International Institute of Information Technology - Hyderabad

Research in Information Security, 2024

Title : Identity-Based Proxy Signature Scheme

March 24, 2024

Team

Name	RollNumber
Pradhyumna Palore	2023202022
Ayush Rai	2023202020
Shiv Modi	2023202024

Contents

Abstract :

This work presents a new method to secure communication in Industrial Internet of Things (IIoT) networks with an identity-based proxy signature system. Traditionally, there are often large amounts of certificate management that can be slow, complex, and much less efficient as networks scale. In contrast, our method employs identity-based cryptography, so each device can create a public key out of its identity alone (no certificates required). This takes out key management tasks, enabling scalability and ease to the system.

Bilinear pairing is a key part of our method: that enables efficient multi-signature verification, allowing multiple devices to sign and authenticate data with minimal computational overhead. In IIoT environments, this is even more crucial, because devices in large-scale IIoT setups like smart factories or autonomous systems will constantly need to communicate with each other in real-time with minimal slowdown caused by heavy computational demands.

To protect the system against forgery and unauthorized access, we use the well known assumption on computational Diffie Hellman (CDH), assuming that the latter assumption is computationally hard. To securely and flexibly allow devices interacting with our network, our system manages proxy keys carefully and simplifies delegating authority, even while devices join or leave the network.

Finally, this project presents a powerful, and efficient authentication solution for IIoT networks that donates towards the reliable communication of data across various industrial applications.

KEYWORDS :

Identity-Based Cryptography, Proxy Signature Scheme, Industrial Internet of Things (IIoT), Bilinear Pairing, Computational Diffie-Hellman (CDH) Assumption, Multi-Signature Verification, Certificate-Free Authentication

1 Introduction

1.1 Background

The rise of the Industrial Internet of Things (IIoT) has ushered in significant advancements in industrial automation, data collection, and real-time monitoring, and it has done so rapidly. The inherent distributed and resource-constrained nature of IIoT devices, however, poses important security challenges. Without a doubt, secure communication and data integrity over IIoT networks are one point of concern that needs further consideration. Currently, traditional cryptographic techniques can be extremely computationally expensive on IIoT devices, requiring specialized techniques like certificate-based proxy signatures. In such scenarios, secure delegation of signing rights is an important capability, and these techniques enable the distribution of signing rights such that signing can be performed on behalf of a primary user or system by multiple devices or entities. Properly used, certificate-based proxy signatures can be applied in IIoT environments in data security transmission, device and network authentication, and multi-party signature verification for industrial automation environments, healthcare monitoring, and supply chain management.

1.2 Network Model

The main paper describes a certificate-based proxy signature scheme for operation in an IIoT network characterized by many key entities. This model includes:

1. **Cloud Server:** An intermediate node (an intermediate computer) that coordinates data processing and storage for IIoT devices.
2. **Certification Authority (CA):** An entity trusted to generate certificates and keys for IIoT devices to ensure authenticity among the network.
3. **Data Owner:** The user's main entity that allows other devices (to some extent) to act on its behalf and perform signing duties.
4. **Proxy Signer (IIoT Device):** Proxy signing authorized devices (typically resource constrained), that verify and forward data securely on behalf of the Data Owner.

This network model allows secure communication and delegates signing authority in IIoT environments requiring central control and verification to ensure the integrity and trust of data

1.3 Attack Model

IoT environment has many threats that can occur such as Security threats of Authentication and Data integrity. The primary paper considers the following attack vectors:

1. **Man-in-the-Middle (MitM) Attacks:** IIoT applications help attackers intercept and (potentially) alter the data 'in transit' from IIoT devices to the central server, thus compromising the integrity and authenticity of data.
2. **Key Exposure and Unauthorized Delegation:** Attacks could impersonate legitimate devices meaning they could take unauthorized actions in the network if proxy keys are exposed.
3. **Replay Attacks:** Secure communication without suitable signature timestamping or revocation operations is challenging, leaving adversaries with the opportunity to capture and replay legitimate messages.

This attack model brings to light the imperative of the need for secure cryptographic solutions, such as certificate-based proxy signatures, to protect data and deny access in the limited resource context of IIoT networks.

1.4 Research Contributions :

This report makes several key contributions to the field of IIoT security:

1. **Design of a Lightweight Identity-Based Proxy Signature Scheme:** In this project, we introduce a new identity-based proxy signature scheme tailored for IIoT environments. The scheme replaces such certificates with public keys derived from, and uniquely mapped to, device identities, thus dispensing with the computationally intense generation of traditional certificates. In particular, this simple model is highly conducive to IIoT devices with limited resources since it facilitates their communication over a secure and efficient network in an easy, lightweight manner.

2. **Application of Bilinear Pairing for Scalable Multi-Proxy Authentication:** The scheme also takes bilinear pairing, a mathematical operation that enables a group of multiple devices to sign and authenticate the data with one verification step, to support large-scale deployment of IIoT networks. This not only increases the scalability of the system but improves the system performance, and is extremely useful in contexts where there is a lot of frequent and seamless device interaction such as smart manufacturing or autonomous systems.

3. **Enhanced Security through the Computational Diffie-Hellman (CDH) Assumption:** The CDH assumption allows us to additionally strengthen security against forgeries, unauthorized access, and man-in-the-middle attacks. The project shows that by setting up a formal security framework the scheme is resistant to several attacks and is therefore a trustworthy solution for IIoT applications in which device security is and data integrity is essential.

4. **Increased Efficiency in Key Management and Proxy Delegation:** Furthermore, the identity-based nature of this scheme facilitates key management and proxy delegation, two key operation components in dynamic IIoT networks. The scheme enables smooth and secure delegation, helping to reduce the computational load for generating proxy signing keys that allow proxy signing to continue, despite frequently experiencing network new join/leaves. It allows for on the fly modifications, so the system remains efficient and graspable under variation of high dynamics.

2 Literature Review :

Provision of secure, efficient and scalable solutions to IIoT environments in certificate based proxy signature domain has been a focus in the literature, shown through a constant effort to find secure solutions that are also efficient and can be scaled in resource constrained situations. Selected papers and their contributions to this field are summarized below.

2.1 Short Certificate-Based Proxy Signature Scheme from Pairings(2017):

In this paper, we present a proxy signature scheme based on elliptic curve pairings for the case of low bandwidth environment. The scheme addresses the space and bandwidth requirement in wireless communication channels by pairing the scheme. In particular, this method is advantageous for cases involving frequent authentication and delegation, such as mobile communication and online transactions. Though, making use of these pairings adds additional computational complexity, and may not be feasible in many IIoT applications with the least amount of computation resources available.

2.2 Security and Privacy Challenges in Industrial IoT(2015):

This paper provides a complete picture of the security and privacy in the industrial IoT (IIoT) arena. It exposes the fact that cyberattacks on embedded and cyber physical systems may result in severe physical consequences. It proposes that as IIoT systems develop, they require a holistic security framework to support privacy concerns, reduce risk, and shore up the system's resiliency against attacks. Although it is not focused on any important security techniques, this paper emphasizes the importance of security in IIoT applications as the direct responsibility of security influenced the requirement of secure proxy signature schemes.

2.3 Secure and Efficient Certificate-Based Proxy Signature Schemes for IIoT (2021):

This research proposes three novel constructions for certificate-based proxy signatures specifically designed for the IIoT context. Each construction improves on prior schemes by enhancing delegation validity verification and ensuring public verifiability of the delegation process. The authors identify security issues in previous schemes, such as the potential for unauthorized delegation reuse, and resolve these issues with their designs. Through formal proofs based on the discrete logarithm problem and the random oracle model, these schemes demonstrate computational and communication efficiency. However, the schemes still face challenges related to scalability in large-scale IIoT networks.

2.4 An Efficient and Provable Certificate-Based Proxy Signature Scheme for IIoT Environment(2020):

This primary paper presents a pairing-free certificate-based proxy signature (PFCBPS) scheme optimized for IIoT environments. The proposed scheme addresses key escrow and secret key distribution issues that affect other identity-based or certificate-less schemes. With a computational cost that is notably lower than many existing methods, the PFCBPS scheme offers a practical approach for IIoT applications, reducing computational demands and signature length. Despite its improvements, this paper leaves open research gaps, such as advanced protection against key exposure and scalability for diverse IIoT networks.

Paper	**Technique Used**	**Advantages**	**Disadvantages**
Short Certificate-Based Proxy Signature Scheme from Pairings	Proxy signature with elliptic curve pairings	Efficient for low-bandwidth channels; suitable for mobile communication and online transactions	High computational cost due to pairings, limiting feasibility in highly resource-constrained IIoT environments
Security and Privacy Challenges in Industrial IoT	Overview of IIoT security challenges	Highlights the need for robust security frameworks in IIoT; addresses privacy concerns in IIoT systems	Does not propose a specific cryptographic solution; lacks focus on concrete implementation methods
Secure and Efficient Certificate-Based Proxy Signature Schemes for IIoT	Certificate-based proxy signature without pairings	Improved security with formal proofs; efficient for computation and communication; public verifiability	Lacks scalability for large IIoT deployments; does not fully address key exposure vulnerabilities
An Efficient and Provable Certificate-Based Proxy	Pairing-free certificate-based proxy	Lower computational cost compared to other methods; mitigates key exposure vulnerabilities	Research gaps in scalability, advanced threat resistance, and threat response methods
Signature Scheme for IIoT	Signature (PFCBPS)	Addresses escrow and SKD issues; suitable for IIoT	Limited by lack of distributed ledger integration

It is shown in this literature survey that there remain ongoing challenges and developments in certificate based proxy signature schemes for use in IIoT. However, each of these schemes has unique benefits, but also has flaws particularly in regard to computational feasibility and scalability. More work is required to develop complete, scalable solutions for addressing the advanced threats, as IIoT networks scale.

3 Our Proposal :

3.1 Motivation :

In such applications as manufacturing systems, autonomous vehicles, and smart infrastructure, the number of devices that interact in real-time trading sensitive information with each other can become highly heterogeneous, thus being large, or resource-constrained. United States, traditional certificate-based approach to security in the IIoT lacks efficiency as a result of high computational overhead, complex key issues and limited scalability. Certificate-based systems are not an easy solution to deploy in IIoT when the devices require secure, rapid and resource-light communication. In this proposal, we seek to meet these challenges through the design of a lightweight, scalable and secure identity-based proxy signature scheme that eliminates the need for the traditional certificates. The proposed approach is not only computationally efficient and simplified key management but also secure and suitable for dynamic IIoT networks with high device interactivity.

3.2 Proposal :

This proposal introduces an **identity-based proxy signature** scheme optimized for IIoT networks, eliminating the need for traditional certificates by deriving public keys directly from device identities. Using **bilinear pairing** for efficient multi-signature verification, it enables rapid, scalable, and secure authentication across resource-constrained IIoT environments. Underpinned by **the Computational Diffie-Hellman (CDH)** assumption, the scheme provides enhanced security against forgery and unauthorized access, making it ideal for real-time, dynamic IIoT applications.

4 Analysis of Our Proposal :

The proposed identity-based bilinear pairing scheme provides substantial improvements over traditional certificate-based proxy signature systems in IIoT applications. In certificate-based schemes, challenges include complex key management, high computational overhead, and limited scalability—all crucial for resource-constrained IIoT devices. This section offers an in-depth mathematical analysis, incorporating equations, proofs, and explanations to clarify how the identity-based bilinear pairing approach enhances security, reduces computational demands, and improves scalability.

4.1 Key Concepts :

4.1.1 Bilinear Pairing Properties :

Bilinear pairing is a foundational operation in identity-based cryptographic schemes. Formally, bilinear pairing is defined as a map:

$$e : G_1 \times G_1 \to G_2,$$

where G_1 and G_2 are groups of prime order q(i.e., every element in these groups has order q), and there is a generator P in G_1. This map satisfies specific properties that make it suitable for cryptographic operations:

- **Bilinearity:** For $P, Q \in G_1$ and scalars $a, b \in \mathbb{Z}_q$ (the set of integers modulo q), the following holds:

  $$e(aP, bQ) = e(P, Q)^{ab}$$

  This property allows the transformation of scalar multiplications in the group into an exponentiation in the target group G_2. This is essential for cryptographic operations that involve combining multiple signatures or keys.

- **Nondegeneracy:** There exists at least one pair $P, Q \in G_1$ such that $e(P, Q) \neq 1$. This ensures that the pairing map produces meaningful outputs and is not trivial.

- **Efficient Computability:** The pairing operation $e(P, Q)$ can be computed efficiently for any $P, Q \in G_1$.

Implications: Bilinearity enables efficient multi-signature verification. This property is crucial in IIoT, where multiple devices may need to authenticate a single message. The ability to aggregate signatures and verify them in a single operation, using e, reduces computational and communication overhead, making the system scalable.

4.1.2 Computational Diffie-Hellman (CDH) Assumption :

The CDH assumption secures the identity-based scheme against forgery by making certain operations computationally infeasible. The assumption is stated as follows:

- **CDH Problem:** Given elements $P, aP, bP \in G_1$ where $a, b \in \mathbb{Z}_q$, it is computationally infeasible to compute abP.
- **CDH Assumption:** No polynomial-time algorithm can solve the CDH problem with a non-negligible probability of success. This assumption ensures that adversaries cannot easily derive shared keys or forge signatures by manipulating known elements.

Implications: The CDH assumption provides a foundation for the security of identity-based multiproxy signature schemes (Identity based proxy signature). By ensuring that computing shared keys from partial values is infeasible, the CDH assumption prevents adversaries from forging valid proxy signatures. This is particularly relevant for IIoT, where compromised devices could otherwise pose significant security risks.

4.2 Applications in Identity-Based Signature Scheme

4.2.1 Identity-Based Key Generation

Identity-based schemes eliminate the need for certificates by deriving public and private keys directly from unique identities, such as device IDs. This process reduces the management burden and computational complexity associated with certificates.

- **Public Key Generation:** For a device with identity ID_i, its public key Q_{ID_i} is computed as:

  $$Q_{ID_i} = H_1(ID_i)$$

  where H_1 is a hash function that maps the identity ID_i to a point on the elliptic curve in G_1. This operation has $O(1)$ complexity since it only requires a single hash computation.

- **Private Key Generation:** The trusted authority (TA) computes the private key S_{ID_i} for the device as:

  $$S_{ID_i} = s \cdot Q_{ID_i}$$

  where s is a master secret key known only to the TA. The scalar multiplication $s \cdot Q_{ID_i}$ ensures that only the TA can generate valid private keys.

4.2.2 Delegation Generation

- **Step 1: Warrant Message**

  The original signer U_0 generates a warrant message w containing:

  - Identity information for U_0 and the proxy group.
  - A delegation period.
  - The scope of the proxy authority.
  - Message types to be delegated.

  The warrant message is critical as it encapsulates all necessary information for the delegation. This includes the identity of the original signer U_0, which is essential for traceability, and the proxy group that will perform the signing. The delegation period and scope ensure that the proxy's authority is limited and specified, preventing misuse of power.

- **Step 2: Random Selection and Computation**

  The original signer U_0 randomly chooses $r_0 \in \mathbb{Z}_q^*$ and computes:

  $$R_0 = r_0 P$$

  Computes:

  $$h_0 = H_2(w, R_0)$$

  Computes the delegation value:

  $$V_0 = r_0 h_0 + SID_0$$

  The random choice of r_0 ensures that the computation of R_0 introduces a level of unpredictability, which is crucial for security. The computation of $h_0 = H_2(w, R_0)$ provides a hash that binds the warrant message and the random value, ensuring integrity. The delegation value V_0 combines r_0, the hash h_0, and the private key SID_0. This construction allows V_0 to serve as a proof of delegation that can be verified by proxy signers.

- **Step 3: Sending Delegation Data**

  For each proxy signer U_i (for $1 \leq i \leq n$), the original signer U_0 sends the tuple

  $$\sigma_0 = (R_0, V_0)$$

  along with the warrant w.

  Sending $\sigma_0 = (R_0, V_0)$ along with the warrant w is how U_0 communicates the delegation to the proxy signers. This tuple contains all the information necessary for each proxy signer to validate the authority they are granted.

- **Step 4: Verification by Proxy Signer**

  Upon receiving (w, R_0, V_0) through a secure channel, each proxy signer U_i computes:

  $$h_0 = H_2(w, R_0)$$

  Then checks the following verification equation:

  $$e(P, V_0) = e(P_{pub}, QID_0) \cdot e(R_0, h_0)$$

  If the equality holds, U_i accepts σ_0 as a valid delegation.

  The proxy signer U_i computes h_0 again using the received warrant and R_0 to ensure that it matches the original context of the delegation. The verification equation is pivotal as it ensures that V_0 is indeed valid and corresponds to the original signer's public key QID_0. If this equality holds, it confirms that U_i has the right to act on behalf of U_0 without the risk of forgery or misuse.

- **Step 5: Proof of Correctness for Delegated token :**

$$\begin{aligned}
e(P, V_0) &= e(P, r_0 h_0 + S_{ID_0}) \\
&= e(P, r_0 h_0) \cdot e(P, S_{ID_0}) \\
&= e(P, h_0)^{r_0} \cdot e(P, s \cdot Q_{ID_0}) \\
&= e(P, h_0)^{r_0} \cdot e(P, Q_{ID_0})^s \\
&= e(r_0 \cdot P, h_0) \cdot e(s \cdot P, Q_{ID_0}) \\
&= e(R_0, h_0) \cdot e(P_{pub}, QID_0) \\
&= e(P_{pub}, QID_0) \cdot e(R_0, h_0)
\end{aligned}$$

4.2.3 Proxy Key Generation

Before generating multiproxy signatures on a message m and a warrant w, each proxy signer U_i first generates a proxy signing key using the delegation (R_0, V_0) and their private key S_{U_i} as follows:

- **Step 1: Random Selection and Public Key Computation**

  U_i selects a random secret $r_i \in \mathbb{Z}_q^*$ and computes the public proxy key:

  $$R_i = r_i P$$

  This public proxy key R_i is then broadcasted to the proxy group.

- **Step 2: Proxy Signing Key Generation**

  U_i generates the proxy signing key as follows:

  $$S_{U_i} = r_i h_0 + S_{ID_i} + V_0$$

  where $h_0 = H_2(w, R_0)$. The generation of S_{U_i} ensures that each proxy signer has a unique signing key derived from their random selection r_i and the previously established values S_{ID_i} and V_0.

- **Step 3: Public Parameter Publication**

  U_i publishes a public parameter list:

  $$\text{Public Parameters} = (R_i, R_0, w)$$

  Note that the random secret r_i is no longer needed for the verification process, which simplifies the verification phase for other proxy signers.

- **Step 4: Final Multiproxy Signature Generation**

  To realize a multiproxy signature with the proxy signing key, the only proxy signer who obtains V_0 and S_{ID_i} computes:

  $$X = \sum_{i=1}^{n} X_i$$

  such that:

  $$V_i = X_i h + S_{U_i}$$

  where $h = H_3(m, X)$.

- **Step 5: Sending Partial Proxy Signature**

  U_i sends a partial proxy signature:

  $$\sigma_i = (w, R_0, R_i, X_i, V_i)$$

  to a clerk who is the designated proxy signer in the proxy group.

- **Step 6: Verification by Clerk**

  The clerk verifies the validity of σ_i using the verification equation:

  $$e(P, V_i) = e(P_{pub}, QID_0 + QID_i) \cdot e(X_i, h) \cdot e(R_0 + R_i, h_0)$$

  If the verification holds, the clerk computes:

  $$V = \sum_{i=1}^{n} V_i \quad \text{and} \quad R = \sum_{i=1}^{n} R_i$$

  Finally, the clerk generates a multiproxy signature for the message m as:

  $$\sigma = (w, R_0, R, X, V)$$

- **Step 7: Proof of Correctness for single proxy signature :**

$$\begin{aligned}
e(P, V_i) &= e(P, x_i h + S_{U_i}) \\
&= e(P, x_i h) \cdot e(P, r_i h_0) \cdot e(P, S_{ID_i}) \cdot e(P, V_0) \\
&= e(x_i P, h) \cdot e(r_i P, h_0) \cdot e(sP, Q_{ID_i}) \cdot e(r_0 P, h_0) \cdot e(sP, Q_{ID_0}) \\
&= e(X_i, h) \cdot e(R_i, h_0) \cdot e(P_{pub}, Q_{ID_i}) \cdot e(R_0, h_0) \cdot e(P_{pub}, Q_{ID_0}) \\
&= e(P_{pub}, Q_{ID_0} + Q_{ID_i}) \cdot e(R_0 + R_i, h_0) \cdot e(X_i, h).
\end{aligned}$$

4.2.4 Multiproxy Verification

After receiving the multiproxy signature $\sigma = (w, R_0, R, X, V)$ for the message m, anyone can verify σ as follows:

- **Step 1: Conformance Check**

  Given the set of identities $\{ID_j\}_{j\in M}, m$, and σ, the verifier first checks if the message m conforms to the warrant w. The warrant w typically includes the message types to be delegated and other relevant information. If the message does not conform to the specifications laid out in the warrant, the verification fails immediately, ensuring that only properly authorized messages can be processed.

- **Step 2: Proxy Signer Verification**

  The verifier then checks if the n proxy signers $U_1, U_2, \ldots, U_n$ are correctly listed in the warrant w. Each proxy signer must be a member of the designated group specified in w. If any of the signers are not authorized members as per the warrant, the verification fails. This step is crucial as it maintains the integrity of the delegation, ensuring that only valid signers can participate in the signature generation process.

- **Step 3: Signature Validation**

  The final step involves the verification of the multiproxy signature itself. The verifier accepts σ if and only if the following equation is satisfied:

$$e(P, V) = e\left(P_{pub}, QID_0 + \sum_{i=1}^{n} QID_i\right) \cdot e(X, h) \cdot e(R + nR_0, h_0).$$

  Here:

  - $e(P, V)$ represents the pairing of the generator point P with the multiproxy signature value V.
  - The term $e(P_{pub}, QID_0 + \sum_{i=1}^{n} QID_i)$ ensures that the public key of the original signer QID_0 and the public keys of all proxy signers QID_i are correctly aggregated and associated with the signature.
  - The component $e(X, h)$ links the combined partial signatures to the hash of the message and the aggregate of the partial signatures.
  - Finally, $e(R + nR_0, h_0)$ verifies that the aggregate of the public proxy keys aligns with the computed hash value h_0 derived from the warrant and the original random value R_0.

- **Step 4: Proof of Correctness for Multi proxy signature :**

$$\begin{aligned}
e(P, V) &= e\left(P, \sum_{i=1}^{n} (x_i h + S_{U_i})\right) \\
&= e\left(P, h\sum_{i=1}^{n} x_i\right) \cdot e\left(P, \sum_{i=1}^{n} (r_i h_0 + S_{ID_i})\right) \cdot e(P, nr_0 h_0 + nS_{ID_0}) \\
&= e\left(\sum_{i=1}^{n} x_i P, h\right) \cdot e\left(\sum_{i=1}^{n} r_i P, h_0\right) \cdot e\left(sP, \sum_{i=1}^{n} Q_{ID_i}\right) \cdot e(nr_0 P, h_0) \cdot e(sP, nQ_{ID_0}) \\
&= e(X, h) \cdot e(R, h_0) \cdot e\left(P_{pub}, \sum_{i=1}^{n} Q_{ID_i}\right) \cdot e(nR_0, h_0) \cdot e(P_{pub}, nQ_{ID_0}) \\
&= e\left(P_{pub}, nQ_{ID_0} + \sum_{i=1}^{n} Q_{ID_i}\right) \cdot e(nR_0 + R, h_0) \cdot e(X, h).
\end{aligned}$$

5 Future Research Directions :

A security, efficiency and scalability promising identity based bilinear pairing scheme proposed for IIoT networks has been demonstrated. However, while the IIoT becomes most relevant as applications evolve, though, there may further be improvements and refinements to make it more useful and useful. Here are five potential directions for future research:

5.1 Composed for Low Power Devices :

While this identity-based scheme is much more efficient than traditional certificate based systems, a pair of bilinear(pairing) operations is still harsh on small, battery powered IIoT devices like sensors. Other cryptographic approaches that do not require as much processing power could also be explored as future research, as could simplification of the pairing computations, making them lighter. This would facilitate deployment in an ubiquitous IIoT drive with highly resource constrained devices.

5.2 Continuous Authorisation Protocols for Energy Efficiency

Continuous data authentication is required for IIoT applications such as autonomous systems, real time monitoring, and smart city infrastructure. Even in identity based schemes, traditional signature verification can consume a lot of energy. Research into energy efficient authentication protocols requiring less pairings or using ephemeral keys and cached credentials could enable continuous authentication with low energy expenditure, keeping battery life in remote and mobile IIoT.

5.3 Enhancements with Privacy Preservation

Identity based cryptography directly links public key to device identity, raising privacy concern as this is applied to sensitive applications. Future research could develop privacy enhancing techniques for identity based schemes including pseudonyms or ways to hide device identity to allow authenticity. Such protections would protect device and user privacy without compromising the data that was exchanged.

5.4 Dynamic IIoT Networks

The IIoT networks are dynamic with devices frequently joining or leaving. Future research could be to make the scheme flexible to these changes; easy key management, delegation and revocation. Such real world applications as smart factories or autonomous vehicles would require a dynamic model since devices connect, disconnect or move tasks continuously.

5.5 Real World Testing and Case Writing

This scheme is implemented in real world IIoT cases, i.e. smart cities, healthcare and industrial automation, which can yield the firsthand performance and applicability experience. Future studies may also perform pilot projects or simulations to evaluate the scheme in practical scenarios with a view to modifying it to improve it according to real usage patterns and challenges.