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 sharing of data and private information has been greatly improved by Industry 4.0's broad usage of cloud technologies. In their quest to improve their services, many firms have made automation and effective authentication a priority. As a result, in Industry 4.0, Attribute-Based Encryption (ABE) and Attribute-Based Authentication (ABA) have established themselves as dependable models for data sharing across cloud environments. For difficult situations like fine-grained access control and secure authentication, these models offer practical solutions. Organizations can utilize ABA to perform authentication based on user attributes, ensuring appropriate and safe access to critical data. Despite the significance of ABE and ABA within Industry 4.0 and the wide range of applications that they have, systematic and thorough studies that include all variations of these models, as well as their historical and present condition, are lacking in the literature. This paper offers a complete and organized evaluation of works on Industry 4.0 by ABE and ABA. Our study's methodology, findings, and suggested follow-up work will advance the field of ABE and ABA research and improve the safety of data sharing in Industry 4.0. Organizations working within Industry 4.0 can improve the security of their cloud-based systems by integrating attribute-based authentication mechanisms and machine learning, making sure that only vetted individuals have access to sensitive data. ABE and ABA architectures in safe data-sharing situations within Industry 4.0, as well as the potential of ABE and ABA deployment in the context of the most recent technical breakthroughs, will also be better understood by researchers and practitioners with the aid of this study.

Keywords: industry 4.0, cybersecurity, cloud computing, ABA, ABE.

1 Introduction

Machine learning, particularly in the context of authentication, is essential for improving the security of cloud-based applications. Machine learning can be used to create sophisticated authentication models that can identify and authenticate users based on their distinctive qualities, behavioural patterns, and other pertinent features using the vast amounts of data saved in the cloud. The existing Attribute Based Encryption (ABE) and Attribute-Based Authentication (ABA) systems get an additional layer of protection as a result of this [4].

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.

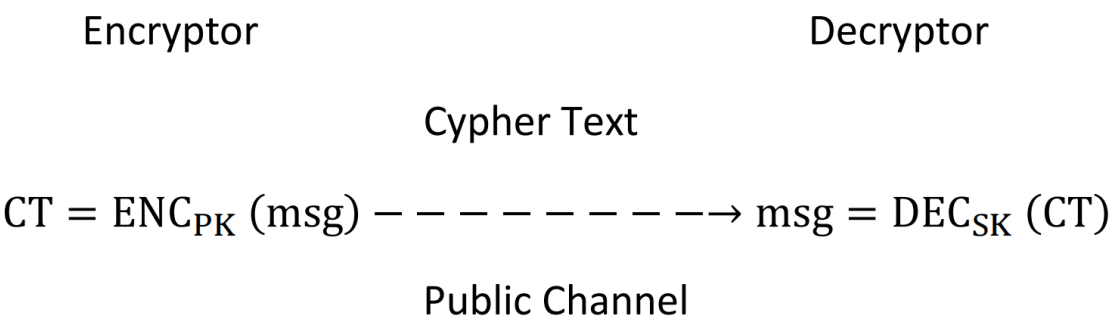

Figure 1. The equation above illustrates the concept of public key cryptology where messages can be encrypted using public key and then decrypted using corresponding private key.

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 [1], 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 [5, 6]. 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.

In terms of architectural efficiency, ABE has demonstrated important outcomes, such as collusion resistance, quicker key generations, fewer fungible public-private key pairs, and reduced polynomial time. Industry 4.0 has successfully shared data by embracing cloud computing's advantages, but it faces challenges concerning reliability, practicality, and the need for flexible, scalable, fine-grained access control [7, 8].

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 [9].

Despite the importance of ABE and ABA in establishing distinguished 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

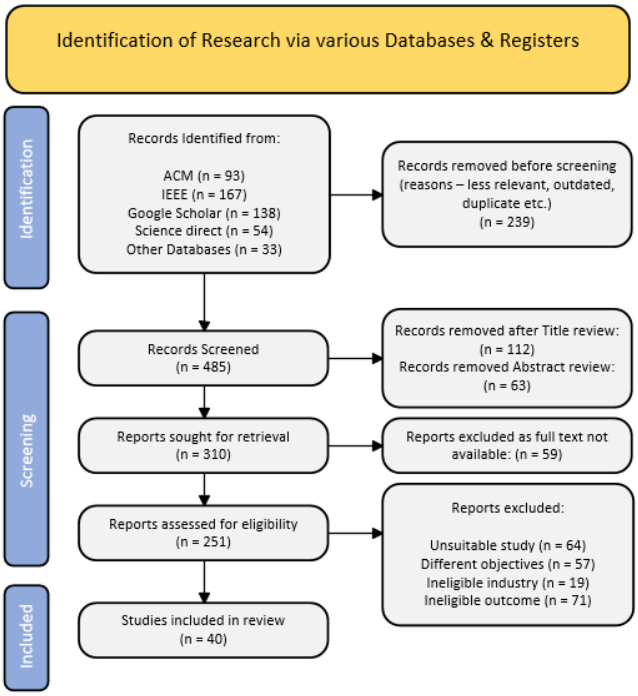

Figure 2. Database search methodology.

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

Instead of using conventional credentials like usernames and passwords, attribute-based authentication (ABA) identifies users based on their properties. More flexible and precise access control is possible with this type of authentication. When users need to be authenticated based on their attributes rather than a central authority, it is frequently employed in distributed and decentralized systems [10].

There are three connected concepts related to Attribute-Based Authentication:

1. Attribute-Based Access Control (ABAC) is determined by analysing a set of attributes related to the subject (user), object (resource), and environment under the Attribute-Based Access Control (ABAC) model. Policies that outline the circumstances in which access is allowed or denied are used to guide the access control decision.

2. Attribute-Based Encryption (ABE) is a type of cryptography in which attributes are used to base both encryption and decryption. In ABE, a ciphertext is linked to an access control over attributes and a user's private key to a collection of attributes. If and only if a user's attributes meet the requirements of the access policy, they can decrypt the ciphertext [2]. Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE) are the two primary varieties of ABE.

3. Attribute-Based Signatures (ABS) is a cryptographic primitive where a signer can sign a message on behalf of a group of users that share certain attributes [3]. The signature can be verified without revealing the signer's identity, but only the fact that the signer possesses the required attributes. ABS can be used for anonymous authentication and privacy-preserving applications.

These concepts offer a comprehensive framework for effectively managing security activities, taking into account unique qualities. In comparison to the conventional binary decisions of giving or denying access, they provide a more flexible and sophisticated approach to security policy. At the core of these principles is the conviction that qualities, whether pertaining to the user, the object, or the surrounding context, exert significant influence on the outcome of a security operation. When integrated, these elements establish the basis for a comprehensive security framework. For instance, a first step in the process could involve the utilisation of Attribute-Based Authentication (ABA), followed by the application of Attribute-Based Access Control (ABAC) to determine and validate access privileges. After obtaining authorization, Attribute-Based Encryption (ABE) can be utilised to decipher the data, while Attribute-Based Signatures (ABS) can be employed to verify any modifications done. In contemporary contexts characterised by complex systems, whether in decentralised settings or situations emphasising the protection of privacy, attribute-centric techniques hold significant value [11]. They prioritise maintaining security while also preserving adaptability and minimising the disclosure of unnecessary information.

3.1 The Genesis of ABA: From RBAC to Attributes

The emergence of Attribute-Based Authentication (ABA) can be seen as a logical evolution from the preexisting Role-Based Access Control (RBAC) framework. The advent of Role-Based Access Control (RBAC) was a notable paradigm shift in the realm of access control, wherein the emphasis shifted from individual user identities to a framework that revolved on the roles assumed by individuals within an organizational context [12]. In the context of a Role-Based Access Control (RBAC) model, individuals are allocated distinct roles, each of which is accompanied by a set of predetermined access permissions. When a user attempts to gain access to a particular resource, the system verifies the user's designated role and subsequently allows or refuses access in accordance with the permissions associated with said role.

Although RBAC represented progress compared to identity-based access control, it became apparent that roles alone were inadequate for managing the progressively intricate and varied user contexts that arose with the expansion of digital technologies and networked systems. The rigidity and predefinition of roles often imposed limitations on their capacity to effectively accommodate the diverse range of factors that impact access decisions, including user location, device type, and time of day [13]. It was evident that a more versatile and adaptable approach was required.

The solution to this difficulty was ABA, which expanded on the concept of RBAC by incorporating a wider range of user qualities in addition to roles. In the field of Applied Behaviour Analysis (ABA), attributes pertain to any discernible characteristic or inherent quality linked to a user, which can be utilized to determine access-related decisions. In contrast to roles, characteristics possess a higher level of granularity and diversity, as they cover a wide range of static and dynamic information pertaining to people [14].

Static attributes refer to characteristics that exhibit a relatively stable nature over a period of time, such as an individual's age, occupational designation, or organizational department affiliation. These qualities are frequently predetermined and can be readily linked to a user's profile or account.

In contrast, dynamic qualities refer to those that exhibit frequent variability and are contingent upon the user's present circumstances or contextual factors. Dynamic attributes encompass various factors that can influence user interactions inside a system [15]. These factors may include the user's present geographical location, the specific device employed to access the system, or even the time of day. These characteristics are frequently obtained from data in real-time and can be utilized to facilitate access decisions that are more cognizant of the surrounding context.

In an ABA (Attribute-Based Access) system, access policies are established by considering various combinations of user traits. This technique enables a flexible and adaptable method for controlling access. When a user endeavours to get access to a particular resource, the system assesses the qualities of the user in relation to the access policy and makes a determination regarding granting or denial of access. The aforementioned technique offers a considerable level of adaptability and specificity in the administration of access privileges, rendering it highly suitable for the intricate and varied user environments that are emblematic of the contemporary digital realm [16].

Examples of some distinct attributes used to verify eligibility of Humans and Machines to access services behind ABA are listed in Figure 3.

3.2 The link between Industry 4.0 & Attribute Based Authentication (ABA)

Industry 4.0, commonly known as the Fourth Industrial Revolution, encompasses a paradigm shift within the industrial domain. This shift entails the assimilation of digital technologies, including the Internet of Things (IoT), artificial intelligence, robotics, and cloud computing, into manufacturing operations.

The fundamental focus of this revolution lies in the incorporation of contemporary intelligent technology within industrial settings, with a particular emphasis on the utilization of cyber-physical systems to oversee the physical operations of a plant and facilitate decentralized decision-making.

The fundamental constituents of the industry encompass several elements such as Internet of Things (IoT) devices, Cyber Physical systems (CPS), Big Data and analytics, autonomous robotics, computer simulation, system integrations, augmented reality, and additive manufacturing.

The advent of Industry 4.0 technologies has facilitated increased connectivity and automation, hence necessitating the implementation of robust and secure authentication procedures.

Attribute-based authentication (ABA) is a technology

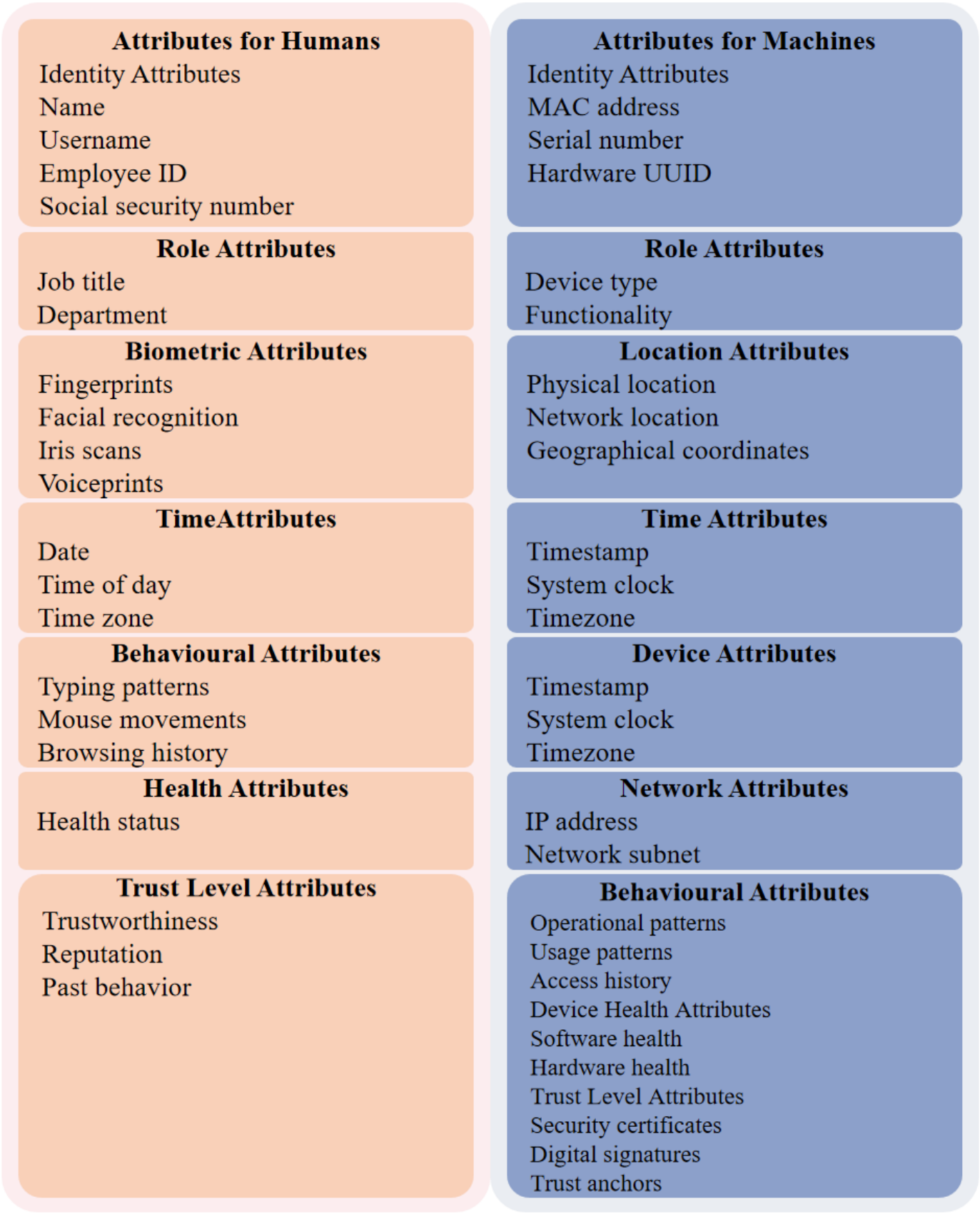

Figure 3. ABA attributes used to verify user's eligibility for authorisation.

that is gaining popularity in the realm of Industry 4.0. In contrast to conventional authentication methods that depend on a solitary element, such as a password, ABA facilitates a more sophisticated and detailed

approach to authentication by considering several attributes linked to an individual or device [17]. The aforementioned attributes encompass a range of factors, including biometrics, behavioural patterns, device information, and contextual details such as location and time.

3.3 Applications of Attribute-Based Authentication

Cloud computing is a prominent field where ABA is in significant use. In the context of a cloud storage service, users have the ability to upload and securely store files that contain sensitive information. Instead of explicitly designating individual users with access privileges to certain files, the owner may want to establish policies that restrict access to specific groups, such as "solely users affiliated with my organization" or "exclusively users holding managerial positions" [18]. The authentication process of the storage system is contingent upon several factors, such as the user's affiliation with a specific organization or their designated title. Access to the system is then either granted or denied based on these attributes.

Similarly, within the manufacturing industry, ABA proves invaluable. Access to confidential manufacturing records and high-value production process information stored on servers may be contingent upon specific attributes. Authorized individuals are granted access based on attributes defined in the database, while those lacking these characteristics are denied access to the records [19].

Moreover, the utilization of ABA can be effectively applied to the Internet of Things (IoT) as well. In the context of an Internet of Things (IoT)-enabled smart home, it is plausible for gadgets to engage in communication with one another, predicated upon specific features [20]. As an illustration, a device may exclusively interact with devices that have obtained certification from manufacturer X or operate on software version 2.0 and higher. This measure can enhance the resilience of the system to potential security risks arising from uncertified or obsolete devices.

Digital Rights Management (DRM) systems, especially in the context of online movie streaming platforms, may utilize Access Based Authorization (ABA) to ascertain user access privileges. Individuals may choose to access particular films or television programs based on several factors such as their subscription tier, geographical area, or age group. Likewise, within collaborative settings such as inter-university research endeavours, the availability of some data may be limited to researchers possessing specific qualifications, such as affiliation or expertise in a particular subject matter [21].

Likewise, electronic government services represent a field in which ABA can be exceptionally valuable. A government service portal in the online domain has the potential to provide tailored services to citizens based on their individual traits. Veterans, who hold the characteristic of having served in the military, are able to avail themselves of certain privileges that are not accessible to others lacking this feature [22]. Furthermore, educational platforms, such as an online portal provided by a university, may provide access to resources contingent upon certain features, such as enrolment in specific courses or declaration of a particular major [23].

So, although ABA offers some benefits like as flexibility, scalability, and improved privacy, it is not exempt from encountering certain difficulties. The task of managing attributes, particularly when their quantity increases, might be perceived as challenging [24, 25]. Furthermore, it is important to note that the intricacy of rules can intensify, hence necessitating a fundamental reliance on the credibility of the institution responsible for assigning and validating attributes. Nevertheless, when implemented in a comprehensive manner, ABA provides a sophisticated way to managing access control in diverse sectors.

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 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 CP-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 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.

The process of generating the ciphertext involves utilising a collection of attributes. In order to successfully decipher the ciphertext, the user must possess a private key that aligns with the access structure connected with the attributes linked to the ciphertext [26]. Whereas the KP-ABE encryption strategy involves the inclusion of the access policy within the ciphertext, while the characteristics are linked to the private key of the user [28]. In the context of CP-ABE, a specific ciphertext is linked to an access structure. The decryption of said ciphertext is only possible for a user if the attributes connected with their private key meet the requirements of the access structure associated with 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

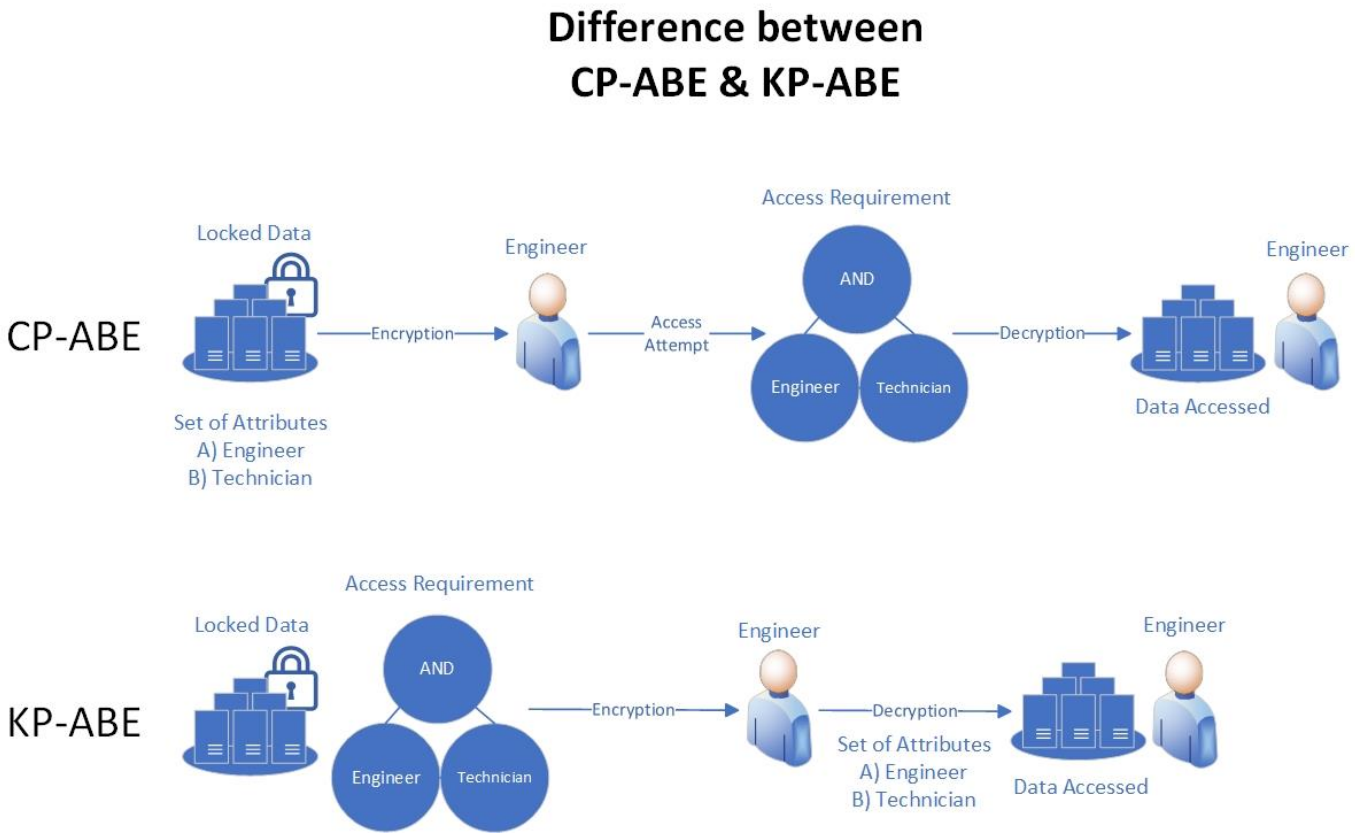

Figure 4. Distinction between two main ABE Schemes.

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

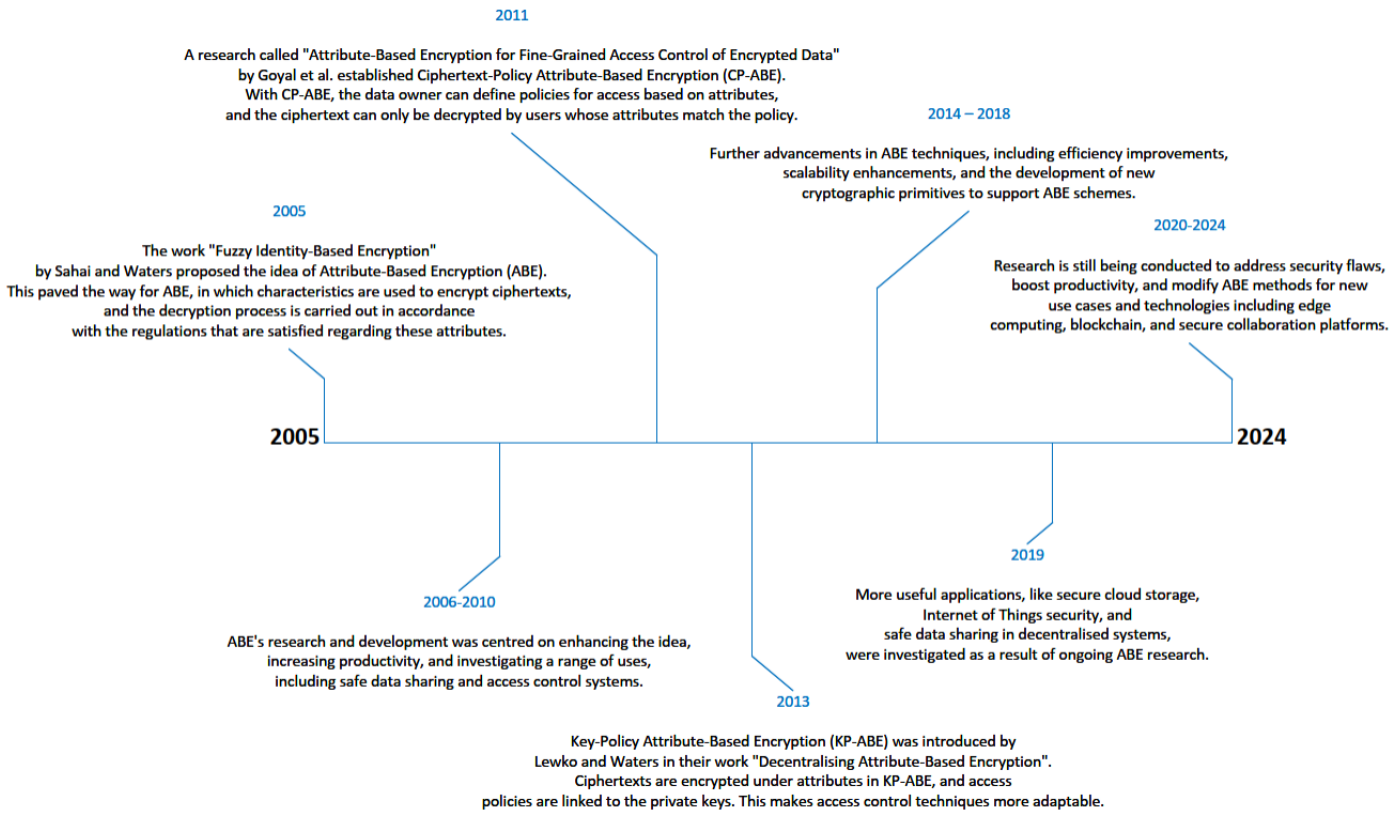

Figure 5. Evolution of Attribute-Based Encryption (ABE): A Timeline from 2005 to 2024.

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.

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 is utilised in secure cloud storage, healthcare information exchange, and corporate data protection, where the ability to regulate access based on roles and departments is of utmost importance [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 *Sahai-Waters Key-Policy Attribute-Based Encryption (KP-ABE)*

Sahai-Waters Key-Policy Attribute-Based Encryption (KP-ABE) is a sophisticated cryptographic system created by Amit Sahai and Brent Waters, which expands upon the fundamental notion of KP-ABE initially proposed by Goyal et al [32]. The main goal of Sahai-Waters KP-ABE is to improve the security and efficiency of fine-grained access control, while also maintaining the ability to describe intricate access restrictions [34].

During the initial setup phase, a reliable entity is accountable for choosing cryptographic parameters and creating public parameters. In addition, the authority creates a master secret key that is crucial for deriving private keys for individual users. Users are subsequently allocated collections of attributes according to their qualities, which can be numerical numbers or texts.

When a user wishes to have access to encrypted data, they initiate a request for key generation to the governing body. The authority employs the user's qualities and the public parameters to create a user-specific private key that aligns with the intended access policy. The access policy is commonly represented as a Boolean expression that incorporates attributes.

The encryption procedure entails the data owner encrypting sensitive data using a designated access policy. The resulting ciphertext comprises the encrypted data along with the corresponding access policy. In order to decrypt the data, the user needs to have a private key that meets the access requirements specified in the encrypted message. The decryption procedure involves the utilization of the user's private key in conjunction with the ciphertext to get the original plaintext.

The Sahai-Waters KP-ABE plan presents various significant enhancements in comparison to previous methods. Firstly, it attains selective security, which implies that it maintains its security even in the presence of adversaries who can dynamically select the problems they want to overcome. In addition, the scheme is specifically designed to be resistant

to adaptive selected ciphertext assaults, ensuring its durability against a wide range of security vulnerabilities. Optimizations improve the efficiency of key generation, encryption, and decryption procedures.

Bilinear pairings, a type of mathematical operations performed on groups of elliptic curves, have a significant impact on the attainment of the security objectives of Sahai-Waters KP-ABE. These pairings provide the validation of specific connections between encrypted data without disclosing the actual data, hence enabling the application of comprehensive access rules in a secure way.

It is crucial to acknowledge that Sahai-Waters KP-ABE is an advanced cryptographic technique, and its security is dependent on the difficulty assumptions associated with bilinear pairings. The successful execution and installation of such plans necessitate meticulous evaluation of particular application prerequisites and any compromises in security [35].

5.2.4 *Lewko-Waters Fully Collusion-Resistant Key-Policy Attribute-Based Encryption (KP-ABE)*

Lewko-Waters Fully Collusion-Resistant Key-Policy Attribute-Based Encryption (KP-ABE) is an improved version of the traditional KP-ABE scheme that effectively tackles the weaknesses related to collusion attacks. Suggested by Allison B. Lewko and Brent Waters, this method implements enhanced security measures to protect against collusion, which refers to the situation where numerous users cooperate to undermine the security of the system. In the beginning, a reliable entity is responsible for choosing cryptographic parameters and creating public parameters, as well as a master secret key for future actions. Attributes are assigned to users, and private keys are created by the authority according to the user's attributes and the desired access policy [36].

In order to enhance the security of the scheme against collusion assaults, the Lewko-Waters Fully Collusion-Resistant KP-ABE incorporates elements such as a Collusion-Resistant Master Secret Key (CR-MSK), which guarantees that users who collude cannot obtain any compromising data. The key derivation process is specifically designed to thwart collusion attempts, so preventing users from pooling their private keys in order to obtain illegal access. In addition, the technique offers protection against arbitrary collusion, ensuring that any group of users, regardless of their number, cannot collectively decrypt ciphertexts for which none of them individually possess the necessary access. The achievement of these qualities that defy collusion is made possible by employing sophisticated cryptographic techniques, such as bilinear pairings, as well as mathematical structures like lattices or multilinear maps [35].

Although the improved security against collusion is a notable advantage, it is crucial to take into account the potential rise in computational complexity. The selection of an Attribute-Based Encryption (ABE) scheme, including the decision to choose a variation that is resistant to collusion, should be determined by the precise security needs and performance concerns of the particular application. The Lewko-Waters Fully Collusion-Resistant KP-ABE scheme provides enhanced security measures to effectively mitigate collusion threats in a comprehensive manner.

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.
- On the other hand, the Lewko-Waters Fully Collusion-Resistant KP-ABE scheme improves security by providing complete protection against collusion. This functionality guarantees that information remains inaccessible to users until their combined attributes meet the requirements of the access policy, even if they collaborate and combine their keys. This method exhibits a notable progression in security when compared to previous KP-ABE models, rendering it well-suited for high-security applications where collusion constitutes a considerable threat [39].
- The Sahai-Waters KP-ABE scheme, an early contribution in this field, presented the idea of including access controls into users' private keys. While it established the foundation for future advancements in ABE, it is less proficient at managing collusion and scalability when compared to more recent methods.
- 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 prevention of collusion, which enhances security. On the other hand, the Sahai-Waters' scheme is valuable for comprehending the fundamental principles of KP-ABE due to its simplicity and foundational nature. 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 Access Control) 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 sophisticated behavioural analytics (ABA) and anomaly-based detection (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 explores the uses of Attribute-Based Encryption (ABE) and Attribute-Based Authentication (ABA) technologies, particularly in the dynamic environments of Industry 4.0 and IoT devices. We examined the impact of cryptographic and authentication models on improving data sharing and security in cloud environments, particularly in situations that necessitate accurate access control and strong authentication techniques. An integral component of our study entails investigating the possible incorporation of these models with machine learning methodologies, offering a chance to enhance security in cloud-based systems. The analysis thoroughly examines different ABE schemes, including Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE), evaluating their efficiency, access control methods, and appropriateness for data sharing systems. The examination included a wide range of applications of ABA across multiple domains. An important issue emphasised in this paper is the need to effectively handle a growing number of attributes in a sophisticated manner, while also complying with various legal frameworks. The significance of strong authentication protocols in the context of Industry 4.0, which is characterised by increased automation, is also emphasised in this study. As a result, we feel that there needs to be continued necessity for investigation in ABE (Attribute Based Encryption) and ABA (Attribute-Based Access Control), in accordance with the changing requirements of Industry 4.0, to guarantee the safe, effective, and expandable interchange and authentication of data in industrial and technical 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] Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering–a systematic literature review. *Information and software technology*, 51(1), 7-15. [CrossRef]

[2] 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]

[3] Mohassel, P. (2011). One-time signatures and chameleon hash functions. In *Selected Areas in Cryptography: 17th International Workshop, SAC 2010, Waterloo, Ontario, Canada, August 12-13, 2010, Revised Selected Papers 17* (pp. 302-319). Springer Berlin Heidelberg. [CrossRef]

[4] Wang, S., J. (2022). Application of User Identity Authentication Technology in Network Information Security. Inf. Comput. (Theor. Ed.), vol. 08, pp. 221–223.

[5] Chen, Y., J., Gao, H., R., and Ding, Z. J. (2023). Credit Evaluation Model Based on Dynamic Machine Learning. Comput. Sci., vol. 01, pp. 59–68.

[6] Yin, F., F. (2021). Research on Revocable and Searchable Attribute-Based Encryption Algorithms. (Master's thesis, Xidian University).

[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] Papadamou, K., Zannettou, S., Chifor, B., Teican, S., Gugulea, G., Caponi, A., ... & Sirivianos, M. (2019). Killing the password and preserving privacy

with device-centric and attribute-based authentication. *IEEE Transactions on Information Forensics and Security*, 15, 2183-2193. [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. [CrossRef]

[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. [CrossRef]

[23] Liagkou, V., Metakides, G., Pyrgelis, A., Raptopoulos, C., Spirakis, P., & Stamatiou, Y. C. (2014). Privacy preserving course evaluations in Greek higher education institutes: an e-Participation case study with the empowerment of Attribute Based Credentials. In *Privacy Technologies and Policy: First Annual Privacy Forum, APF 2012, Limassol, Cyprus, October 10-11, 2012, Revised Selected Papers 1* (pp. 140-156). 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] Hariss, K., & Noura, H. (2022). Towards a fully homomorphic symmetric cipher scheme resistant to plain-text/cipher-text attacks. *Multimedia Tools and Applications*, 81(10), 14403-14449. [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 stand-alone authentication in IoT. *IEEE Internet of Things Journal*. [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*, 1-19. [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). [CrossRef]

[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 was awarded a 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)