significant administrative effort and are less suited for high-security environments. Finally, Certificate Trust Lists (CTLs) improve reliability by decentralizing trust but become harder to scale as the list grows, with centralized control limiting their efficiency. Each model offers trade-offs between scalability, complexity, and security, highlighting that no single model solves all PKI challenges.

However, a combination of models can help balance security and scalability. For large-scale applications, Hybrid models emerge as a strong option, combining the security benefits of hierarchical models with the flexibility and scalability of cross-certification and mesh models. These hybrid approaches allow for efficient trust management across diverse domains while mitigating single points of failure and ensuring resilience through loop-free trust chains. For secure and scalable PKI implementations in large-scale applications like e-government and e-commerce, it's crucial to adopt models that distribute trust and liability, optimize certificate issuance and revocation, and implement automation to handle increasing complexity and scale. Ultimately, a well-structured combination of PKI models that emphasizes security, decentralization, and scalability will facilitate the secure and efficient implementation of large-scale systems.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this paper.

ACKNOWLEDGEMENT

This research was funded by the Ministry of Higher Education (MOHE) of Malaysia under the Fundamental Research Grants Scheme (FRGS/1/2024/ICT07/USIM/02/1).

REFERENCES

[1] Zhang, Chengyuan, Changqing An, Tao Yu, Zhiyan Zheng, and Jilong Wang. "Investigate and Improve the Certificate Revocation in Web PKI." In NOMS 2024-2024 IEEE Network Operations and Management Symposium, pp. 1-5. IEEE, 2024. doi: 10.1109/NOMS59830.2024.10575605.

[2] Xiong, Qin, Yujian Zhang, Junhao Li, and Fei Tong. "Enhancing Security of Certificate Authorities by Blockchain-based Domain

Transparency." In 2022 IEEE 28th International Conference on Parallel and Distributed Systems (ICPADS), pp. 304-311. IEEE, 2023. doi: 10.1109/ICPADS56603.2022.00047.

[3] Margariti, Vicky, Dimosthenis Anagnostopoulos, Anastasia Papastilianou, Teta Stamati, and Sofia Angeli. "Assessment of organizational interoperability in e-Government: A new model and tool for assessing organizational interoperability maturity of a public service in practice." In Proceedings of the 13th international conference on theory and practice of electronic governance, pp. 298-308. 2020. doi: 10.1145/3428502.3428544.

[4] Jain, Alok, Sarthak Gupta, Mangalesh Vyas, Diptikant Pathy, Gitika Khare, Alpana Rajan, and Anil Rawat. "Open source EJBCA public key infrastructure for e-governance enabled software systems in RRCAT." In ICT Based Innovations: Proceedings of CSI 2015, pp. 127-139. Springer Singapore, 2018. doi: 10.1007/978-981-10-6602-3.

[5] Ma, Yong Li. "Study on the Solution of PKI Interoperation." Advanced Materials Research 271 (2011): 1136-1141. doi: 10.4028/www.scientific.net/AMR.271-273.1136.

[6] Kong, Ini, Marijn Janssen, and Nitesh Bharosa. "Challenges in the Transition towards a Quantum-safe Government." In DG. O 2022: The 23rd Annual International Conference on Digital Government Research, pp. 282-292. 2022. doi: 10.1145/3543434.3543644.

[7] Panigrahi, Amrutanshu, Ajit Kumar Nayak, and Rourab Paul. "Smart contract assisted blockchain based public key infrastructure system." Transactions on Emerging Telecommunications Technologies 34, no. 1 (2023): e4655. doi: 10.1002/ett.4655.

[8] Obiri, Isaac Amankona, Jingcong Yang, Qi Xia, and Jianbin Gao. "A sovereign PKI for IoT devices based on the blockchain technology." In 2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), pp. 110-115. IEEE, 2021. doi: 10.1109/ICCWAMTIP53232.2021.9674095.

[9] Dulia, Oleksandr, and Dmytro Minochkin. "An exploration of public key infrastructure applications across diverse domains: a comparative analysis." (2023). doi: 10.20535/2411-1031.2023.11.2.293496.

[10] El Uahhabi, Zakia, and Hanan El Bakkali. "A comparative study of PKI trust models." In 2014 International Conference on Next Generation Networks and Services (NGNS), pp. 255-261. IEEE, 2014. doi: 10.1109/NGNS.2014.6990261.

[11] Linn, J. "Trust Models and Management in PKI." RSA Security Laboratories (2000). Available: http://storage.jak-stik.ac.id/rsasecurity/PKIPaper.pdf

[12] Moher, David, Alessandro Liberati, Jennifer Tetzlaff, Douglas G. Altman, and Prisma Group. "Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement." International journal of surgery 8, no. 5 (2010): 336-341. doi: 10.1016/j.ijsu.2010.02.007.

[13] Zakaria, Abdul Alif, A. H. Azni, Farida Ridzuan, Nur Hafiza Zakaria, and Maslina Daud. "Systematic literature review: trend analysis on the design of lightweight block cipher." Journal of King Saud University-Computer and Information Sciences 35, no. 5 (2023): 101550. doi: 10.1016/j.jksuci.2023.04.003.

[14] Ellaky, Zineb, Faouzia Benabbou, and Sara Ouahabi. "Systematic literature review of social media bots detection systems." Journal of King Saud University-Computer and Information Sciences 35, no. 5 (2023): 101551. doi: 10.1016/j.jksuci.2023.04.004.

[15] Oudah, Mohammed AM, and Mohd Fadzli Marhusin. "SQL Injection Detection using Machine Learning: A Review." Malaysian Journal of Science Health & Technology 10, no. 1 (2024): 39-49. doi: 10.33102/mjosht.v10i1.368.

[16] Havinga, Marieke, Martijn Hoving, and Virgil Swagemakers. "Alibaba: a case study on building an international imperium on information and E-Commerce." Multinational Management: A Casebook on Asia’s Global Market Leaders (2016): 13-32.

[17] Liu, Changping, Yong Feng, Mingyu Fan, and Guangwei Wang. "PKI mesh trust model based on trusted computing." In 2008 The 9th International Conference for Young Computer Scientists, pp. 1401-1405. IEEE, 2008. doi: 10.1109/ICYCS.2008.384.

[18] Chung, Yu Fang, and Hui Fang Chen. "Cross platform layer for public key infrastructure interoperability." International Journal of Innovative Computing, Information and Control 5, no. 6 (2009): 1699-1710.

[19] Hiller, Jens, Johanna Amann, and Oliver Hohlfeld. "The boon and bane of cross-signing: Shedding light on a common practice in public key infrastructures." In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, pp. 1289-1306. 2020. doi: 10.1145/3372297.3423345.

[20] Kakei, Shohei, Yoshiaki Shiraishi, Masami Mohri, Toru Nakamura, Masayuki Hashimoto, and Shoichi Saito. "Cross-certification towards distributed authentication infrastructure: A case of hyperledger fabric." IEEE Access 8 (2020): 135742-135757. doi: 10.1109/ACCESS.2020.3011137.

[21] Ma, Yongli. "Research on the solution of PKI interoperability based on validation authority." In 2011 International Conference on Computer Science and Service System (CSSS), pp. 697-700. IEEE, 2011. doi: 10.1109/CSSS.2011.5974568

[22] Paulus, Sachar, Norbert Pohlmann, Helmut Reimer, InKyung Jeun, Jaeil Lee, and SangHwan Park. "Asia PKI Interoperability Guideline." In ISSE 2004—Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2004 Conference, pp. 309-320. Vieweg+ Teubner Verlag, 2004. doi: 10.1007/978-3-322-84984-7_31.

[23] Chia, Jason, Swee-Huay Heng, Ji-Jian Chin, Syh-Yuan Tan, and Wei-Chuen Yau. "An Implementation Suite for a Hybrid Public Key Infrastructure." Symmetry 13, no. 8 (2021): 1535. doi: 10.3390/sym13081535.

[24] Satizábal, Cristina, Rafael Páez, and Jordi Forné. "Building a Virtual Hierarchy for Managing Trust Relationships in a Hybrid Architecture." J. Comput. 1, no. 7 (2006): 60-68. doi: 10.4304/jcp.1.7.60-68.

[25] Msahli, Mounira, Houda Labiod, and Gilles Ampt. "Security interoperability for cooperative its: Architecture and validation." In 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), pp. 1-6. IEEE, 2019. doi: 10.1109/NTMS.2019.8763819.

[26] Polk, William T., and Nelson E. Hastings. "Bridge certification authorities: Connecting b2b public key infrastructures." In PKI Forum Meeting Proceedings, pp. 27-79. 2000.

[27] Li, Mingchu, Yizhi Ren, Zhihui Wang, Jun Xie, and Hongyan Yao. "A new modified bridge certification authority PKI trust model." In 2006 First International Symposium on Pervasive Computing and Applications, pp. 23-26. IEEE, 2006. doi: 10.1109/SPCA.2006.297465.

[28] Slagell, Adam, Rafael Bonilla, and William Yurcik. "A survey of PKI components and scalability issues." In 2006 IEEE International Performance Computing and Communications Conference, pp. 10-pp. IEEE, 2006. doi: 10.1109/.2006.1629442.

[29] Tanwar, Sarvesh, and Anil Kumar. "Extended Design and Implementation of Certificate Authorities." International Journal of Security and its Applications 11, no. 8 (2017): 13-26. doi: 10.14257/ijsia.2017.11.8.02.

[30] Satizabal, Cristina, Rafael Paez, and Jordi Forne. "PKI trust relationships: from a hybrid architecture to a hierarchical model." In First International Conference on Availability, Reliability and Security (ARES'06), pp. 8-pp. IEEE, 2006. doi: 10.1109/ARES.2006.93.

[31] Nawari, Mustafa, and Asma Abdalrahman. "Crossover under the root of a certification authority." In 2013 International Conference On Computing, Electrical And Electronic Engineering (ICCEEE), pp. 182-185. IEEE, 2013. doi: 10.1109/ICCEEE.2013.6633929.

[32] Singh, Priyadarshi, Abdul Basit, N. Chaitanya Kumar, and V. Ch Venkaiah. "Towards a hybrid Public Key Infrastructure (PKI): a review." Cryptology ePrint Archive (2019).

[33] Prodanović, Radomir I., and Ivan B. Vulić. "Model za PKI interoperabilnost u Republici Srbiji." Vojnotehnički Glasnik/Military Technical Courier 65, no. 2 (2017): 530-549. doi: 10.5937/vojtehg65-11041.

[34] Al-Janabi, Sufyan Faraj, and Amer Kais Obaid. "Development of certificate authority services for web applications." In 2012 International Conference on Future Communication Networks, pp. 135-140. IEEE, 2012. doi: 10.1109/ICFCN.2012.6206857.

[35] Millán, Gabriel López, Manuel Gil Pérez, Gregorio Martínez Pérez, and Antonio F. Gómez Skarmeta. "PKI-based trust management in inter-domain scenarios." Computers & Security 29, no. 2 (2010): 278-290. doi: 10.1016/j.cose.2009.08.004.

[36] Steve, L., D. Fillingham, R. Lampard, and S. Orlowski. "CA-CA Interoperability." In PKI Forum, March. 2001.

[37] Cuijpers, Colette, and Jessica Schroers. "eIDAS as guideline for the development of a pan European eID framework in FutureID." (2014).

[38] D. W. Wood and D. W. Wood, “United States Department Of The Treasury,” 2021.