REVIEW ARTICLE

Transforming Industry 4.0 Security: Analysis of ABE and ABA Technologies

Jibran Saleem[1], **Umar Raza**[1,*] **and William Holderbaum**[1,*]

[1] Manchester Metropolitan University, Manchester, United Kingdom

Abstract

The increasing deployment of intelligent cyber-physical systems (CPS), autonomous devices, and IoT infrastructures in Industry 4.0 has introduced complex and dynamic security challenges that static, identity-based mechanisms are no longer sufficient to address. Intelligent industrial environments demand security frameworks capable of fine-grained, context-aware, and adaptive access control that can operate at scale across heterogeneous networked systems. In response to this need, Attribute-Based Encryption (ABE) and Attribute-Based Authentication (ABA) have emerged as essential building blocks for intelligent security architectures, enabling policy-driven data protection and authentication that are inherently aligned with the dynamic, attribute-rich nature of Industry 4.0 systems. This paper presents a structured review of ABE and ABA schemes, analysing key variants including KP-ABE, CP-ABE, and Decentralised ABE with respect to security, computational efficiency, and suitability for AI-augmented access control in Industry 4.0. Real-world deployments and future research directions, including AI-driven dynamic policy adaptation and energy-efficient schemes for intelligent edge devices, are also examined. The findings advance the understanding of ABE and ABA as core intelligent security control components, supporting the design of robust and autonomously adaptive security systems for next-generation industrial environments.

Keywords: intelligent cyber-physical systems, machine learning, industry 4.0, cybersecurity, cloud computing, ABA, ABE.

1 Introduction

The emergence of Industry 4.0 has fundamentally transformed industrial operations through the integration of intelligent cyber-physical systems (CPS), autonomous robotics, Internet of Things (IoT) devices, and AI-driven decision-making infrastructures. These technologies enable unprecedented levels of automation and connectivity across manufacturing, logistics, and critical infrastructure. However, this interconnectedness also introduces significant security challenges: the vast number of heterogeneous devices, dynamic operational contexts, and the sensitivity of industrial data collectively demand security mechanisms that are not only robust but also intelligent, adaptive, and capable of fine-grained

Academic Editor:
Quanmin Zhu

Submitted: 19 September 2024
Accepted: 22 September 2024
Published: 21 October 2024

Vol. 1, **No.** 3, 2024.
10.62762/TIS.2024.993235

***Corresponding authors:**
✉ Umar Raza
u.raza@mmu.ac.uk
✉ William Holderbaum
w.holderbaum@mmu.ac.uk

Citation
Saleem, J., Raza, U., & Holderbaum, W. (2024). Transforming Industry 4.0 Security: Analysis of ABE and ABA Technologies. *ICCK Transactions on Intelligent Systematics*, 1(3), 127–144.

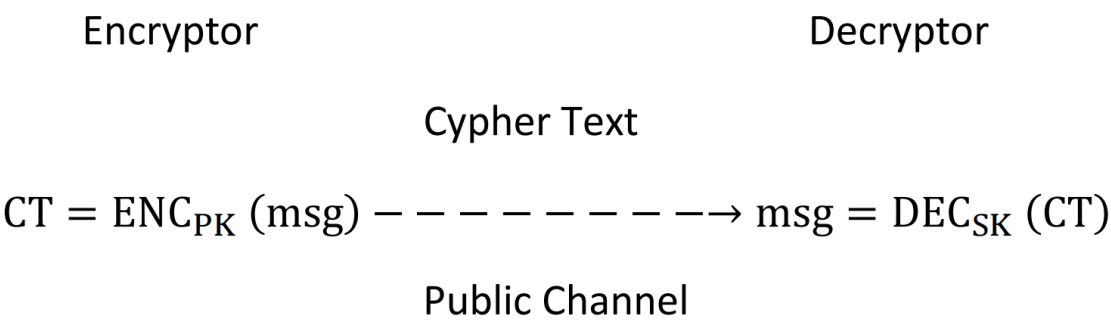

Figure 1. The equation above illustrates the concept of public key cryptology where messages can be encrypted using public key and then decrypted using corresponding private key.

control [1].

Additionally, extended data retention and accessibility from any platform are made possible by cloud technologies. According to the large quantity of study that has been done [2], cloud technology has created a number of opportunities for varied applications to flourish across all disciplines during the last ten years. Cloud solutions must guarantee dependability and strong security because there is a big volume of sensitive and important data being kept in the clouds. Several industries in Industry 4.0 are switching from traditional database management structures to open-source cloud architectures as a result of the clear advantages of cloud computing. The protection of privacy and security for the enormous amounts of data that Industry 4.0 systems produce and handle is essential during this shift.

Numerous researches have been undertaken in recent years to investigate ways to reduce privacy threats utilizing Attribute-Based Encryption (ABE), in recognition of the significance of this technology [3, 4]. Integrity maintenance and granular access control, which are essential to any framework giving privacy and security first priority, are the major reasons for integrating this public key framework, i.e., ABE, with the exchange of sensitive data in Industry 4.0. Figure 1 illustrates the core mechanism of public-key cryptology, which underpins ABE by allowing messages to be securely encrypted using a public key and decrypted only by the holder of the corresponding private key. This ensures robust encryption during data exchanges and strengthens privacy protection.

Traditional security approaches based on static credentials or role-based access control are increasingly inadequate in such environments. Intelligent industrial systems require authentication and data protection frameworks that can respond dynamically to contextual changes — such as shifts in device status, user location, or operational mode — without compromising system performance or scalability [7, 8]. This need has driven growing interest in Attribute-Based Encryption (ABE) and Attribute-Based Authentication (ABA) as foundational components of intelligent security architectures in Industry 4.0.

In addition to ABE, Attribute-Based Authentication (ABA), a complementary strategy, increases the security of data exchange in Industry 4.0 by enabling safe user authentication based on attributes. In order to address the problems of reliability and practicality in cloud computing, ABA is particularly important in guaranteeing that only authorized users can access sensitive data, and can be further combined with attribute-based signature schemes to provide non-repudiation alongside authentication [9].

Despite the importance of ABE and ABA in establishing fine-grained privacy and access control in data sharing, there aren't enough appropriate literature reviews outlining earlier achievements and ongoing trends in a well-established systematic study. Hence, within the framework of Industry 4.0 services, this paper endeavours to bridge that void by conducting a detailed analysis of attribute based encryption.

2 Methodology

The goal of this research is to thoroughly assess the effectiveness of different ABE and ABA systems in various industrial settings and to identify possible future areas of research in this field, which will create opportunities for advanced uses and research in industry 4.0.

Therefore, to prepare this paper, we employed hybrid methodology, combining qualitative and quantitative research approaches to obtain a thorough

comprehension of the topic.

The methodology relies heavily on an in-depth examination of a wide range of academic journals, conference proceedings, technical reports, and industrial publications, which constitutes a fundamental part of the research process. This review highlights the utilization of resources such as IEEE Xplore and Google Scholar to collect relevant studies and articles.

Each database was searched using keyword combination and subject heading concerning attribute based encryption and authentication in industry 4.0 as well as other industries to established current methods being used in this area of research. The Figure 2 represent results of different combination of ABE & ABA keyword searches we conducted to identify largest, most recent and relevant studies for this research.

3 Attribute-Based Authentication in Intelligent Systems

Attribute-Based Authentication (ABA) identifies and verifies users or devices based on descriptive properties rather than conventional credentials such as usernames and passwords. This paradigm offers a flexible and precise access control mechanism that is particularly well-suited to the distributed, heterogeneous, and dynamic environments characteristic of intelligent industrial systems [10]. In Industry 4.0, where autonomous machines, IoT sensors, and human operators continuously interact within shared cyber-physical infrastructures, ABA provides the contextual awareness and adaptability that static credential-based approaches fundamentally lack.

Three interconnected concepts underpin the ABA framework as applied to intelligent systems:

1. **Attribute-Based Access Control (ABAC)** governs access decisions by evaluating attributes associated with the subject (user or device), the object (resource), and the operational environment. In intelligent industrial contexts, environmental attributes such as machine state, network condition, or production phase can be derived directly from real-time sensor data, enabling access policies that respond dynamically to the operational status of a cyber-physical system.
2. **Attribute-Based Encryption (ABE)** embeds access control logic within the cryptographic structure itself, linking ciphertext or private keys to attribute-based policies [5]. This tight coupling between encryption and access policy makes ABE a natural fit for intelligent systems, where data confidentiality must be maintained across distributed nodes — including edge devices, cloud servers, and autonomous controllers — without relying on a centralised trust authority. Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE) represent the two principal variants, each offering distinct trade-offs in terms of policy flexibility and control delegation.
3. **Attribute-Based Signatures (ABS)** allow a signer to authenticate a message on behalf of any group of users satisfying a specified attribute policy, without revealing individual identity [6]. In autonomous industrial environments, ABS enables privacy-preserving verification of machine or operator actions — a capability increasingly important as intelligent systems are required to log and audit decisions made by automated agents.

Together, these components establish a layered intelligent security framework. ABA first authenticates an entity based on its attributes; ABAC then enforces access policies derived from those attributes; ABE ensures that data remains protected throughout transmission and storage; and ABS provides verifiable, privacy-preserving accountability for actions performed within the system, an integrated model demonstrated in deployed privacy-preserving attribute-based authentication systems for sensitive domains such as e-health networks [11]. This integrated model is particularly valuable in decentralised intelligent environments where traditional perimeter-based security is insufficient, and where security decisions must be made autonomously at the device or edge level.

3.1 From RBAC to Intelligent Attribute-Based Control

The evolution from Role-Based Access Control (RBAC) to ABA reflects the growing complexity of intelligent industrial environments and the limitations of rigid, identity-centric security models. RBAC introduced a significant improvement over individual identity management by organising access permissions around organisational roles [12]. Under RBAC, a user's access rights are determined by their assigned role, providing a manageable and auditable structure suitable for

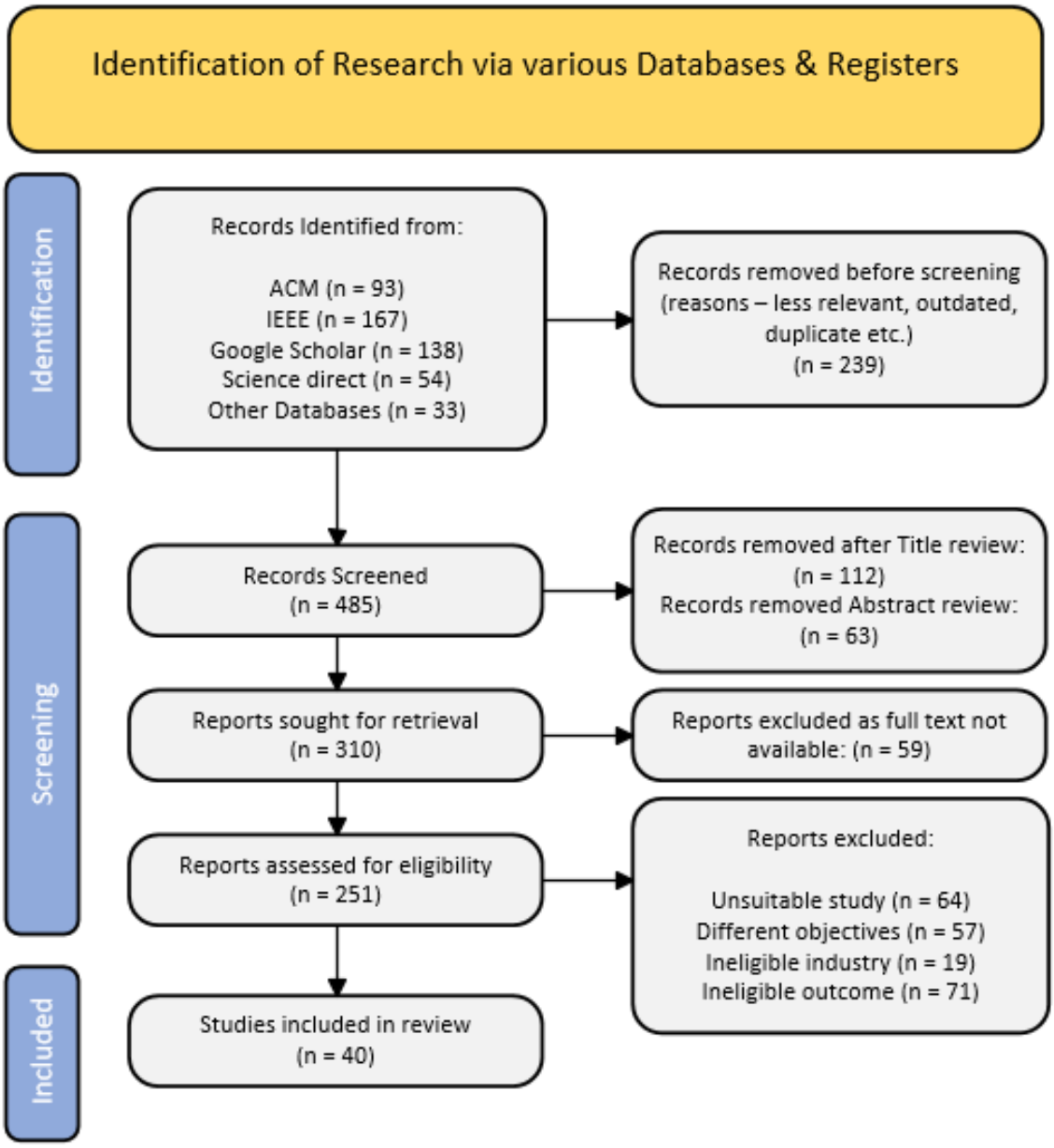

Figure 2. Database search methodology.

relatively stable organisational hierarchies.

However, as industrial systems evolved toward greater automation and connectivity, the static nature of RBAC became increasingly inadequate. Intelligent systems operating within Industry 4.0 environments require access decisions that account for a broad range of contextual variables — including device type, geographic location, network security status, and real-time operational conditions. Attribute-based authentication systems, such as those developed for mobile health networks, address precisely this need by driving access decisions from rich contextual attributes rather than fixed role assignments [13]. The inability of RBAC to accommodate such dynamic factors represents a fundamental architectural limitation in the context of intelligent cyber-physical systems.

ABA addresses this limitation by replacing discrete roles with rich, multidimensional attribute sets that can encode both stable characteristics and real-time contextual information. This attribute-driven paradigm extends naturally to cryptographic operations: attribute-based signatures, for instance, allow actions to be authenticated on behalf of any principal satisfying a given attribute policy, further decoupling identity from access rights [14]. This shift is directly aligned with the requirements of intelligent systems, where access control must function as a dynamic, data-driven process rather than a static

policy lookup.

Static attributes — such as organisational role, security clearance level, or device certification status — provide a stable foundation for access policy definition, analogous to roles in RBAC but with greater granularity.

Dynamic attributes introduce the critical intelligence dimension: these properties are derived from real-time data sources, including IoT sensor streams, location services, and system monitoring outputs [15]. In a CPS environment, for example, a robotic assembly unit may be granted write access to a production database only when its operational status attribute confirms it is within a calibrated tolerance range — a decision that can be evaluated and enforced autonomously without human intervention.

This capacity for automated, context-sensitive access arbitration positions ABA as a core mechanism for intelligent access control in Industry 4.0, enabling security systems to adapt continuously to the evolving state of the operational environment [16]. Figure 3 illustrates representative static and dynamic attributes used to verify the eligibility of both human operators and autonomous machines within ABA-governed systems.

3.2 ABA in Industry 4.0 Intelligent Architectures

Industry 4.0 represents a convergence of physical production systems with intelligent digital technologies, including IoT, artificial intelligence, cyber-physical systems, and cloud computing. This convergence introduces security requirements that are fundamentally different from those of traditional enterprise IT: access control must operate across heterogeneous device ecosystems, support autonomous decision-making, and remain effective under the highly dynamic operational conditions of smart manufacturing environments.

ABA is particularly well-positioned to meet these requirements. Unlike conventional authentication methods that rely on a single static factor, ABA evaluates multiple attributes simultaneously — including biometric indicators, behavioural patterns, device characteristics, and contextual signals such as location and time [17]. This multi-dimensional evaluation enables a level of authentication granularity that aligns naturally with the complexity of intelligent industrial architectures.

Furthermore, the integration of machine learning with ABA significantly enhances its effectiveness in Industry 4.0 settings. ML models can analyse historical access patterns, detect behavioural anomalies, and refine attribute-based policies dynamically — transforming ABA from a rule-based mechanism into an adaptive intelligent control component. This capability is especially valuable in environments where the volume and velocity of access events exceed the capacity of manual policy management, and where security responses must be both rapid and contextually informed.

3.3 Applications of ABA in Intelligent Industrial Systems

The flexibility and contextual awareness of ABA make it applicable across a broad range of intelligent systems domains within Industry 4.0.

In *intelligent cloud manufacturing*, ABA governs access to shared production resources and sensitive process data. Rather than assigning explicit permissions to individual users, system owners define attribute-based policies — for example, restricting access to process parameters to engineers affiliated with a specific production line and operating from approved network nodes [18]. This approach scales naturally with the dynamic workforce and multi-tenant architectures typical of cloud-integrated manufacturing platforms.

Within *smart factory environments*, ABA controls access to high-value production systems and proprietary process information. Access decisions are executed automatically based on verified operator attributes, eliminating manual authorisation bottlenecks and reducing the risk of privilege misuse in time-critical production contexts [19].

In *IoT-enabled cyber-physical systems*, ABA governs inter-device communication and service access based on device-level attributes such as firmware version, manufacturer certification, and operational health status [20]. This enables intelligent systems to autonomously exclude uncertified or compromised devices from sensitive data exchanges — a critical capability for maintaining the integrity of industrial control networks.

Digital Rights Management (*DRM*) systems in industrial and media contexts benefit from ABA's ability to enforce nuanced, attribute-driven access policies across geographically distributed user populations [21]. Similarly, *e-participation and public-sector platforms* can leverage ABA to deliver privacy-preserving, attribute-verified services — as

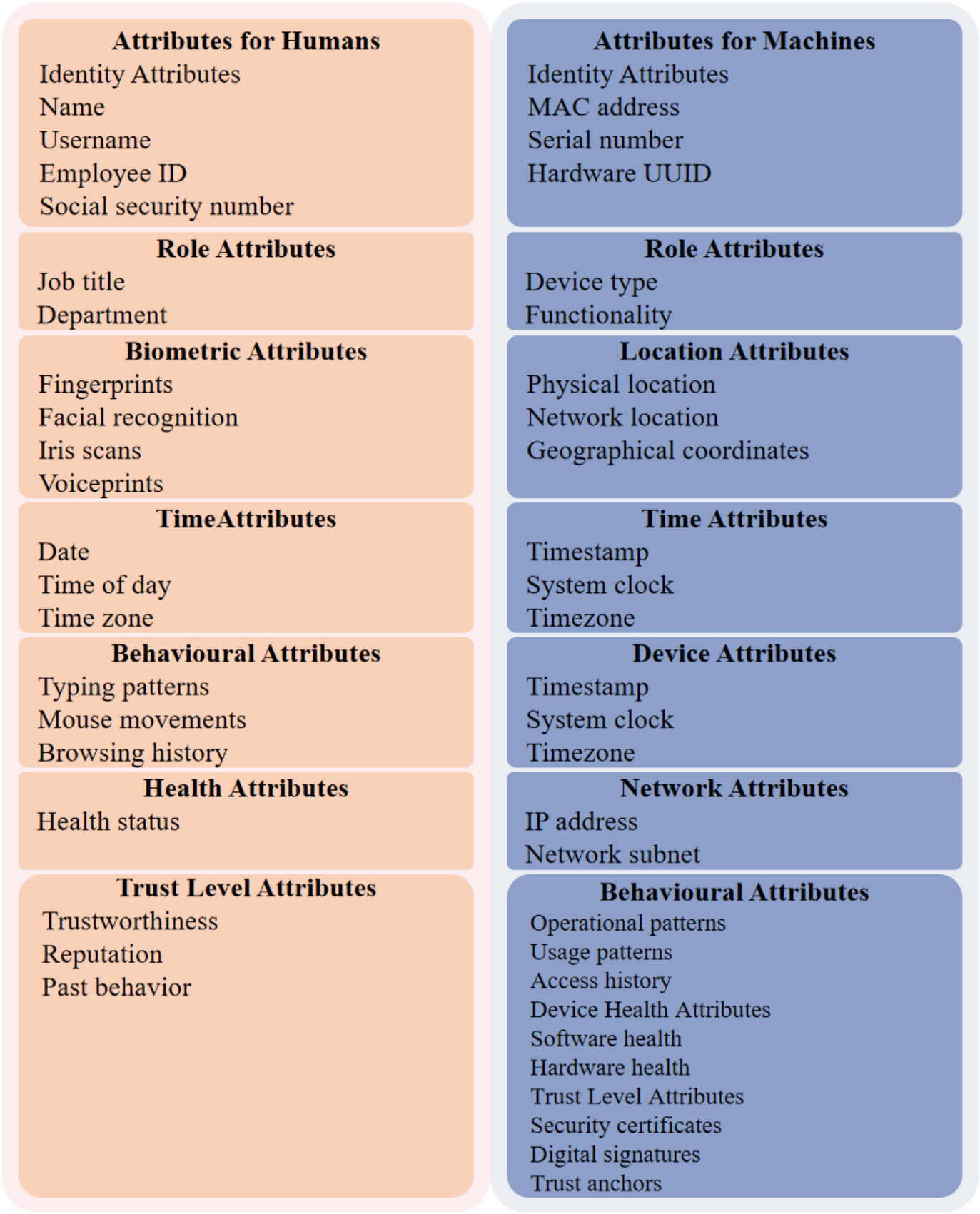

Figure 3. Static and dynamic ABA attributes used to verify eligibility of human operators and autonomous devices in intelligent Industry 4.0 systems.

demonstrated in a higher-education course-evaluation deployment built on attribute-based credentials — with access rights reflecting users' verified status or entitlement [23]. Attribute-based encryption has similarly been applied in defence and military networks to enforce fine-grained, policy-driven access control over classified data [22].

While ABA offers substantial advantages in terms of flexibility, scalability, and privacy preservation, its deployment in intelligent systems also introduces specific engineering challenges. Attribute management complexity increases with system scale, and the correctness of access decisions depends critically on the reliability of attribute sources — particularly when dynamic attributes are derived from potentially noisy or adversarially influenced sensor data [24, 25]. Addressing these challenges through ML-assisted attribute validation and anomaly detection represents a productive direction for advancing intelligent ABA systems in Industry 4.0.

4 Case Studies

This section examines various case studies on the implementation of attribute-based authentication (ABA) within the context of Industry 4.0. Drawing from examples published in the Journals, this section explores how different institutions transitioned to Industry 4.0 principles and improved security measures by adopting an attribute-based authentication and access models.

These case studies highlight the benefits of ABA, including enhanced security, flexibility, scalability, improved authentication, and streamlined access management and serves as a compelling example of how ABA can effectively address the unique challenges posed by modern manufacturing environments.

4.1 HSBC's SecureBanking ABAC Protocol

HSBC, a global banking and financial services institution, has adopted a SecureBanking system based on attribute-based access control (ABAC) to oversee and regulate access to its confidential data and systems.

The SecureBanking ABAC system is specifically developed to offer access control to a wide range of resources within the enterprise, including client data, financial records, investment portfolios, and banking applications. It utilizes characteristics linked to persons, resources, and environmental factors to establish and implement access control policies. HSBC users are categorized according to their responsibilities, departments, locations, and other pertinent factors. Attributes are assigned to resources, such as client data and banking applications, based on their sensitivity levels, data classifications, and functional domains. Additionally, environmental factors such as the user's geographical location, type of device being used, network circumstances, and operating settings are also taken into account.

Access control policies are established by utilizing logical combinations of user attributes, resource attributes, and environmental attributes. As an illustration, a policy could provide bankers and loan officers at the customer's designated branch location with the ability to both read and write customer financial records. However, other authorized personnel would only have the ability to read these records in certain operational situations, such as an agent processing a loan application for the customer. The adoption of SecureBanking ABAC at HSBC yielded numerous advantages, such as enhanced data security and privacy, precise access control, heightened operational efficiency, and simplified adherence to financial regulations and industry standards.

By implementing Attribute-Based Access Control (ABAC), HSBC was able to guarantee that only authorized people with specific attributes were permitted access to sensitive customer data and financial systems. This implementation significantly improved data security and safeguarded client privacy. Additionally, it facilitated the enforcement of careful access control procedures, granting precise control over which individuals can access particular resources based on specified circumstances. In addition, ABAC optimized access control management throughout HSBC's worldwide banking activities, enhancing operational efficiency and minimizing administrative burden. Moreover, SecureBanking ensured adherence to diverse financial legislation and industry standards, including the Payment Card Industry Data Security Standard (PCI DSS), by implementing attribute-based access control restrictions for safeguarding sensitive data and systems.

This example showcases how HSBC, a prominent financial institution, has effectively utilized attribute-based access control (ABAC) to safeguard confidential customer data and financial systems. ABAC has enabled HSBC to implement precise access control, enhance operational efficiency, and ensure compliance with financial regulations and

industry standards. This demonstrates the practical applications and advantages of ABAC in the financial services sector.

4.2 Use of ABAC in Lockheed Martin

Lockheed Martin, an established defence manufacturing firm, has successfully used attribute-based access control (ABAC) as an effective method for ensuring safe information sharing and access management.

The SecureAccess ABAC system functions by assigning attributes to users, resources, and operational conditions. Lockheed Martin assigns attributes to its users depending on their roles, security clearance levels, organizational affiliations, and other relevant variables. Resources, such as classified information, military systems, and research data, are classified based on their sensitivity levels, data classifications, and functional domains. Moreover, the analysis includes environmental factors such as the user's geographical location, type of device being used, network circumstances, and other operating contexts.

Access control policies are established by logically merging user attributes, resource attributes, and environmental attributes. For example, a policy may provide engineers and program managers with the necessary security clearance level access to secret military system data. This access would be limited to specific programs and would only be allowed from within Lockheed Martin's secure facilities. This high level of control guarantees that access to sensitive information and essential systems is tightly restricted and given exclusively to authorized persons based on predetermined conditions.

Implementing SecureAccess Attribute-Based Access Control (ABAC) at Lockheed Martin has resulted in a multitude of advantages. The primary benefit is the enhancement of information security and compliance through the implementation of attribute-based policies. This ensures that only authorized workers with the appropriate attributes are provided access to sensitive data and vital defence systems. This strategy improves information security and guarantees compliance with several defence laws.

Furthermore, ABAC has facilitated precise access control by granting authority over individuals' access to specific resources based on particular circumstances, such as their positions, security clearances, or operational settings. This level of control reduces the likelihood of unwanted access and potential breaches of data security.

In addition, SecureAccess has enabled cooperation among Lockheed Martin's many divisions, government partners, and subcontractors, while enforcing stringent access control based on attributes. This cohesive partnership promotes the exchange of information and improves the effectiveness of activities within the defence sector.

In summary, the use of attribute-based access control at Lockheed Martin demonstrates a thorough and efficient strategy for safeguarding confidential information and vital defence equipment. Lockheed Martin has achieved enhanced information security, compliance with defence standards, effective access control, safe collaboration, and reduced the likelihood of data breaches by utilizing user, resource, and environmental variables to establish access control policies. This practical illustration demonstrates the effectiveness of Attribute-Based Access Control (ABAC) in dealing with the intricate security obstacles encountered by enterprises working in sensitive domains.

4.3 Attribute based Controlled Access at Chevron

Chevron, a leading energy company, used attribute-based access control (ABAC) to effectively manage access to its crucial systems and data assets. The company's dedication to improving information security and operational efficiency is demonstrated.

The ABAC solution, known as SecureShare, is specifically built to offer secure access control to a range of resources within the organization, including exploration data, production systems, and engineering applications. The fundamental concept of SecureShare is to utilize the properties linked to users, resources, and environmental factors in order to establish and implement access control policies. This method entails attributing characteristics to users based on their responsibilities, business units, clearance levels, and other relevant variables. Furthermore, resources are allocated certain characteristics according on their levels of sensitivity, classifications of data, and functional domains. In addition, environmental factors such as the user's geographical location, type of device being used, network circumstances, and specific operational settings (such as drilling or maintenance activities) are also considered.

SecureShare utilizes logical combinations of user, resource, and environmental factors to establish access control rules. This allows for precise control over

which users can access certain resources under specific conditions. As an example, a policy could provide geologists and engineers working on certain projects with the ability to both read and write exploration data, while allowing other authorized people to only have read access during ongoing drilling activities. Implementing access control policies at such a detailed level improves information security by allowing only authorized workers with specific attributes to access sensitive data and vital systems. This measure helps safeguard proprietary data.

The deployment of SecureShare Attribute-Based Access Control (ABAC) at Chevron has resulted in numerous advantages. Firstly, it has enhanced information security by implementing attribute-based controls, which guarantee that only authorized workers are permitted access to sensitive data and essential systems. Furthermore, ABAC has facilitated the enforcement of detailed access control policies, enabling precise regulation of resource access based on specified criteria, such as user roles, data classifications, or operational situations. Furthermore, ABAC has optimized access control management throughout Chevron's worldwide operations, improving operational efficiency and minimizing administrative burdens. SecureShare has successfully enabled secure sharing and collaboration of information among Chevron's many business units, partners, and contractors. This has been achieved by implementing strict access control measures based on specific attributes.

This example showcases how Chevron effectively implemented attribute-based access control to safeguard sensitive data and critical systems. This approach enables precise access control, enhances operational efficiency, and promotes secure information sharing and collaboration across Chevron's worldwide operations.

4.4 Google's Secure Resource Access System – Zanzibar

Google, a renowned technology company, has incorporated attribute-based access control (ABAC) into its enterprise security architecture.

Google utilizes the ABAC system, named Zanzibar, to implement precise access control for different resources within the organization, such as data repositories, applications and services. Like in the examples provided above, Zanzibar's fundamental premise is to use the characteristics linked to users, resources, and environmental factors in order to establish and enforce access control regulations. This method entails attributing characteristics to users based on their responsibilities, organizational units, job activities, and other applicable variables. Similarly, attributes are assigned to resources based on their sensitivity levels, data classifications, and function. Furthermore, environmental factors such as the user's geographical location, type of device used, network conditions, and time of access are also considered.

Zanzibar employs logical combinations of user, resource, and environmental factors to build access control rules. This allows for precise control over which individuals can access specific resources based on specified criteria. As an example, a policy may provide permission for users in the "Data Analyst" job, who are working on a specific project, to have read access to a sensitive data store. This access would only be allowed while they are accessing the resource from within Google's corporate network and during business hours. The high level of detail in access control policies improves data security by guaranteeing that only authorized workers with specific attributes can access sensitive data and resources. This helps safeguard proprietary information.

Implementing Zanzibar Attribute-Based Access Control (ABAC) at Google has resulted in several significant advantages. Firstly, it has enhanced data security by implementing attribute-based controls, which guarantee that only authorized workers are permitted access to sensitive data and resources. Furthermore, ABAC has facilitated the enforcement of detailed access control policies, enabling precise regulation of individuals' access to specific resources based on specific circumstances, such as their jobs, data classifications, or environmental conditions. Furthermore, ABAC has offered enhanced versatility, enabling Google to adjust to evolving operational needs and dynamic surroundings by adjusting attribute-based regulations without making changes to the fundamental infrastructure or apps. Zanzibar has implemented a single platform to effectively manage and enforce access control restrictions across different Google services and applications. This has resulted in reduced administrative burden and enhanced uniformity.

This case study illustrates how Google effectively employed attribute-based access control to safeguard sensitive data and resources, facilitate precise access

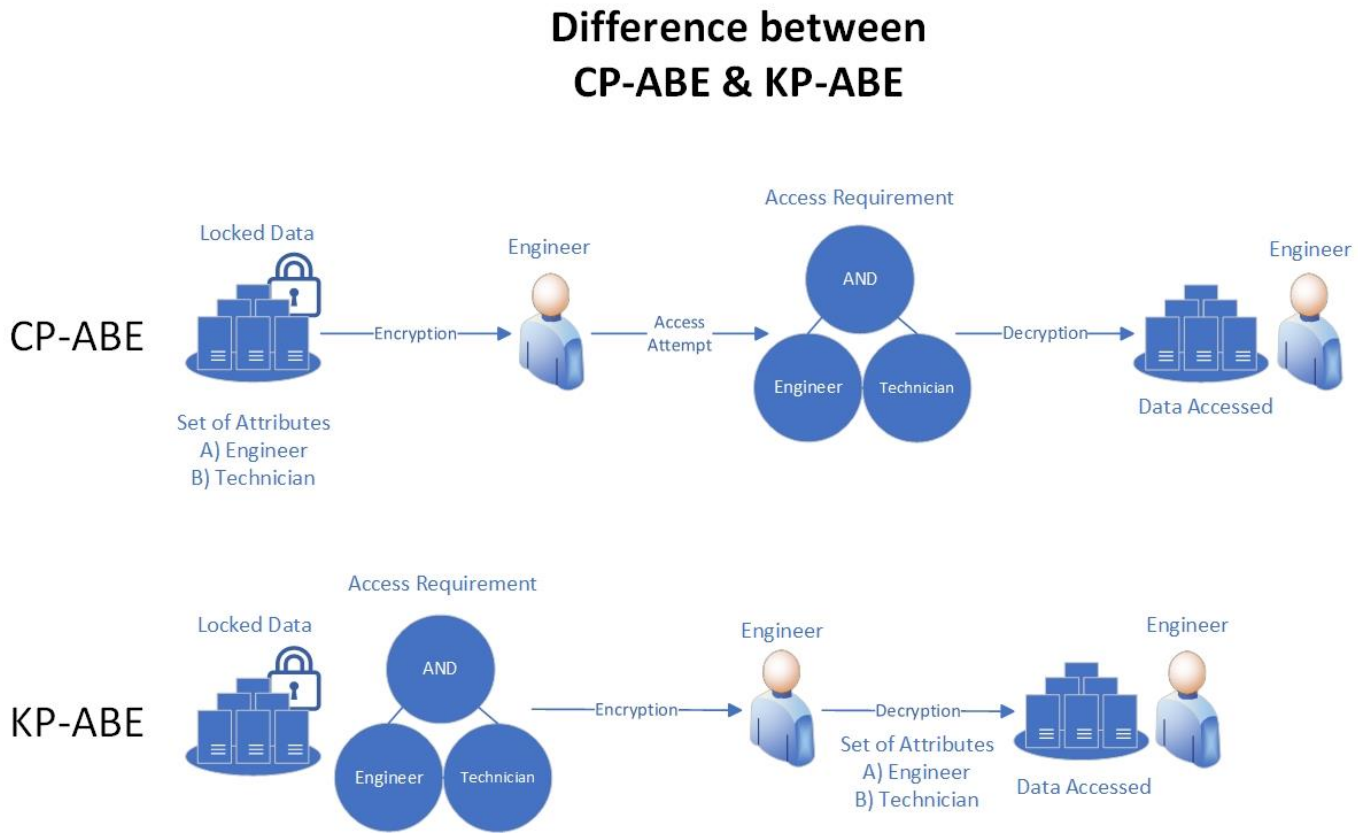

Figure 4. Distinction between two main ABE Schemes.

control, and offer adaptability in response to evolving operational needs. Additionally, this approach allowed for centralized policy management throughout their organization.

5 Key Policy (KP-ABE) & Ciphertext Policy (CP-ABE)

The two most significant variants of ABE are Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE).

The KP-ABE encryption system involves the integration of the access policy into the private key of the user, while the attributes are linked to the ciphertext. In the context of Ciphertext-Policy Attribute-Based Encryption (CP-ABE), a specific ciphertext is linked to an access structure. In the context of Key-Policy Attribute Based Encryption (KP-ABE), an individual's private key is linked to an access structure, typically represented as a tree structure. This access structure specifies the characteristics that are necessary for successfully decrypting a given ciphertext.

In KP-ABE, the ciphertext is generated over a collection of descriptive attributes, while the access policy is embedded within the user's private key; decryption succeeds only when the attributes labelling the ciphertext satisfy the access structure encoded in that key [26, 28]. In CP-ABE, by contrast, a specific ciphertext is linked to an access structure, and decryption is possible only if the attributes associated with the user's private key meet the requirements of the access structure embedded in the ciphertext [27].

Figure 4 illustrates the distinction between two primary schemes in Attribute-Based Encryption (ABE): Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE). In KP-ABE, the encryption process links a set of attributes to the data, while the access policy is embedded within the user's private key. This scheme allows decryption only if the user's private key satisfies the policy linked to the encrypted attributes. Conversely, CP-ABE operates by embedding the access policy in the ciphertext itself, granting decryption rights to users whose attributes, as defined by their private key, match the policy outlined in the ciphertext. This diagram highlights the key structural differences between these two cryptographic models and demonstrates their respective approaches to access control and encryption.

5.1 Comparison between KP-ABE & CP-ABE

The CP-ABE scheme has a higher level of efficiency in comparison to the KP-ABE scheme. The CP-ABE mechanism is deemed more suitable for the data sharing system due to its ability to empower data owners with control over access policy decisions. One limitation of Key Policy Attribute-Based Encryption (KP-ABE) is the lack of control over the selection of entities authorised to decrypt the encrypted material [29]. The system has the capability to facilitate access control in real-world settings. Furthermore, the private key belonging to the user is incorporated into the scheme as a collection of attributes. Consequently, the user can only utilise this specific set of attributes to fulfil the access structure required for accessing the encrypted data. However, the CP ABE system still has several drawbacks. The current CP-ABE schemes have limitations that prevent them from fully meeting the access control needs of enterprises, particularly in terms of flexibility and efficiency. The CP-ABE scheme exhibits certain limitations with regards to the specification of policies and the management of user attributes. In a CP-ABE (Ciphertext-Policy Attribute-Based Encryption) system, the decryption keys are designed to exclusively accommodate user characteristics that are logically structured as a unified set. Consequently, users are restricted to employing all conceivable combinations of attributes inside a single set, as specified in their keys, in order to fulfil the required policies [30].

5.2 List of Successful ABE Implementations

Figure 5 presents the evolutionary timeline of Attribute-Based Encryption (ABE), tracing its development from 2005 to 2024. The figure highlights key advancements and breakthroughs in ABE technology, starting with the introduction of Fuzzy Identity-Based Encryption (IBE) in 2005 by Sahai and Waters. As the timeline progresses, significant milestones such as the development of Key-Policy ABE (KP-ABE), Ciphertext-Policy ABE (CP-ABE), and enhancements in collusion resistance are depicted. The figure also captures the growing integration of ABE schemes with modern technologies like cloud computing, Internet of Things (IoT), and machine learning. By 2024, ABE has evolved into a critical component for secure, fine-grained access control across diverse industries, reflecting continuous innovation in cryptographic techniques to address emerging security challenges.

The state-of-the-art cryptographic technologies that have shown to be effective in offering secure and detailed access control to encrypted data are listed below. These schemes exemplify the cutting-edge progress in Attribute-Based Encryption, specifically focusing on crucial aspects such as security, efficiency, and adaptability.

5.2.1 Bethencourt et al.'s CP-ABE Scheme

The CP-ABE system proposed by Bethencourt, Sahai, and Waters in 2007 represents a significant milestone in the field of attribute-based encryption. The primary objective of its design was to effectively tackle the complexities associated with implementing precise access control mechanisms for encrypted data, with a special emphasis on cloud computing environments [31]. In this context, individuals or entities with ownership of data have the ability to securely store encrypted data on cloud servers, thereby establishing a mechanism that restricts access just to authorised users, contingent upon their specific attributes.

A complete understanding of the CP-ABE scheme proposed by Bethencourt et al. [31] can be achieved by examining its operation method.

In the first stage, public parameters that are applicable to the entire system are created, together with a master secret key. This procedure is performed just once. During the encryption phase, data owners utilise a tree access structure or policy to encrypt their data, employing characteristics and logical gates such as AND and OR. Only users whose private key attributes fit with this access structure can decrypt the resulting ciphertext.

The authority is responsible for generating private keys for users, taking into account their distinct attributes. Decryption is the following step where persons possessing private keys make an effort to decode a certain ciphertext. The effective decryption relies on the private key qualities aligning with the access structure (policy) encoded in the ciphertext.

The security of this technique is based on the fundamental assumption of bilinear pairing. Bethencourt et al. [31] present corroborating evidence, affirming that their approach demonstrates discerning security based on this fundamental assumption. The CP-ABE technology greatly enhances the field of attribute-based encryption by prioritising access control precision and its suitability in cloud environments.

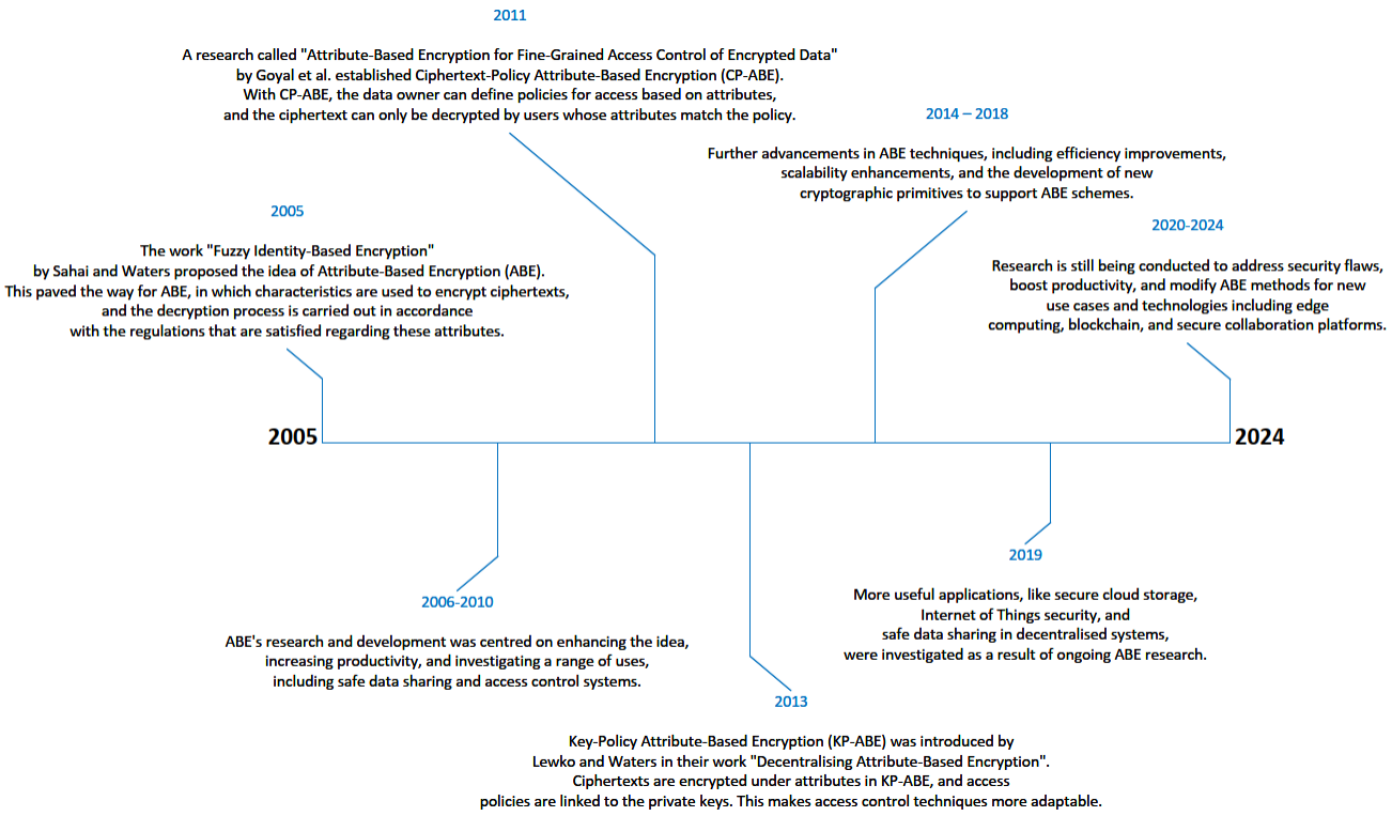

Figure 5. Evolution of Attribute-Based Encryption (ABE): A Timeline from 2005 to 2024.

5.2.2 *Improved KP-ABE Scheme*

The Key-Policy Attribute-Based Encryption (KP-ABE) scheme developed by Goyal et al. [32] is a novel cryptographic system that provides a versatile mechanism for encrypting data and controlling access. Central to this method are attributes, which are descriptive identifiers.

Access policies in KP-ABE are incorporated into the user's private keys and serve as regulations that determine the requirements for decrypting data. These regulations establish the essential characteristics required to decipher a certain set of data. During the system's setup phase, a public key is generated for encryption purposes, and a master secret key is created to generate user keys. Subsequently, users are provided with individualised private keys that are determined by their qualities. These keys encompass access policies that precisely define the circumstances in which they can be utilised to decrypt data [32].

The encryption in KP-ABE is based on attributes rather than being customised to individual users. The data is encrypted using a certain set of properties, and only individuals possessing private keys that align with these attributes are able to decrypt the data. The decryption process relies on the congruence between a user's private key policy and the qualities employed in encrypting the material.

The KP-ABE scheme has various benefits, such as precise access control, the ability to handle large scale systems, and adaptability, which proves especially valuable in situations where managing individual keys or permissions is not feasible. It can also be adapted to remove key-escrow dependence, supporting standalone authentication for resource-constrained Internet of Things devices, where access must be regulated by attribute without reliance on a fully trusted key authority [33].

Nevertheless, the method encounters obstacles, such as the arduousness of retracting access after a key is granted and the heightened intricacy and diminished effectiveness as the quantity of qualities and policies expands. Notwithstanding these difficulties, the KP-ABE proposed by Goyal et al. [32] continues to be a powerful tool in contemporary cryptography, offering a means to protect data while also providing comprehensive and adaptable access control.

5.2.3 *Waters' Expressive CP-ABE Scheme*

The Ciphertext-Policy Attribute-Based Encryption scheme proposed by Waters represents a significant advancement in expressive, efficient, and provably secure ABE constructions [34]. Building upon earlier

CP-ABE work, this scheme was designed to support expressive access policies — including arbitrary monotone Boolean formulae — while achieving full security under standard assumptions, addressing limitations of prior constructions that attained only selective security.

During the setup phase, public parameters and a master secret key are generated by a trusted authority. Data owners encrypt sensitive data under an access policy expressed as a Boolean formula over attributes; the resulting ciphertext embeds both the encrypted data and the access policy. The authority issues users with private keys tied to their attribute sets. Decryption succeeds if and only if the user's attributes satisfy the access policy embedded in the ciphertext.

A key contribution of this scheme is the achievement of full (adaptive) security — meaning security holds even against adversaries who choose their challenge ciphertext after seeing the system's public parameters and adaptively querying for private keys. This is a strictly stronger guarantee than the selective security of earlier constructions, where the adversary must commit to a target ciphertext before seeing the public parameters.

Bilinear pairings on elliptic curve groups underpin the cryptographic operations of this scheme, enabling the verification of attribute-policy relationships without revealing the underlying data. The result is a construction that is simultaneously expressive, practically efficient, and rigorously provable — qualities that make it a widely referenced benchmark in the ABE literature. The security trade-offs and efficiency characteristics of this scheme relative to other CP-ABE and KP-ABE constructions are documented in comparative surveys of attribute-based encryption [35].

5.2.4 *Lewko-Waters Decentralised Attribute-Based Encryption*

The decentralised Attribute-Based Encryption scheme proposed by Lewko and Waters eliminates the single-authority trust bottleneck inherent in conventional ABE constructions [36]. In this scheme, no single central authority holds the complete master secret key; instead, multiple independent authorities each govern a distinct subset of attributes and issue the corresponding private key components directly to users. A user obtains key material from every authority whose attributes they possess, and decryption succeeds only when the combined key material satisfies the access policy embedded in the ciphertext.

A central security property of this construction is full collusion resistance across authorities: even if users served by different authorities pool their key material, they cannot jointly decrypt a ciphertext for which none of them individually holds sufficient attributes. This property is achieved without any inter-authority communication during key issuance, which significantly improves scalability and fault tolerance. The realisation of these collusion-resistant properties has been surveyed across multi-authority and decentralised ABE constructions, in which preventing colluding users — possibly served by different authorities — from pooling their keys is treated as a central security requirement [35].

Although decentralisation substantially improves resilience and removes single points of failure, it introduces coordination complexity: the correctness and security of the overall system depend on the integrity of each participating authority and the reliability of the channels through which users obtain their distributed key components. The selection of this scheme is therefore most appropriate for large-scale distributed environments — such as cloud or IoT deployments — where centralised trust is operationally infeasible.

5.2.5 *Decentralized Attribute-Based Encryption (DABE)*

Decentralized Attribute-Based Encryption (DABE) expands upon the conventional Attribute-Based Encryption framework by dispersing the responsibility and control of cryptographic keys among several groups or authorities. Within this decentralized architecture, there is no singular central authority that possesses control over the entirety of the key management process. This arrangement provides enhanced scalability, flexibility, and resilience. The initial configuration entails the choosing of cryptographic parameters in a worldwide setup phase [37].

However, in contrast to standard Attribute-Based Encryption (ABE), this configuration is decentralized across numerous governing bodies. Every decentralized authority is tasked with the role of overseeing a particular subset of qualities or policies. Users are granted traits by the appropriate authority to depict their distinctive qualities. When a user wants to retrieve encrypted material, they get private keys from the appropriate authorities according to their attribute domains [38]. Data owners employ encryption techniques to safeguard

sensitive information, wherein they define an access policy. The final ciphertext incorporates this access policy.

In order to decipher the encrypted message, an individual must obtain the private keys from all pertinent authorities whose qualities are necessary to fulfil the access policy. The decentralization of Attribute-Based Encryption (ABE) offers benefits such as increased scalability, enhanced resilience against individual authority failures, and more flexibility in attribute policy management. Nevertheless, the decentralized technique introduces intricacy, necessitating meticulous deliberation of safe communication and collaboration across authorities to guarantee the system's comprehensive security and efficacy. The effectiveness and safety of a decentralized Attribute-Based Encryption (ABE) system depend on the specific needs of the application, with particular emphasis on the trust model and communication routes being essential for a successful implementation.

5.2.6 Comparison of Schemes

Analysis of different Attribute-Based Encryption (ABE) schemes showcases distinct characteristics and scenarios where they might be applied, emphasising the many methodologies in the realm of cryptographic security.

- The Decentralised Attribute-Based Encryption (DABE) is characterised by its decentralised architecture, which enables different authorities to autonomously issue attributes. The decentralisation of control is especially advantageous in extensive dispersed systems, such as cloud computing environments, where centralised control is not feasible or unwanted.
- The Lewko-Waters Decentralised ABE scheme eliminates the single-authority trust bottleneck by distributing key issuance across multiple independent authorities, each governing a separate attribute domain. Full collusion resistance is achieved without inter-authority communication: users who pool key material obtained from different authorities still cannot decrypt ciphertexts for which neither holds sufficient attributes individually. This makes the scheme well-suited for large-scale distributed or IoT environments where centralised trust is not feasible — an advance catalogued among the broader authentication and authorisation developments surveyed for Internet of Things environments [39].
- The Waters CP-ABE scheme [34] advances beyond earlier constructions by achieving full adaptive security under standard assumptions, while supporting expressive monotone Boolean access policies. Compared with selectively secure schemes, it provides strictly stronger security guarantees, though this comes at some additional computational cost relative to more recent optimised constructions.
- The CP-ABE scheme developed by Bethencourt et al. [31] in 2007 introduces a novel approach by incorporating the access policy into the ciphertext rather than the user's private key. This method is more conducive to user convenience, particularly in situations when the encryptor desires to exert control over data access permissions. In contrast to KP-ABE schemes, the policy in this case is stored in the ciphertext rather than the user's private key.
- The KP-ABE Scheme developed by Goyal et al. [32] in 2006 is a fundamental system in which the user's private key contains the access policy, and the data is encrypted using a group of attributes. This technique is especially appropriate for contexts where user attributes unambiguously determine their access privileges, such as in organisations with well-defined roles and responsibilities.

Every system has its own unique benefits and constraints [40]. The decentralised aspect of DABE stands in opposition to the centralised approaches employed by other schemes. The Lewko-Waters scheme prioritises the elimination of centralised trust through multi-authority key issuance, while achieving full collusion resistance across authorities. The Waters CP-ABE scheme is valuable for its combination of full adaptive security and expressive policy support, establishing a widely cited benchmark for provably secure CP-ABE constructions. CP-ABE system ensures that the encryptor's control is in line with the policy specified in the ciphertext. This is different from the user-centric policy approach used in KP-ABE schemes, such as the one proposed by Goyal et al. [32]. The selection of one of these schemes is contingent upon specific requirements, such as the desired level of security, the extent of control over data access, the degree of decentralisation, and the overall context in which the encryption system will be implemented.

6 Emerging Horizons: Future Perspectives in ABE Research in Industry 4.0 & AI

There are multiple potential avenues for future research that can enhance the fields of Attribute Based Encryption (ABE) and Attribute-Based Authentication (ABA) in Industry 4.0 and IoT settings.With the enablement of AI within these technologies, security in the aforementioned domains can be significantly augmented.

a) Hybrid Attribute-Based Encryption. An important focus should be on the advancement of hybrid Attribute-Based Encryption (ABE) systems, which would combine the advantages of several ABE methods to construct models that are more robust, effective, and adaptable. Furthermore, it is essential to tackle the scalability obstacles presented by the increasing prevalence of IoT devices. This requires the development of novel algorithms and architectures that can expand in size without sacrificing security.

b) Merging ABE and ABA with Cutting-Edge Technologies. The fusion of ABE (Attribute-Based Encryption) and ABA (Attribute-Based Authentication) with state-of-the-art technologies such as blockchain, quantum computing, and powerful machine learning algorithms offers a captivating realm for research. This has the potential to enable novel opportunities for the secure exchange of data and verification of identity. Furthermore, additional real-world applications and empirical analyses are required to gain a more comprehensive understanding of the practical obstacles and performance measurements of Attribute-Based Encryption (ABE) and Attribute-Based Access Control (ABA) in operational settings.

c) Elevating User Experience & Compliance. User experience and usability are important factors that come to the forefront. Subsequent investigations should focus on enhancing the user-friendliness of these technologies and evaluating their influence on the user experience, particularly in industrial contexts. Moreover, in light of the growing intricacy of laws in the context of Industry 4.0, it is imperative to create ABE and ABA systems that adhere to international norms and regulations.

d) Dynamic Access Control and Encryption. Artificial intelligence enhances the flexibility of accessing control and encryption configurations. By utilising Attribute-Based Access Control (ABA) and Attribute-Based Encryption (ABE), artificial intelligence (AI) analyses real-time data and user behaviours to dynamically adjust access policies and encryption configurations, thereby improving security and efficiency by customising them to specific situational requirements. AI automates the process of assigning attributes, making attribute management more efficient and lowering the likelihood of human mistakes.

e) Proactive Maintenance and Data Management. AI in Industry 4.0 facilitates predictive maintenance, which involves anticipating and scheduling equipment maintenance and updates. By integrating it with ABA (Access Based Authentication) and ABE (Attribute Based Encryption), this system can potentially guarantee that only authorised entities are able to access critical data or perform changes, thereby improving both security and operational efficiency. AI can also aid in the optimisation of data management by efficiently organising and safeguarding large databases to ensure confidentiality and convenient accessibility.

f) Advanced threat detection and response. The integration of artificial intelligence (AI) with ABA and ABE enables the prediction and analysis of potential threats in advance. Artificial intelligence, in conjunction with attribute-based authentication (ABA) and attribute-based encryption (ABE), allows for the anticipation and identification of potential security risks prior to their actualization. Automated threat responses, such as altering encryption levels or adjusting access limits, enable systems to take proactive measures in addressing recognised risks, thereby limiting the escalation of security breaches.

g) Enhancing Resilience against Attacks. Another crucial aspect involves bolstering the resilience of ABE and ABA systems against sophisticated cybersecurity threats, such as AI-driven attacks. This would guarantee the resilience of these systems against emerging threats. Moreover, the task of incorporating novel technology into preexisting legacy systems must not be disregarded. Future research should prioritise the development of compatible ABE and ABA solutions that can be effortlessly integrated with legacy technologies.

h) Energy-Efficient ABE and ABA Schemes. The development of energy-efficient Attribute-Based Encryption (ABE) and Attribute-Based Access Control (ABA) schemes is crucial due to the energy limitations of IoT devices. The objective should be to reduce power usage while upholding stringent security standards. Finally, investigating

the capabilities of decentralised Attribute-Based Encryption (ABE) systems in the Internet of Things (IoT) setting, specifically in regards to edge computing and distributed data processing, offers a compelling field for future research.

The integration of ABA and ABE with Artificial Intelligence (AI) has the potential to significantly revolutionise security, usability, efficiency and access control methods, particularly in the domains of Industry 4.0, Internet of Things (IoT), and cloud computing. Tackling these various domains would greatly enhance the progress of these schemes, guaranteeing their strength, effectiveness, and significance in the rapidly changing context of aforementioned industries. Nevertheless, it is also crucial to thoroughly analyse the intricacies, privacy issues, and the requirement for ongoing maintenance and upgrades while dealing with this revolutionary association.

7 Conclusion

This study examines Attribute-Based Encryption (ABE) and Attribute-Based Authentication (ABA) as intelligent security control mechanisms for Industry 4.0 environments, where cyber-physical systems, autonomous devices, and IoT infrastructures demand adaptive and fine-grained protection frameworks. The analysis demonstrates that ABE and ABA are not merely cryptographic constructs, but foundational components of intelligent security architectures capable of supporting autonomous access decisions across heterogeneous industrial and cloud environments.

Key ABE schemes — including KP-ABE, CP-ABE, and Decentralised ABE — have been evaluated with respect to security, computational efficiency, and compatibility with AI-augmented access control. The analysis reveals that their suitability for intelligent industrial deployment is critically determined by their capacity to handle dynamic attributes, integrate with machine learning pipelines, and operate within resource-constrained edge environments. ABA is similarly confirmed as an adaptive intelligent authentication layer, capable of incorporating real-time contextual signals — including sensor data, device state, and behavioural patterns — into automated access decisions.

The integration of machine learning with ABE and ABA represents the most significant opportunity for advancing intelligent security in Industry 4.0, enabling dynamic policy adaptation and anomaly-based threat detection that transform these mechanisms from static rule-based systems into self-adaptive intelligent control components. Continued research in this direction is essential to meet the security demands of next-generation intelligent industrial environments.

Data Availability Statement

Not applicable.

Funding

This work was supported without any funding.

Conflicts of Interest

The authors declare no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Li, J., Zhang, Y., Ning, J., Huang, X., Poh, G. S., & Wang, D. (2020). Attribute based encryption with privacy protection and accountability for CloudIoT. *IEEE Transactions on Cloud Computing, 10*(2), 762-773. [CrossRef]

[2] Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. *Journal of internet services and applications, 1*(1), 7-18. [CrossRef]

[3] Chase, M., & Chow, S. S. (2009, November). Improving privacy and security in multi-authority attribute-based encryption. In *Proceedings of the 16th ACM conference on Computer and communications security* (pp. 121-130). [CrossRef]

[4] Han, J., Susilo, W., Mu, Y., & Yan, J. (2012). Privacy-preserving decentralized key-policy attribute-based encryption. *IEEE transactions on parallel and distributed systems, 23*(11), 2150-2162. [CrossRef]

[5] Sahai, A., & Waters, B. (2005). Fuzzy identity-based encryption. In *Advances in Cryptology–EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005. Proceedings 24* (pp. 457-473). Springer Berlin Heidelberg. [CrossRef]

[6] Oberko, P. S. K., Obeng, V. H. K. S., Xiong, H., & Kumari, S. (2022). A survey on attribute-based signatures. *Journal of Systems Architecture, 124*, 102396. [CrossRef]

[7] Sebbah, A., & Kadri, B. (2020, June). A privacy and authentication scheme for IoT environments using ECC and fuzzy extractor. In *2020 International*

Conference on Intelligent Systems and Computer Vision (ISCV) (pp. 1-5). IEEE. [CrossRef]

[8] Punithavathi, P., Geetha, S., Karuppiah, M., Islam, S. H., Hassan, M. M., & Choo, K. K. R. (2019). A lightweight machine learning-based authentication framework for smart IoT devices. *Information Sciences*, 484, 255-268. [CrossRef]

[9] Li, J., Au, M. H., Susilo, W., Xie, D., & Ren, K. (2010, April). Attribute-based signature and its applications. In *Proceedings of the 5th ACM symposium on information, computer and communications security* (pp. 60-69). [CrossRef]

[10] Sucasas, V., Mantas, G., Papaioannou, M., & Rodriguez, J. (2021). Attribute-based pseudonymity for privacy-preserving authentication in cloud services. *IEEE Transactions on Cloud Computing*, 11(1), 168-184. [CrossRef]

[11] Guo, L., Zhang, C., Sun, J., & Fang, Y. (2012, June). Paas: A privacy-preserving attribute-based authentication system for ehealth networks. In *2012 IEEE 32nd International Conference on Distributed Computing Systems* (pp. 224-233). IEEE. [CrossRef]

[12] Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *Computer, 29*(2), 38-47. [CrossRef]

[13] Guo, L., Zhang, C., Sun, J., & Fang, Y. (2013). A privacy-preserving attribute-based authentication system for mobile health networks. *IEEE Transactions on Mobile Computing*, 13(9), 1927-1941. [CrossRef]

[14] Maji, H. K., Prabhakaran, M., & Rosulek, M. (2011, February). Attribute-based signatures. In *Cryptographers' track at the RSA conference* (pp. 376-392). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[15] Dzurenda, P., Casanova-Marqués, R., Malina, L., & Hajny, J. (2022, August). Real-world Deployment of Privacy-Enhancing Authentication System using Attribute-based Credentials. In *Proceedings of the 17th International Conference on Availability, Reliability and Security* (pp. 1-9). [CrossRef]

[16] Schläger, C., Priebe, T., Liewald, M., & Pernul, G. (2007). *Enabling attribute-based access control in authentication and authorisation infrastructures*. Paper presented at the 20th Bled eConference, Bled, Slovenia. https://aisel.aisnet.org/bled2007/3/

[17] García-Rodríguez, J., & Skarmeta, A. (2023). A privacy-preserving attribute-based framework for IoT identity lifecycle management. *Computer Networks*, 236, 110039. [CrossRef]

[18] Liu, Z., Yan, H., & Li, Z. (2015). Server-aided anonymous attribute-based authentication in cloud computing. *Future Generation Computer Systems*, 52, 61-66. [CrossRef]

[19] Bhatt, S., Pham, T. K., Gupta, M., Benson, J., Park, J., & Sandhu, R. (2021). Attribute-based access control for AWS internet of things and secure industries of the future. *IEEE Access*, 9, 107200-107223. [CrossRef]

[20] Yu, Y., Zhao, Y., Li, Y., Du, X., Wang, L., & Guizani, M. (2019). Blockchain-based anonymous authentication with selective revocation for smart industrial applications. *IEEE Transactions on Industrial Informatics*, 16(5), 3290-3300. [CrossRef]

[21] Huang, Q., Ma, Z., Yang, Y., Niu, X., & Fu, J. (2014). Attribute based DRM scheme with dynamic usage control in cloud computing. *China Communications*, 11(4), 50-63. [CrossRef]

[22] Prasanna, V. L., & Kumar, C. K. R. (2015). A novel cipher text policy attribute based encryption algorithm for a secure data retrieval in military networks. *Journal of Computing Technologies, 5*(1), 111–117. https://jctjournals.com/January2016/v18.pdf

[23] Liagkou, V., Metakides, G., Pyrgelis, A., Raptopoulos, C., Spirakis, P., & Stamatiou, Y. C. (2012, October). Privacy preserving course evaluations in Greek higher education institutes: an e-Participation case study with the empowerment of Attribute Based Credentials. In *Annual Privacy Forum* (pp. 140-156). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[24] Bakar, K. A. A., & Haron, G. R. (2013, June). Adaptive authentication: Issues and challenges. In *2013 World Congress on Computer and Information Technology (WCCIT)* (pp. 1-6). IEEE. [CrossRef]

[25] Servos, D., & Osborn, S. L. (2017). Current research and open problems in attribute-based access control. *ACM Computing Surveys (CSUR)*, 49(4), 1-45. [CrossRef]

[26] Rouselakis, Y., & Waters, B. (2013, November). Practical constructions and new proof methods for large universe attribute-based encryption. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security* (pp. 463-474). [CrossRef]

[27] Lai, J., Deng, R. H., & Li, Y. (2011). Fully secure cipertext-policy hiding CP-ABE. In *Information Security Practice and Experience: 7th International Conference, ISPEC 2011, Guangzhou, China, May 30–June 1, 2011. Proceedings 7* (pp. 24-39). Springer Berlin Heidelberg. [CrossRef]

[28] Touati, L., & Challal, Y. (2016, May). Collaborative kp-abe for cloud-based internet of things applications. In *2016 IEEE International Conference on Communications (ICC)* (pp. 1-7). IEEE. [CrossRef]

[29] Kim, J., Susilo, W., Guo, F., Au, M. H., & Nepal, S. (2017, April). An efficient KP-ABE with short ciphertexts in prime ordergroups under standard assumption. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security* (pp. 823-834). [CrossRef]

[30] Chen, N., Li, J., Zhang, Y., & Guo, Y. (2020). Efficient CP-ABE scheme with shared decryption in cloud storage. *IEEE Transactions on Computers*, 71(1), 175-184.

[CrossRef]

[31] Bethencourt, J., Sahai, A., & Waters, B. (2007, May). Ciphertext-policy attribute-based encryption. In *2007 IEEE symposium on security and privacy (SP'07)* (pp. 321-334). IEEE. [CrossRef]

[32] Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006, October). Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM conference on Computer and communications security* (pp. 89-98). [CrossRef]

[33] He, X., Li, L., & Peng, H. (2023). A key escrow-free KP-ABE scheme and its application in standalone authentication in IoT. *IEEE Internet of Things Journal, 11*(7), 11381-11394. [CrossRef]

[34] Waters, B. (2011, March). Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In *International workshop on public key cryptography* (pp. 53-70). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[35] Oberko, P. S. K., Obeng, V. H. K. S., & Xiong, H. (2022). A survey on multi-authority and decentralized attribute-based encryption. *Journal of Ambient Intelligence and Humanized Computing, 13*(1), 515-533. [CrossRef]

[36] Lewko, A., & Waters, B. (2011, May). Decentralizing attribute-based encryption. In *Annual international conference on the theory and applications of cryptographic techniques* (pp. 568-588). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[37] Binbusayyis, A., & Zhang, N. (2015, June). Decentralized attribute-based encryption scheme with scalable revocation for sharing data in public cloud servers. In *2015 International Conference on Cloud Technologies and Applications (CloudTech)* (pp. 1-8). IEEE. [CrossRef]

[38] Oosterhout, J. (2023). Formal Verification of Lightweight Decentralized Attribute-based Encryption (Master's thesis, University of Twente). https://purl.utwente.nl/essays/97069

[39] Trnka, M., Abdelfattah, A. S., Shrestha, A., Coffey, M., & Cerny, T. (2022). Systematic review of authentication and authorization advancements for the Internet of Things. *Sensors*, 22(4), 1361. [CrossRef]

[40] Arshad, H., Johansen, C., & Owe, O. (2022). Semantic attribute-based access control: A review on current status and future perspectives. *Journal of Systems Architecture*, 129, 102625. [CrossRef]

Jibran Saleem received the MSc in Network Security from Manchester Metropolitan University, UK in 2017. Jibran is also currently a PhD candidate. (E-mail: Jibran.saleem@stu.mmu.ac.uk)

Umar Raza received his BSc in Engineering Electronics from (DeMontfort Leicester), MSc in Electronics and Computer Based Systems Design from (Huddersfield University). He completed his PhD in the Application of Wireless Sensor Networks (WSN) to the plastics industry at the Polymer IRC Laboratory at the University of Bradford. He has worked in industry for 7 years as a Software Engineer and then moved back into academia as a Lecturer in Robotics, Networking and Computing at Staffordshire University.

He is currently working as a Senior Lecturer in Industrial IoT, Computer and Networking Technology at Manchester Metropolitan University and is the Manager/Coordinator of the Cisco Network Academy in the Department of Engineering at Manchester Metropolitan University. (E-mail: u.raza@mmu.ac.uk)

William Holderbaum received his Ph.D. degree in Automatic Control with his PhD thesis focusing on developing new methodology to design control laws for hybrid systems. He currently works at the Manchester Metropolitan University as Professor in Control Engineering.

He has been involved in research with mathematical modelling and control theory with applications mainly to health, energy, and robotics. In particular Rehabilitation Engineering, Smart Grid, Power Generation, Wireless Power Transfer, Autonomous Vehicle, Motion planning, visualisation control. Professor Holderbaum has published over 100 papers in leading journals and international conferences. (E-mail: w.holderbaum@mmu.ac.uk)