

Federated public key infrastructure management for secure internet of things interoperability

Omar Ahmed Abdulkader, Muhammad Jawad Ikram

Faculty of Computer Studies, Arab Open University, Riyadh, Saudi Arabia

Article Info

Article history:

Received Jan 8, 2024

Revised Aug 18, 2024

Accepted Sep 3, 2024

Keywords:

Federated learning

Internet of things

Interoperability

Public key infrastructure

Security

ABSTRACT

Proliferating the internet of things (IoT) across all industry fields offers numerous possibilities for invention. It also multiplied the issues of ensuring uniform interoperability among a wide range of devices and platforms. The focus of this paper is to propose an approach for enhancing the security of IoT networks. This study investigated the possible efficacy of employing a federal public key infrastructure (PKI) structure system to serve IoT-based ecosystems. To achieve this goal, we have developed an elaborate experimental framework incorporating different trust models, security protocols, privacy enhancements, and performance metrics that demonstrate the practical benefits of this kind of federated system. One of the contributions of this study is an experimental model that mimics a real IoT ecosystem. It entails many IoT devices, installing vital PKI elements, and the development of safe information transmission channels. Measurements such as latency pointed out the feasibility of various IoT concepts, including such short response time as 2.8 ms for vehicular IoT (V2X). Measures for interoperability ranged with V2X having a 96.4% success, indicating the strength of the standards within that segment. This study reveals the benefits of a federated PKI management system for solving issues of IoT interconnectedness.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Omar Ahmed Abdulkader

Faculty of Computer Studies, Arab Open University

Riyadh, Saudi Arabia

Email: o.abdulkader@arabou.edu.sa

1. INTRODUCTION

Internet of things (IoT) is experiencing a great expansion, spreading to diverse fields like health care, production, logistics, and intelligent urbanism. However, this growth is heralding a new age of unprecedented communication and information sharing with smarter, more intelligent, more responsive, and more productive industries [1]. On the other hand, the huge communication system of various connected devices is challenged with many problems regarding safety, confidentiality, and compatibility [2], [3]. To ensure that the heterogeneous set of IoT devices and their widespread deployment will lead to strong security measures, one needs the proper mechanism for trust establishment. This indicates that perhaps public key infrastructure (PKI) could be the answer to curbing this issue and forming the basis of digital communication by introducing digital certificates as well crypto keys. Nevertheless, there are many hurdles associated with traditional PKI when employed in the IoT context. A traditional PKI system also suffers from inherent difficulties due to its centralized structure and heterogenous environment of an evolving IoT [4], [5]. Finally, a close scrutiny of the PKI practice will be necessary if interoperability between different devices, media and so forth is aimed at. New approach of federated management of PKI (FM-PKI) aims at combining the security advantages of PKI's while integrating rarely encountered attributes in IoT's networks. It provides a

distributed model where certificates are issued by individual certificate authorities (CAs), validated by CAs and revoked at designated CAs. This increases scaling capabilities, eliminates one points of failures, and strengthens PKI's reliability. In a new approach for securing IoT interoperation, this paper provides a detailed analysis of federated PKI management systems. The paper covers IoT networks, specifies special security and interoperability requirements for these networks, points potential gaps in standard PKI models. Finally, we present the architecture of federated PKI management, explaining its components, processes, and trust models, and show how the same is uniquely suitable for providing scalable, flexible, and secure solutions in IoT networks. This paper further seeks to emphasise the efficacy of federated PKI by providing more on what can be applied to achieve security and interoperability among IoT devices and platforms. We seek to participate in the intellectual and practical debate on IoT security, providing advice, solutions, and a strong model of federated PKI management that could be applied in any IoT environment. Therefore, this paper lays the foundation for further investigations on safety, interoperability, and robustness that underlie the emerging IoT future.

2. BACKGROUND

2.1. Internet of things

In recent studies, emphasis has been laid upon the internet of things (IoT), an intricate and evolving network of interconnected devices and systems that communicate seamlessly over the internet [6]. These entities range from commonplace household appliances to sophisticated industrial machinery, all embedded with computational capabilities. Their integration into the physical realm aims to enhance and automate facets of daily human activity. However, different kinds and types of hardware as well as functionality make this challenging even though they use lots of different networking techniques such as Wi-Fi Bluetooth, and mobile network [7]. The growth of the IoT landscape calls for a reliable system that can handle the increasing amount of generated and distributed information through multiple gadgets. This growth is usually accompanied by challenges, especially in security, interoperability, privacy, and due limitations that emanate from most IoT devices [8].

2.2. Public key infrastructure

The public key infrastructure is a system that handles, disseminates, and keeps digital keys and certificates. The core principle of PKI is based on asymmetrical cryptography with every participant having a set of public and private keys [9]. Digital certificates are much like ID cards that are tied up with the identity of a person or an entity, and their public key. The certificates issued by the CA form a core part of the PKI system [10]. The CA meticulously verifies the identity of the party requesting for the certificate before issuing it. At certain stages, the registration authority (RA) helps CA with identity verifications. Whereby, if the authenticity of a certificate is questioned and it becomes untrustworthy, then it is listed in the certificate revocation list signifying loss of validity. Chain of trust is one more important element of PKI – if you trust in certain CA then all certificates issued by this CA or with which CAs it trusts are considered as trusted ones. Such an architecture is crucial for the purposes of securing e-mail privacy and augmenting the power of virtual private networks (VPNs) [11]. To conclude, it should be noted that the crucial point in security assurance of IoT is the presence of an essential infrastructure called PKI, which represents a common platform for management of amazing number of elements of IoT. It can enable authentication of devices through issuing distinct digital certificates to every device. Such reliable participants alone will have safe data delivery [12]. It also ensures encrypted transfer of data to keep it safe and sound as well. The scalable trust architecture of PKI supports hundreds of thousands of devices in a single network and allows trusted interactions across several manufacturers [13]. The use of PKI is critical during the life cycle management process, which includes authorization to access, authentication, and cessation due to a breach of security [14].

2.3. Federated architecture

Federated PKI management for secure IoT interoperability represents an architectural technique that lets multiple, self-sustaining IoT systems or businesses collaborate using a shared PKI framework [15]. Instead of centralised PKI devices, the federated version guarantees that every entity retains its personal PKI but adheres to common protocols and requirements for seamless and stable interactions. This decentralisation ensures flexibility, scalability, and neighbourhood control while promoting steady records exchanges and tool authentication across IoT ecosystems [16]. By aligning trust frameworks and shared authentication standards, federated PKI helps a relied-on environment where devices from various networks can reliably and securely speak, ensuring robust IoT interoperability without centralising authority or management.

3. RELATED WORK

IoT devices are rapidly increasing due to the ever-developing digital world. Due to this mass production, the complexity of managing them all so they can improve quality and security is extremely difficult. However, Bai *et al.* [17] noted this challenge should be addressed because it implies a solution for automatically identifying both previous and new devices. Evidently, safe V2X communication moved to vehicular public key infrastructures for many years. These infrastructures serve a dual purpose: providing efficient certificate handling and authorisation functions with a primary concern for personal data protection. A study by Giannetsos and Krontiris [18] highlighted some of these problems in present-day PKI-based frameworks. Currently, industries are undergoing digital changes, utilising ICT to bring out joint operations among all parties. At its intersection is building information modelling (BIM), where smart infrastructure can incorporate IoT blueprints, allowing easy flow of information through communications, data transfer, and user collaboration. However, Siountri *et al.* [19] went beyond this, exploring the convergence of BIM, IoT, blockchain, and advanced digital technologies to ensure high security. According to Rech *et al.* [20], federated service management represents a new revolutionary approach that seeks to enhance interoperability between various services provided in contexts such as Smart mobility or Smart cities. This strategy ensures secure authentication and authorisation processes regarding the vehicle owners, its operators, and supplementary information systems while maintaining user-defined privacy levels. The growth in network data due to IoT has left multi-party computation wanting. A study by Yin *et al.* [21] suggested adopting a federated deep-learning-based secure data collaboration framework (FDC) since the associated concerns with fragmentation, volume, and security pose delicate issues in IoT-based computations. A study by Swamy and Kota [22] discusses key system-level properties such as energy efficiency, robustness, and security, among others, that determine IoT success. The above perspective outlines core aspects of IoT and emerging IoT applications to guide researchers to innovatively implement feasible and reliable real-time IoT solutions. Modern industrial operations, modern healthcare sectors, and state-of-the-art blockchain security require robust industrial IoT systems in this century. A study by Sodhro *et al.* [23] and Abdulkader *et al.* [24] highlights the importance of developing innovative block chain-based cybersecurity frames in conjunction with smart random key generation processes that work efficiently in fast encrypting/distributing data across long-range networks. Therefore, with the rise of distributed environments, federated learning (FL) becomes an important solution for efficient ML, especially concerning IoT and mobile edge computing. Xu *et al.* [25] introduce blockchain-empowered secure and incentive federated learning (BESIFL) paradigm, for privacy protection in distributed environments.

4. PROPOSED MODEL

4.1. Overview

The rise in penetration of IoT devices in different industry verticals has underscored the importance of uninterrupted interoperability. Nevertheless, the variety of these devices creates a serious security issue. The problem of achieving interoperability and security is quite difficult if we consider such factors as various producers. Nevertheless, standard norms and communication protocols. This gap is sought to be bridged through the proposed scheme that proposes implementing a federated PKI approach. The basis of the model is in creating a single trust environment. It's important to find a way to verify credibility when handling various IoT-related communications within a vast ocean of such devices and networks. The model achieves this by federating or uniting various PKIs so that credentials issued in one credential ecosystem can be validated by a device from another. In this way, a single methodology helps eliminate the need for each entity to know about other entities' PKI details, reducing the complexities involved with trust verification in large-scale IoT systems. The goal is global interoperability, however, there is a unique need for differing IoT systems. For instance, a healthcare IoT system would require more stringent security mechanisms than a smart home system. Hence, the federate PKI model enables each IoT system to manage and maintain its own PKI. Such localised control enables every system to finetune its security parameters as it requires flexibility. PKI's advantage includes the perfect balance between the ability to work across global borders while still accepting local specifics. Firstly, it allows devices from various participating IoT systems to interact safely with each other. It does not impose one-size-fits-all models on independent components; each component maintains its autonomy to tailor decisions best suited for the context or needs. Threat profiles will continue to evolve with the changes brought by IoT. The adopters of a federated PKI system can make use of a dynamic and flexible framework. Because these individual IoT systems hold on to their own PKIs, it implies that they can quickly respond to any threat within the system itself. At the same time, this is achieved at a general level by the single trust framework, which prevents an upset in the overall interoperability of the ecosystem. Figure 1 depicts a general overview of federated PKI management for IoT's.

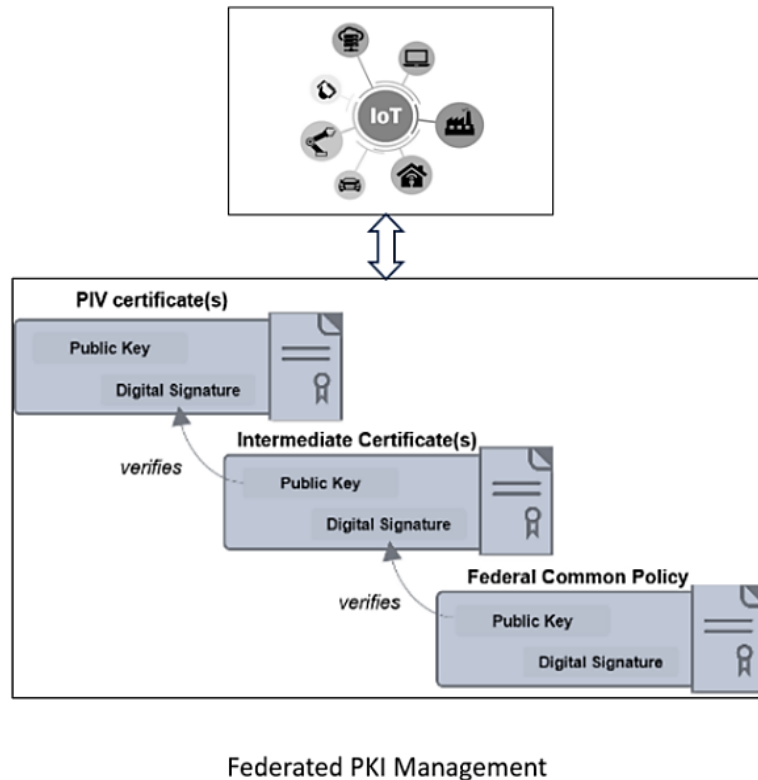


Figure 1. Overview of federated PKI management for IoT's

4.2. Key components of the federated PKI system for IoT interoperability

With the IoT edge technologies are the key are edge connecting endorsing the digital growth. Such technologies allow the internet of things to be run effectively because the most fundamental devices collaborative and communicating sensors–will be specifically customized to coordinate with a large number of transactions. This is what is fundamental as accuracy and sovereignty of these devices determines how much the IoT ecosystem will be able to succeed. Moreover, they deliver immediate feedback, which ensures low or does not use a lot of bandwidth (a resource needed as a source of networking efficiency). Edge technologies come now and make IoT devices the so essential tool in the story of the digital evolution because they now allow IoT devices to perform their functions better [26].

4.2.1. Sensors

Sensors are like “eyes and ears” in an IoT landscape. They are complex units for monitoring all important environmental conditions like humidity, temperature, and gases [27]. For instance, while your smart home may have a temperature sensor tracking the ambience to ensure that you are comfortable, specialized sensors could monitor equipment in an industrial setting, looking out for heat spots, any unusual vibration, or any impending danger signs. Sensors form the backbone of all data inputs and span across a broad spectrum from basic light identification in home garden lights all the way to complex chemical composition analysis in the factory setting.

4.2.2. Actuators

Sensors gather data while actuators act. They convert electronic signals into actual world actions. Just imagine how sophisticated it is when an irrigation system with soil-moisture sensors commands an actuator to open a valve that eventually replenishes a barren field. Actuators fulfil tasks from changing the mood in a room to controlling huge industrial plants; they unite the digital and material worlds together [28].

4.2.3. Gateways

A gateway is a middle point where data gathered from various sensors can be filtered, aggregated, or pre-processed before being forwarded to the central servers or clouds. But their role is not unilateral. Furthermore, they send responses or update from base station to the remote devices, allowing two-way traffic for communication. They are the “gatekeepers” that facilitate proper data traffic control [29].

4.3. Other IoT components

The IoT's universe is gigantic and varied. In addition to the standard sensors, actuators, and gateways, we boast a range of specialized devices fulfilling specific demands. The wearable health monitor that tracks vitals, the real-time security camera, and the smart refrigerator that suggests recipes based on its contents. The numerous devices specially designed for particular uses are contributing different dimensions to the IoT fabric [30].

4.4. Local PKI authorities

Internet of things, a web network of interconnected devices that must trust each other, requires utmost care when establishing and maintaining trust. This is a difficult question when considering the vastness of the sea that exists in the world of communication. The local PKI authorities act as guardians or sentinels of security for the respective IoT subsystems in the trust ecosystem [31]. This provides vital services such allowing secure device authentication, permitting encrypted communication, and providing digital certificates. By doing this, its guarantee that any device connected to the network can be independently validated, protecting the security and integrity of data sent over the IoTs.

4.4.1. Issuance of digital certificates

In this case, the digital certificate is an identity card for an IoT, also referred to as a unique stamp or stamp of approval. In much the same way as a passport authenticates a person's identity on international voyages, certificates for electronic signatures affirm the genuineness of devices in the IoT network. To become part of the IoT network, the PKI authority verifies the device and, upon approval, issues the certificate. It is not just an identity but a credential which guarantees that only authentic devices are involved in communication [32].

4.4.2. Management of cryptographic keys

Communication's protection in the electronic world is crypto keys. These are the means to ensure that no unwanted change occurs when any information moves from one device to another. The keys are taken on this important journey under the management of the PKI [33]. It begins the process of their creation and ensures that strong formulae are used in generating them. It monitors their distribution and ensures that only authorized devices obtain the correct keys. It stores them safely and keeps them away from unauthorized access, and then when the end of the lifecycle comes, whether through possible exposure or being terminated, the PKI monitors how safe their discontinuation or revocation will be.

4.4.3. Revocation services

One can hardly keep eyes closed in IoT world which is free from any danger. Devices can be compromised, certificates misused, or even expired. For example, the PKI will ensure that such machines lose their trusted nature during such a situation. The PKI continuously monitors the communication system and keeps an up-to-date certificate revocation list (CRL). Whenever a device that no longer meets the trust criteria is recognized, such a device is quickly removed from the list so as not to continue taking part in the future [34].

4.4.4. Local trust decisions

The world of IoT is so wide and dynamic. Security requirements and trust thresholds may vary among different entities. The ultimate objective is smooth and safe interaction among all devices. However, there is a need to honor and accommodate these divergent trust attitudes [35].

4.5. Federation gateway

The federation gateway enables interconnection between various distinct PKIs. Acting as a bridge, the gateway ensures that PKIs with different standards and protocols can securely exchange and validate credentials. The harmonizer is what makes it possible for varying PKIs with their own peculiarities and standards to interoperate peacefully [36]. By resolving differences between PKIs, the federation gateway promotes a unified, secure environment where diverse PKI systems can function cohesively.

4.5.1. Translates trust models

Trust is a kind of universal translator. Trust can also be spoken in different tongues by various PKIs, with their own trust models and certificate standards. The gateway makes sure that these languages of trust translate seamlessly into this world [37].

4.5.2. Facilitates key exchanges

Devices from two different systems that would like to communicate with each other. The gateway would facilitate this by enabling them to exchange cryptographic keys [38]. The gateway acts as a trusted

intermediary, securely exchanging cryptographic keys to establish an encrypted communication channel between the devices. By handling the key exchange process, the gateway ensures that both devices can authenticate each other, reducing the risk of unauthorized access. This mechanism not only initiates secure communication but also simplifies interoperability between devices from distinct systems, as the gateway manages the complexities of key negotiation and distribution [38].

4.5.3. Interoperability protocols

The gateway serves a critical role, extending its function beyond merely securing trust between systems. It actively formats, encrypts, or decrypts data to ensure seamless interpretation and accessibility for the intended recipient, which is essential for preserving data integrity and confidentiality throughout its journey. The gateway carefully adjusts the data's format and encryption level, aligning it with diverse protocols and security requirements, which helps to reduce the likelihood of disruptions or misunderstandings when the data is received. In this way, the gateway not only acts as a protector of trust but also as an enabler, preparing data for accurate delivery and comprehension by the recipient, thus enhancing communication and efficiency across the network [39].

4.6. Shared trust repository

The IoT is an enormous place to navigate. shared trust repository. Serving as a digital stronghold, this repository functions much like an archival library or a fortified vault, safeguarding the most critical elements of digital trust: public keys and certificates [40]. By centralizing these essential security assets, the repository enables devices to verify each other's identities and maintain trusted interactions across the IoT landscape. This centralized approach not only streamlines the authentication process but also reduces the risk of man-in-the-middle attacks, enhancing overall network security. Additionally, the repository can facilitate efficient key management, ensuring that cryptographic keys are regularly updated and securely stored. Ultimately, a robust shared trust repository is vital for fostering a secure and resilient IoT ecosystem.

4.6.1. Storage of public keys

When new entities join the federated system, each carry along its own public key, a digital signature that serves as an identity badge. Likewise, a key in an archival library is carefully filed and indexed within the repository. It is not simply an act of storing. Rather, it represents that the entity has become part of the trusted inner circle of the federated system, indicating that they have been accepted and approved [41].

4.6.2. Certificate verification

As opposed to being a mere storage area, the shared trust repository is an active validation node. Consider this resource as a reference library. Similarly, researchers would rely on an archive to authenticate information. At the same time, in the virtual world, this is done using a credential where a device or entity goes to this registry, for instance, [42], [43]. They can instantaneously check the certificate's validity in an interaction through the repository. That continuous verification procedure assures the entry of authenticated entities into secure communication.

4.6.3. Updates and synchronization

In the world of IoT, entities are always coming in; some drop out or change their credentials. key management includes updating new keys and removing old or compromised keys for validity. However, it becomes increasingly difficult as the decentralization of repositories takes place. There could be many examples of this repository or different pieces of the trust puzzle. Synchronization schemes come into play here, intending to make sure everyone else reflects the rest so that they always maintain a uniform and consistent trust view among themselves.

4.7. Mathematical framework

The mathematical framework for evaluating trust, security, and data transmission dynamics in a federated PKI management system for IoT interoperability is given as N is total number of IoT entities; D_i is number of devices by entity i ; and $P_{i,j}$ is trust probability of an entity i towards j , $0 \leq P_{i,j} \leq 1$.

$$T = [t_{ij}] \text{ where } t_{ij} = P_{ij} \quad (1)$$

where C_i : certificate of entity; i : certificate of entity i .

$$V_{ij}(C_j) = \begin{cases} 1 & \text{if } C_j \text{ is valid and not in } R_i \\ 0 & \text{otherwise} \end{cases} \quad (2)$$

where I_{ij} : Interaction frequency between devices of entity i and j .

$$TWIS_{ij} = I_{ij} \times P_{ij} \quad (3)$$

$$RF_{ij} = \frac{R_{ij}}{D_j} \quad (4)$$

where L_j : Lifespan of certificates issued by entity j ; and A_{ij} : Average age of certificates from entity j as perceived by entity i .

$$CF_{ij} = \frac{L_j - A_{ij}}{L_j} \quad (5)$$

where DI_{ij} : Times data integrity was maintained between entities.

$$DIS_{ij} = \frac{DI_{ij}}{I_{ij}} \times P_{ij} \quad (6)$$

$$CSS_{ij} = TWIS_{ij} \times (1 - RF_{ij}) \times CF_{ij} \times DIS_{ij} \quad (7)$$

$$S_{ij} = P_{ij} \times V_{ij}(C_j) \times CF_{ij} \quad (8)$$

$$E_{ij} = f(\text{data}, C_j) \text{ where } f \text{ is an encryption function} \quad (9)$$

$$M_{ij} = \sqrt{P_{ij} + P_{ji}} \times P_{ji} \quad (10)$$

$$H_i = \frac{\sum_{k=1}^N DI_{ik}}{N-1} \quad (11)$$

where L_{ij} : latency in communication between entity i and j ; B_{ij} : bandwidth of the communication channel between entity i and j .

$$Q_{ij} = \alpha \times B_{ij} - \beta \times L_{ij} \quad (12)$$

$$G_{ij} = \omega_1 \times S_{ij} + \omega_2 \times M_{ij} + \omega_3 \times H_{ij} + \omega_4 \times Q_{ij} \quad (13)$$

In (1) delineates a trust matrix constructed from trust probabilities across all entities. In (2) signifies the digital certificate of an entity. In (3) defines the trust weighted interaction score, measuring interactions modulated by the trust. In (4) enumerates instances where entity i revokes' certificates from entity j . In (5) introduces the certificate freshness index, indicating the relevance of a certificate. In (6) unveils the data integrity score, which combines interaction frequency with upheld data integrity events modulated by trust. In (7) presents the composite security score, an inclusive metric incorporating trust, revocation, certificate freshness, and data integrity. In (8) gauges the overall security reliability of entity j as discerned by entity i . In (9) demarcates the representation of encrypted data. The (10) melds reciprocal trust perceptions between entities i and j . In (11) captures the total instances where entity i maintained data integrity with other entities. In (12) computes the quality of service (QoS), considering attributes like bandwidth and latency between i and j . Finally, in (13) synthesizes the global trustworthiness score, harmonizing facets of security, mutual trust, data integrity, and QoS.

5. EVALUATION METHOD

The proposed approach is evaluated based on scalability (latency), interoperability (success rate), and security (incident detection). The proposed approach is put through a rigorous assessment process with an emphasis on important performance indicators: security is which is provided by incident detection cars, communications interoperability is which is judged by the success rate, and scalability is which is checked by the latency. In order to test scalability designs, random tests are very important for the real-time application because they help it with working capacity of the system even if the workloads are big without affecting response time. The assessment of interoperability is about how well the system would work as a whole

despite having integrated with so many devices and different protocols which is vital in the case of internet of things. Security assessment examines the ability of the system to identify and mitigate attackers, thus data integrity and user privacy will be safe guarded.

5.1. Scalability (latency)

The scalability for an IoT system refers to how the system can consistently transmit data between an ever-increasing number of devices at acceptable timings (latencies). Fundamentally, it assesses whether the system is effective in managing load growth (greater number of devices and volume of data flow) without appreciable deterioration of functioning, specifically with respect to data rate of delivery between devices. To achieve low latency, especially for real-time applications, it is necessary to scale the network so that data is transmitted over the IoT ecosystem in a timely way with quick actions. Given N IoT devices and their communication times t_1, t_2, \dots, t_n where t_i denotes the commutation time for the i^{th} the device in milliseconds, the average latency (L).

$$L(ms) = \frac{1}{N} \sum_{i=1}^N t_i \quad (14)$$

5.2. Interoperability (success rate)

In the context of interoperability (success rate), it measures how effectively the different systems, equipment and other devices can work together in IoT environments. This parameter measures the percentage of successful interactions between diverse devices or systems and their level of operability. Let S be the number of successful interactions, and T be the total number of interactions between IoT devices from different ecosystems. The interoperability success rate (SR) is given in (15).

$$SR(\%) = \left(\frac{S}{T} \right) \times 100 \quad (15)$$

5.3. Security (incident detection)

Incident detection is one form of security in IoT. It measures the success rate of how efficiently the system detects and handles all security breaches, thereby giving an overall measure of the security and incident response. Given D as the number of detected security incidents I as the total number of security incidents, the security incident detection rate (DR) is defined as (16).

$$DR(\%) = \left(\frac{D}{I} \right) \times 100 \quad (16)$$

6. EXPERIMENTAL RESULTS AND ANALYSIS

For this wide-ranging experimental setup, we used various types of IoT devices, including smart thermostats, security cameras, wearables, smart lighting systems, and home automation controllers. These were chosen based on commonness and mixed companies for major players and upstart firms across the global IoTs marketplace. These experiments took place in a highly planned testbed located at a specific lab devoid of external disturbances. We opted to have our dedicated server hosted with high-performance hardware consisting of multi-core processors, fast-speed RAM, and SSD-based storage. Redundancy provisions were made to establish the CA server, which would continuously generate, validate, and manage digital certificates. A separate RA ensured the authentication of device identity as an added measure of security. Also, it had a validation server installed with a firewall and intrusion detection system that verified device certificates when they communicated. It has built upon state-of-the-art networking hardware for its backbone. Enterprise-grade routers and layer 3 switches were used in implementation of simulations that aimed at optimal traffic routing under different complex network situations. Our security layer improved due to firewalls which are in hardware and software forms that guard us against potential external threats. We leveraged the richness of EJBCA's functions for our PKI management, profiting from its meticulous control and thorough reportage. With the aid of the NS3 simulator and custom scripts, we could emulate a sprawling IoT landscape and then test our platform under difficult circumstances. The multiple devices were orchestrated running on the dedicated server having compatibility with various IoT protocols. With Wireshark used for live packet inspection and certificate management tools like OpenSSL providing various PKI utilities (*i.e.*, encryption, decryption), our improved security layer ensured heightened security. Devices were subjected to stringent simulation testing throughout the study's various stages that imitated realistic conditions. This included general security issues like man-in-the-middle attacks through the cross-manufacture communication tests to validate our results into useable scenarios as shown in Table 1.

Table 1. Results obtained

Scenario	Scalability (latency)	Interoperability (success rate)	Security (incident detection)	Devices used
Sensor nodes	3.2 ms	92.5%	Strong (99.7%)	Raspberry Pi-based sensor nodes
IoT gateways	5.1 ms	88.3%	Strong (99.5%)	Intel NUC IoT gateways
Industrial IoT devices	4.7 ms	90.1%	Robust (98.8%)	Siemens PLCs and Allen-Bradley HMIs
Healthcare devices	3.5 ms	94.2%	Robust (99.0%)	Wearable health monitors (Fitbit)
Smart home devices	4.9 ms	87.6%	Strong (99.3%)	Philips Hue smart bulbs
Vehicular IoT (V2X)	2.8 ms	96.4%	Robust (98.9%)	Connected vehicles with V2X modules
Agricultural IoT	4.3 ms	89.8%	Strong (99.2%)	Soil moisture sensors and GPS trackers

The information obtained from the experiments provides valuable insight into various aspects related to the installation of IoT. The corresponding latency values depict scalability variations among diverse IoT designs. Latencies were as best as 2.8 ms in vehicular IoT (V2X), an appropriate indication of its performance potential for real-time vehicle applications that are key for road safety. The same applies to medical devices where their low latency suggests how fast they can deliver data, which may be critical for monitoring and intervention purposes. Conversely, a much higher latency that is often associated with IoT gateways operating as a connection medium from devices to centralized systems demands further study on the issue. Another critical aspect was interoperability, which had varying success rates in the scenarios. In this regard, for instance, the V2X scenario with a successful ratio of 96.4% shows the strong reliability of standards and protocols for this area. Given the safety concerns at play in vehicular communications, such a high level of interoperability becomes essential. The smart home category, though with a poor success rate of 87.6%, introduces possible issues in consumer behavior towards such devices. Perhaps this low-rate results from many manufacturers and unique protocols indicating that some level of common standard is needed in the smart home marketplace.

The findings on security were remarkable in the contemporary world of digital technology. Incident detection rates were high, amounting to 99.7% for sensor nodes and 99.5% for IoT gateways. These numbers show how effective these security protocols were. Nevertheless, it is noteworthy that the industrial IoT devices slightly lowered the incidence detection rate. Although that figure is still impressive, one weakness in an industrial setting can lead to exponential consequences, which underscores the constant effort necessary to achieve better results. Also, the use of the range of devices in this study shows its comprehensiveness and includes simple Raspberry Pi based nodes up to the modern connected vehicles' modules. This makes it possible for the findings to be more than limited but widely accepted in the very comprehensive IoT sphere. Therefore, these findings are crucial in the path of IoT research. In addition, they are neutral, pointing out both strong sides and points for improvements in order to maintain the security, efficiency and interoperability of the IoT environment.

7. CONCLUSION

The extent of our experiments with different IoT devices demonstrated the strengths as well as limitations of federated PKI in the security of IoT interoperability. The latency performance varies by sector, and V2X and medical devices emerge as some of the most efficient ones. In this respect, although interoperability performance was rather uneven such as in V2X, which showed incredible reliability again underlines those specific areas, such as the smart home sector, can be markedly improved through standardization of corresponding procedures. Moreover, good rates of incidents are seen to affirm strength in security measures, though there is a need for continued enhancement, especially in the industrial internet world. The diversity of the devices range—from Raspberry Pi-based nodes to current vehicular modules demonstrates this study's comprehensive nature, whose results are highly relevant for IoT. These findings are crucial to the current debate on IoT security and interoperability. By identifying the difficulties of ensuring consistency across heterogeneous systems in the present digital-centric era, this paper introduces some practical steps that can assist organizations and developers in boosting trust and security within an IoT's infrastructure. Our research emphasizes the integral nature of federated PKI in bringing forth the IoT security infrastructure across different sectors where special attention is given to the success in V2X and medical devices, yet unified practices are wanted to improve the interoperability in domains like smart homes.

ACKNOWLEDGMENT

The authors extend their appreciation to the Arab Open University for funding this work through AOU research fund No. (AOURG-2023-015)




REFERENCES

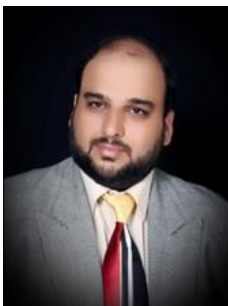
- [1] A. R. Javed *et al.*, "Future smart cities: requirements, emerging technologies, applications, challenges, and future aspects," *Cities*, vol. 129, 2022, doi: 10.1016/j.cities.2022.103794.
- [2] K. Sha, W. Wei, T. Andrew Yang, Z. Wang, and W. Shi, "On security challenges and open issues in internet of things," *Future Generation Computer Systems*, vol. 83, pp. 326–337, 2018, doi: 10.1016/j.future.2018.01.059.
- [3] J. Höglund, S. Lindemer, M. Furuheid, and S. Raza, "PKI4IoT: towards public key infrastructure for the internet of things," *Computers and Security*, vol. 89, 2020, doi: 10.1016/j.cose.2019.101658.
- [4] X. Liu, M. Zhao, S. Li, F. Zhang, and W. Trappe, "A security framework for the internet of things in the future internet architecture," *Future Internet*, vol. 9, no. 3, 2017, doi: 10.3390/fi9030027.
- [5] N. A. Khan, "PKI-based security enhancement for IoT in 5G networks," in *Lecture Notes in Networks and Systems*, Springer Nature Singapore, 2022, pp. 217–225.
- [6] O. Vermesan *et al.*, "Internet of things strategic research roadmap," in *Internet of Things - Global Technological and Societal Trends from Smart Environments and Spaces to Green Ict*, New York: River Publishers, 2022, pp. 9–52.
- [7] J. P. Dias, A. Restivo, and H. S. Ferreira, "Designing and constructing internet-of-Things systems: an overview of the ecosystem," *Internet of Things*, vol. 19, 2022, doi: 10.1016/j.iot.2022.100529.
- [8] A. S. Khan *et al.*, "Blockchain-based lightweight multifactor authentication for cell-free in ultra-dense 6G-based (6-CMAS) cellular network," *IEEE Access*, vol. 11, pp. 20524–20541, 2023, doi: 10.1109/access.2023.3249969.
- [9] A. Rashid, A. Masood, H. Abbas, and Y. Zhang, "Blockchain-based public key infrastructure: a transparent digital certification mechanism for secure communication," *IEEE Network*, vol. 35, no. 5, pp. 220–225, 2021, doi: 10.1109/mnet.101.2000532.
- [10] J. Sedlmeir, R. Smethurst, A. Rieger, and G. Fridgen, "Digital identities and verifiable credentials," *Business and Information Systems Engineering*, vol. 63, no. 5, pp. 603–613, 2021, doi: 10.1007/s12599-021-00722-y.
- [11] A. D. Aguru, S. B. Erukala, and I. Kavati, "Smart contract based next-generation public key infrastructure (PKI) using permissionless blockchain," in *Lecture Notes in Networks and Systems*, Springer International Publishing, 2022, pp. 625–635.
- [12] L. Babun, K. Denney, Z. B. Celik, P. McDaniel, and A. S. Uluagac, "A survey on IoT platforms: communication, security, and privacy perspectives," *Computer Networks*, vol. 192, Jun. 2021, doi: 10.1016/j.comnet.2021.108040.
- [13] P. Shi, H. Wang, S. Yang, C. Chen, and W. Yang, "Blockchain-based trusted data sharing among trusted stakeholders in IoT," *Software: Practice and Experience*, vol. 51, no. 10, pp. 2051–2064, Oct. 2021, doi: 10.1002/spe.2739.
- [14] N. Torres, P. Pinto, and S. I. Lopes, "Security vulnerabilities in LPWANs—an attack vector analysis for the IoT ecosystem," *Applied Sciences*, vol. 11, no. 7, Apr. 2021, doi: 10.3390/app11073176.
- [15] H. Xu, P. V. Klaine, O. Onireti, B. Cao, M. Imran, and L. Zhang, "Blockchain-enabled resource management and sharing for 6G communications," *Digital Communications and Networks*, vol. 6, no. 3, pp. 261–269, Aug. 2020, doi: 10.1016/j.dcan.2020.06.002.
- [16] A. Sharma, S. Kaur, and M. Singh, "A comprehensive review on blockchain and internet of things in healthcare," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 10, Oct. 2021, doi: 10.1002/ett.4333.
- [17] L. Bai, L. Yao, S. S. Kanhere, X. Wang, and Z. Yang, "Automatic device classification from network traffic streams of internet of things," in *2018 IEEE 43rd Conference on Local Computer Networks (LCN)*, Oct. 2018, pp. 1–9, doi: 10.1109/LCN.2018.8638232.
- [18] T. Giannetsos and I. Krontiris, "Securing V2X communications for the future," in *Proceedings of the 14th International Conference on Availability, Reliability and Security*, Aug. 2019, pp. 1–8, doi: 10.1145/3339252.3340523.
- [19] K. Siountri, E. Skondras, and D. D. Vergados, "Towards a smart museum using BIM, IoT, blockchain and advanced digital technologies," in *Proceedings of the 3rd International Conference on Vision, Image and Signal Processing*, Aug. 2019, pp. 1–6, doi: 10.1145/3387168.3387196.
- [20] A. Rech, M. Pistauer, and C. Steger, "A novel embedded platform for secure and privacy-concerned cross-domain service access," in *2019 IEEE Intelligent Vehicles Symposium (IV)*, Jun. 2019, pp. 1961–1967, doi: 10.1109/IVS.2019.8814123.
- [21] B. Yin, H. Yin, Y. Wu, and Z. Jiang, "FDC: a secure federated deep learning mechanism for data collaborations in the internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6348–6359, Jul. 2020, doi: 10.1109/JIOT.2020.2966778.
- [22] S. N. Swamy and S. R. Kota, "An empirical study on system level aspects of internet of things (IoT)," *IEEE Access*, vol. 8, pp. 188082–188134, 2020, doi: 10.1109/ACCESS.2020.3029847.
- [23] A. H. Sodhro, S. Pirbhulal, M. Muzammal, and L. Zongwei, "Towards blockchain-enabled security technique for industrial internet of things based decentralized applications," *Journal of Grid Computing*, vol. 18, no. 4, pp. 615–628, Dec. 2020, doi: 10.1007/s10723-020-09527-x.
- [24] O. Abdulkader, A. M. Bamhdi, V. Thayananthan, F. Elbouraey, and B. Al-Ghamdi, "A lightweight blockchain based cybersecurity for IoT environments," in *2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, Jun. 2019, pp. 139–144, doi: 10.1109/CSCloud/EdgeCom.2019.000-5.
- [25] Y. Xu *et al.*, "BESIFL: blockchain-empowered secure and incentive federated learning paradigm in IoT," *IEEE Internet of Things Journal*, vol. 10, no. 8, pp. 6561–6573, Apr. 2023, doi: 10.1109/JIOT.2021.3138693.
- [26] P. Fraga-Lamas, S. I. Lopes, and T. M. Fernández-Caramés, "Green IoT and edge AI as key technological enablers for a sustainable digital transition towards a smart circular economy: an industry 5.0 use case," *Sensors*, vol. 21, no. 17, Aug. 2021, doi: 10.3390/s21175745.
- [27] S. Munirathinam, "Industry 4.0: industrial internet of things (IIOT)," in *Advances in Computers*, Elsevier, 2020, pp. 129–164.
- [28] T. Poongodi, A. Rathee, R. Indrakumari, and P. Suresh, "IoT sensing capabilities: sensor deployment and node discovery, wearable sensors, wireless body area network (WBAN), data acquisition," in *Intelligent Systems Reference Library*, Springer International Publishing, 2020, pp. 127–151.
- [29] S. Bansal and D. Kumar, "IoT ecosystem: a survey on devices, gateways, operating systems, middleware and communication," *International Journal of Wireless Information Networks*, vol. 27, no. 3, pp. 340–364, Sep. 2020, doi: 10.1007/s10776-020-00483-7.
- [30] S. C. Sethuraman, P. Kompally, S. P. Mohanty, and U. Choppali, "MyWear: a novel smart garment for automatic continuous vital monitoring," *IEEE Transactions on Consumer Electronics*, vol. 67, no. 3, pp. 214–222, Aug. 2021, doi: 10.1109/TCE.2021.3085888.
- [31] S.-R. Oh, Y.-D. Seo, E. Lee, and Y.-G. Kim, "A comprehensive survey on security and privacy for electronic health data," *International Journal of Environmental Research and Public Health*, vol. 18, no. 18, Sep. 2021, doi: 10.3390/ijerph18189668.
- [32] P. R. Carnley and H. Kettani, "Identity and access management for the internet of things," *International Journal of Future Computer and Communication*, vol. 8, no. 4, pp. 129–133, Dec. 2019, doi: 10.18178/ijfcc.2019.8.4.554.
- [33] K. Srinivas, V. Janaki, V. Shankar, and P. KumarSwamy, "Crypto key protection generated from images and chaotic logistic maps," in *Communications in Computer and Information Science*, Springer Singapore, 2021, pp. 253–262.
- [34] Q. Wang, D. Gao, and D. Chen, "Certificate revocation schemes in vehicular networks: a survey," *IEEE Access*, vol. 8, pp. 26223–26234, 2020, doi: 10.1109/ACCESS.2020.2970460.




- [35] E. Leroux and P.-C. Pupion, "Smart territories and IoT adoption by local authorities: a question of trust, efficiency, and relationship with the citizen-user-taxpayer.," *Technological Forecasting and Social Change*, vol. 174, Jan. 2022, doi: 10.1016/j.techfore.2021.121195.
- [36] S. Patil and P. Gokhale, "Multi-criteria approach for handling sophisticated data transmission over gateways in blockchain and internet of things (IoT) federated networks," *Expert Systems*, vol. 39, no. 10, Dec. 2022, doi: 10.1111/exsy.13127.
- [37] H. Hadan, N. Serrano, S. Das, and L. J. Camp, "Making IoT worthy of human trust," *SSRN Electronic Journal*, 2019, doi: 10.2139/ssrn.3426871.
- [38] M. Abdalzaher, M. Fouda, A. Emran, Z. Fadlullah, and M. Ibrahim, "A survey on key management and authentication approaches in smart metering systems," *Energies*, vol. 16, no. 5, Mar. 2023, doi: 10.3390/en16052355.
- [39] P. Rösler and J. Schwenk, "Interoperability between messaging services secure implementation of encryption," *Hackmanit*, 2023.
- [40] J. Byabazaire, G. O'Hare, and D. Delaney, "Data quality and trust: review of challenges and opportunities for data sharing in IoT," *Electronics*, vol. 9, no. 12, Dec. 2020, doi: 10.3390/electronics9122083.
- [41] P. Huang, K. Fan, H. Yang, K. Zhang, H. Li, and Y. Yang, "A collaborative auditing blockchain for trustworthy data integrity in cloud storage system," *IEEE Access*, vol. 8, pp. 94780–94794, 2020, doi: 10.1109/ACCESS.2020.2993606.
- [42] F. Z. D. N. Costa, R. J. G. B. De Queiroz, G. P. Bittencourt, and L. Teixeira, "Distributed repository for software packages using blockchain," *IEEE Access*, vol. 10, pp. 112502–112514, 2022, doi: 10.1109/ACCESS.2022.3216569.
- [43] H. Yigitler, B. Badihi, and R. Jäntti, "Overview of time synchronization for IoT deployments: clock discipline algorithms and protocols," *Sensors*, vol. 20, no. 20, Oct. 2020, doi: 10.3390/s20205928.

BIOGRAPHIES OF AUTHORS



Omar Ahmed Abdulkader    received his B.E. degree in computer science from King Abdulaziz University, Jeddah, KSA, in 2002. He received his M.Sc. degree "traffic parameter extracting using image process" from King Abdulaziz in 2010. He received his Ph.D. degree "analytical cybersecurity model based on lightweight cryptographic for IoT" from King Abdulaziz University in 2019, Jeddah, KSA. His current research interests include cybersecurity, IoT, M2M, artificial intelligence, blockchain, cloud computing, location-based services and machine learning. He can be contacted at email: o.abdulkader@arabou.edu.sa.



Muhammad Jawad Ikram    received the B.E. degree in computer systems engineering from the University of Engineering and Technology, Peshawar, Pakistan, in December 2010, the M.Sc. degree with distinction in networks and performance engineering from the University of Bradford, U.K., in December 2012, and the Ph.D. degree from King Abdulaziz University (KAU), Jeddah, Saudi Arabia, in March 2018. From August 2018 till August 2023, he has served as an assistant professor of computer science at various universities including International Islamic University (IIU), Islamabad, Pakistan (2018–2019), Riphah International University, Pakistan (2019), PMAS Arid Agriculture University, Rawalpindi, Pakistan (2019–2020), Jeddah International College, Saudi Arabia (2020–2023). Since September 3, 2023, he has been working as an assistant professor at the Arab Open University, Saudi Arabia. He has published his research in a number of refereed journals and conferences. His recent research interests include machine learning, energy-aware algorithms, exascale computing, HPC, GPU computing, game theory, internet of things, and performance modeling. He can be reached by his email at m.ikram@arabou.edu.sa.