Review

Not peer-reviewed version

Advancements in Securing Cloud-Stored Data and Managing Sensitive Information: A Comprehensive Review of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) Techniques

Priya S and Amritha R [*]

Posted Date: 28 August 2024

doi: 10.20944/preprints202408.1992.v1

Keywords: Ciphertext-Policy Attribute-Based Encryption (CP-ABE); Blockchain; Key Management; Decentralized Security; Cloud-Stored Data, Yolo V7; Explainable AI (XAI); Online/Offline Multi-Authority Scheme; Hid

Review

Advancements in Securing Cloud-Stored Data and Managing Sensitive Information: A Comprehensive Review of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) Techniques

S.Priya [1] and R.Amritha [2,*]

[1] Assistant Professor, Department of IT PSG College of Technology Coimbatore; India spa.it@psgtech.ac.in
[2] PG Scholar, Department of IT PSG College of Technology Coimbatore, India
* Correspondence: 23pb03@psgtech.ac.in

Abstract: The exploring comprehensive review of cutting-edge techniques for securing cloud-stored data and managing sensitive information in the context of smart cities through the application of Ciphertext-Policy Attribute-Based Encryption (CP-ABE). It highlights the innovative integration of blockchain technology with CP-ABE, which introduces a decentralized and tamper- resistant key management system, thereby enhancing the overall security framework in cloud environments where data sharing is prevalent. Introducing an online/offline multi-authority CP- ABE scheme, characterized by hidden policies, offers significant advancements in protecting user attributes and access structures, ensuring that sensitive information remains confidential even during encryption and decryption processes. This dual approach not only fortifies security but also optimizes the efficiency of data- sharing mechanisms. Furthermore, the paper delves into imple- menting hidden sensitive policies and keyword search techniques within smart city infrastructures, which are designed to facilitate secure and efficient data retrieval. These techniques ensure that while data remains accessible to authorized users, privacy is rigorously maintained. Collectively, these approaches represent significant strides in bolstering the security and confidentiality of data in both cloud-based and smart city applications, addressing the growing demand for robust and efficient data management solutions in increasingly interconnected environments.

Keywords: Ciphertext-Policy Attribute-Based Encryption (CP-ABE); Blockchain; Key Management; Decentralized Secu- rity; Cloud-Stored Data; Yolo V7; Explainable AI (XAI); On- line/Offline Multi-Authority Scheme; Hidden policies; Privacy Preservation; Data Protection; Secure Data Management

I. Introduction

In an era where digital data is increasingly valuable and pervasive, ensuring its security and privacy has become a critical concern. The rapid growth of cloud computing and smart city technologies has introduced new complexities in managing sensitive information. Cloud environments, charac- terized by their dynamic and distributed nature, face significant challenges in maintaining data confidentiality and integrity, especially when dealing with multiple users and varying levels of access. Similarly, smart cities generate vast amounts of data from numerous sources, necessitating robust solutions to pro-tect this information from unauthorized access and breaches. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has emerged as a promising solution, offering a mechanism to enforce fine-grained access control based on user attributes. CP-ABE enables data owners to define policies that specify which attributes must be satisfied for decryption, providing a flexible and scalable approach to securing sensitive informa- tion. Despite its advantages, traditional CP-ABE approaches face challenges related to key management, computational efficiency, and privacy preservation. Key management in CP- ABE can be cumbersome, especially in cloud environments where data is frequently shared among multiple users. The complexity of handling encryption keys and policies can lead to potential vulnerabilities and inefficiencies. Additionally, CP-ABE's performance can be impacted by the need for extensive computations during encryption and decryption pro- cesses. These issues become more pronounced in large-scale systems, where the overhead associated with key distribution and policy enforcement can hinder operational efficiency. To address these challenges, recent advancements have focused on integrating CP-ABE with complementary technologies and features. The incorporation of blockchain technology with CP- ABE provides a decentralized and tamper-proof framework for managing keys, enhancing both security and transparency. Blockchain's immutable ledger ensures that keys are dis- tributed and accessed only by authorized users, mitigating risks associated with key compromise and unauthorized access. Moreover, innovations such as online/offline multi-authority CP-ABE schemes introduce hidden policies that obscure user attributes and access structures during encryption and decryp- tion. This approach not only enhances privacy by protecting sensitive policy information but also improves efficiency by allowing some tasks to be performed offline, reducing com- putational burdens. In the context of smart cities, where data security and efficient retrieval are paramount, the integration of hidden sensitive policies and keyword search techniques with CP-ABE offers significant benefits. Hidden policies ensure that sensitive information about access controls remains concealed, while keyword search capabilities enable users to retrieve encrypted data without exposing its content. This combination addresses both privacy and usability concerns, allowing for secure and efficient data management in environments charac- terized by high data volumes and diverse user needs. Overall, this paper reviews these advanced methods, highlighting their impact on improving data security and privacy in cloud and smart city applications and providing insights into their effectiveness in addressing the evolving challenges of modern data management. Overall these advanced methods, highlight their impact on improving data security and privacy in cloud and smart city applications. Key innovations include the use of blockchain for secure key management, online/offline multi-authority CP-ABE schemes with hidden policies to enhance both security and efficiency and keyword search techniques that facilitate secure data retrieval. These advancements col- lectively address critical challenges such as key distribution vulnerabilities, computational overhead, and privacy concerns, offering robust solutions for managing sensitive information in today's complex digital environments. The paper provides a comprehensive overview of how these techniques contribute to more effective and scalable data protection strategies in both cloud and smart city contexts.

II. Literature Survey

This integration of blockchain technology with Ciphertext- Policy Attribute-Based Encryption (CP-ABE) addresses key management challenges for cloud-stored data. The paper em- phasizes several key advancements. Firstly, the combination enhances security by utilizing blockchain's decentralized and immutable ledger for key distribution, making the process tamper-proof and ensuring that keys are accessible only to authorized users. This integration also offers a more transpar- ent and auditable key management system, enabling contin- uous monitoring and easier detection of potential breaches. Additionally, blockchain helps streamline key management processes, improving efficiency and scalability in cloud en- vironments. By overcoming the limitations of traditional key management systems and providing a robust framework for protecting sensitive data, this approach significantly enhances data security in cloud storage systems [1]. A significant advancement in cloud data security by proposing a novel CP- ABE framework. This approach introduces an online/offline multi-authority model to enhance data sharing security, distributing control over attributes among multiple authorities. This distribution mitigates the risks associated with a single point of failure and strengthens the system's overall resilience. A key innovation is the hidden policy feature, which pro- tects user attributes and access policies from exposure during encryption and decryption, thereby improving privacy and reducing the risk of policy leakage. The paper also addresses efficiency concerns by employing an online/offline model, which allows certain computational tasks to be completed offline. This optimization reduces the time and resources required for encryption and decryption, making the system more operationally efficient. Additionally, the framework en- sures privacy-preserving data sharing by obfuscating sensitive information and controlling access, thus maintaining high privacy standards while facilitating secure data exchange. The scalability and flexibility of the multi-authority setup further support its adaptability to various cloud environments and large-scale data-sharing scenarios, demonstrating its effective- ness in meeting diverse application needs [2]. The privacy- preserving mechanisms are designed for information sharing in Online Social Networks (OSNs), specifically through Privacy Situation Awareness (PSA). OSNs are widely used platforms where users share personal information, which raises signif- icant privacy concerns due to potential exposure to unautho- rized parties. The paper examines mechanisms that enhance privacy by incorporating situational awareness into the data- sharing process. PSA involves understanding and adapting to the privacy context of both the data and the user, allowing for more informed and dynamic control over what information is shared and with whom. Key points include the implementation of context-aware policies that adjust privacy settings based on real-time situational factors and user preferences. The review also covers various approaches to balancing user privacy with the need for effective information sharing, highlighting advancements in privacy technology and their impact on safeguarding sensitive data in OSNs [3].This explores the application of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) in smart cities, focusing on enhancing both security and privacy through hidden sensitive policies and keyword search techniques. In smart city environments, where large volumes of sensitive data are generated and shared, protecting this information while ensuring efficient access is crucial. The paper introduces a CP-ABE scheme that incorporates hidden sensitive policies to obscure the details of access controls and encryption parameters, thereby safeguarding user privacy and preventing unauthorized disclosure of policy information. Ad- ditionally, it integrates keyword search capabilities, allowing users to perform searches on encrypted data without revealing the content or search queries. This approach not only enhances the privacy of the data but also improves retrieval efficiency, addressing the dual needs of security and usability in smart city data management systems [4]. This investigates the application of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) within Internet of Things (IoT) systems, specifically using MQTT (Message Queuing Telemetry Transport) for commu- nication and Raspberry Pi as the hardware platform. CP-ABE is utilized to enhance the security of data transmitted between IoT devices, ensuring that only authorized users with specific attributes can access the encrypted information. The integra- tion of MQTT, a lightweight messaging protocol, facilitates efficient and scalable communication in IoT environments, while Raspberry Pi serves as a cost-effective and versatile computing platform. The paper examines how CP-ABE can be implemented to secure MQTT messages addresses challenges related to key management and computational resources, and evaluates the performance of this approach in a practical IoT setup [5]. This presents a non-interactive verifiable computa-tion model for perceptual layer data using Ciphertext-Policy Attribute-Based Encryption (CP-ABE). The proposed model addresses the challenge of ensuring the integrity and correct- ness of computations performed on encrypted data without requiring interaction between the data owner and the computational entity. By leveraging CP-ABE, the model enables fine-grained access control over encrypted data, ensuring that only authorized parties can perform and verify computations. This approach enhances data security and privacy by allow- ing verifiable results while maintaining the confidentiality of the data. The paper highlights the model's effectiveness in enabling secure and trustworthy computations on encrypted perceptual layer data, making it a valuable contribution to the field of secure data processing and management [6]. The Multi-Layered Ciphertext-Policy Attribute-Based Encryption (CP-ABE) Scheme for Flexible Policy Update addresses the challenge of dynamically updating access policies in the context of Industry 4.0. This scheme enhances traditional CP- ABE by introducing a multi-layered architecture that supports flexible and efficient policy updates. In Industry 4.0 envi- ronments, where systems and access requirements frequently change, the ability to quickly adapt access control policies without compromising security is crucial. The multi-layered approach allows for hierarchical policy management, enabling updates to be made at various levels of the access control structure while maintaining overall security. This method improves scalability and adaptability, making it well-suited for the complex and evolving data management needs of modern industrial systems [7]. The paper on the ”Data Con- firmation Scheme based on Auditable CP-ABE” introduces a novel approach to enhance the verification and auditing of data within Ciphertext-Policy Attribute-Based Encryption (CP- ABE) systems. It focuses on integrating auditing mechanisms into CP-ABE to provide a reliable method for confirming the integrity and authenticity of encrypted data. The scheme allows for periodic or event-driven audits, enabling auditors to verify that data has not been tampered with and that access controls are properly enforced. This integration ensures that the data remains secure and compliant with defined policies, while also providing a transparent and accountable framework for managing encrypted data in both cloud and distributed environments [8].This paper presents an efficient anonymous identity authentication scheme for the Internet of Vehicles (IoV) using Ciphertext-Policy Attribute-Based Encryption (CP-ABE) combined with consortium blockchain technology. The proposed approach addresses the challenge of securely managing and verifying identities in IoV environ- ments, where privacy and authentication are critical. CP-ABE enables fine-grained access control and encryption of identity- related information, while the consortium blockchain provides a secure and tamper-proof infrastructure for managing au- thentication data and transactions. The integration of these technologies ensures that vehicle identities are authenticated anonymously, protecting user privacy while maintaining the integrity and security of the authentication process. This scheme enhances both the security and efficiency of identity management in IoV systems, offering a robust solution for protecting sensitive information in a highly interconnected environment [9]. This paper introduces a Ciphertext-Policy Attribute-Based Encryption (CP-ABE) method that leverages reused sub-policies to improve efficiency and scalability. The proposed method optimizes the encryption process by reusing existing sub-policies, thereby reducing computational over- head and storage requirements associated with policy man- agement. This approach enhances the efficiency of CP-ABE in environments with large-scale or dynamic attribute sets, making it more practical for real-world applications where frequent policy updates and high-performance demands are common. By addressing the challenges of scalability and resource utilization, this method provides a more efficient so- lution for implementing fine-grained access control in various secure data management scenarios [10]. This distributed cryp- tography technique is aimed at enabling lightweight encryption in decentralized Ciphertext-Policy Attribute-Based Encryption (CP-ABE) systems. The focus is on optimizing encryption processes to be more efficient and resource-friendly, par- ticularly in decentralized environments where computational resources may be limited. By leveraging distributed cryp- tographic methods, the approach reduces the computational overhead and enhances the scalability of CP-ABE, making it suitable for use in resource-constrained settings. The paper highlights how these techniques improve the performance of decentralized CP-ABE systems, enabling secure and efficient data encryption and access control in environments with limited computational resources [11]. The lightweight, pairing- free multi-authority Ciphertext-Policy Attribute-Based Encryp- tion (CP-ABE) scheme is designed for cloud-edge-assisted Internet of Things (IoT) environments. The proposed scheme addresses the scalability and efficiency challenges associated with traditional CP-ABE methods, particularly in distributed IoT systems where resource constraints and performance are critical. By eliminating the need for costly pairing operations, the scheme reduces computational overhead and improves sys- tem efficiency. The multi-authority approach enhances security by distributing trust among multiple entities, allowing for more flexible and robust access control in cloud-edge-assisted IoT architectures. This scheme effectively balances security and performance, making it well-suited for the demands of modern IoT applications [12]. The enhancement of Unmanned Aerial Vehicle (UAV) security through the implementation of Zero Trust Architecture (ZTA), incorporating advanced deep learning and Explainable AI (XAI) techniques. The study ad- dresses the growing security challenges faced by UAVs, which require robust measures to protect against potential threats and vulnerabilities. By adopting Zero Trust principles, the ap- proach ensures that no entity—whether internal or external—is inherently trusted, necessitating continuous verification and validation of all access requests. The integration of deep learn- ing models enhances threat detection and response capabilities, while Explainable AI provides transparency and interpretabil- ity of these models, allowing for better understanding and trust in

doi:10.20944/preprints202408.1992.v1

the security decisions made. This combination offers a comprehensive and adaptive security framework for UAVs, improving their resilience against sophisticated attacks and ensuring a higher level of protection in dynamic and complex environments [13]. The integration of YOLO v7 with advanced edge computing for fall detection addresses the pressing issue of elderly safety. Existing fall detection systems often lack speed and accuracy, necessitating a transformative solution. YOLO v7's deep neural network architecture efficiently pro- cesses video feeds, while edge computing minimizes latency. This approach not only ensures rapid analysis and immediate responses but also maintains privacy by keeping data localized. Beyond elder care, this innovative solution holds promise for enhancing safety across various sectors, heralding a future where advanced technology prioritizes personal well-being. A Deep Learning-based smart traffic light system leverages YOLO v7 for image processing to optimize traffic flow. YOLO v7, known for its speed and accuracy, detects and classifies vehicles in real-time from traffic camera feeds. The system adjusts traffic light timings based on vehicle density and move- ment patterns, reducing congestion and improving efficiency. High-quality datasets of annotated traffic images are used to train the YOLO v7 model, ensuring accurate vehicle detection and classification. This smart traffic light system enhances traffic management by minimizing delays and adapting to real-time traffic conditions [14]. Image-based foreign object detection using the YOLO v7 algorithm for electric vehicle wireless charging applications enhances safety and efficiency by identifying and removing obstacles. YOLO v7's speed and accuracy allow real-time detection of foreign objects on charging pads, preventing potential damage or interference. High-quality datasets with annotated images of various objects ensure the model's robustness and accuracy. Implementing this system improves the reliability of wireless charging stations by ensuring a clear, unobstructed charging area, ultimately protecting both the vehicle and the charging infrastructure[15]. Improving object detection accuracy in VVC-coded video using YOLO v7 features involves leveraging YOLO v7's superior detection capabilities. YOLO v7, known for its speed and precision, enhances object detection in compressed VVC video streams. By utilizing high-quality training datasets with annotated objects, the system can accurately detect objects despite video compression artifacts. This integration optimizes the balance between compression efficiency and detection per- formance, leading to more reliable object recognition in VVC- coded videos[16]. An improved nighttime detection algorithm based on YOLO v7 enhances the identification of people and vehicles in low-light conditions by leveraging YOLO v7's advanced detection capabilities. This algorithm is specially designed to overcome the challenges posed by nighttime envi- ronments, such as low visibility, glare from artificial lighting, and varying light conditions. By using high-quality, annotated datasets specifically collected during nighttime, the system ensures robust performance and accuracy. The algorithm can effectively distinguish between people and vehicles even in dimly lit areas, making it particularly useful for applications like surveillance, security, and traffic monitoring at night. This enhanced detection capability contributes to increased safety and security by providing reliable monitoring and alerting systems in environments where traditional detection methods often fail[17]. Automated non-helmet rider detection using YOLO v7 and OCR enhances traffic monitoring by identifying motorcyclists without helmets. YOLO v7's high-speed and accurate object detection capabilities enable real-time identification of riders. By training the model with annotated datasets of helmeted and non-helmeted riders, the system can distinguish between the two effectively. OCR (Optical Character Recognition) is integrated to read license plates, allowing authorities to identify and penalize violators. This automated system improves road safety by ensuring compli- ance with helmet laws and provides a reliable solution for traffic enforcement. The combination of YOLO v7 and OCR ensures thorough monitoring and efficient processing, making it an invaluable tool for modern traffic management systems [18]. This investigates the vulnerabilities and potential decep- tions associated with post-hoc Explainable AI (XAI) methods used in network intrusion detection systems. It examines how these explainability techniques, which are designed to provide insights into AI model decisions, can be manipulated or misled by adversarial attacks. The study highlights the limitations of current XAI approaches in accurately reflecting the true decision-making process of AI models and their susceptibility to deliberate distortions. By analyzing various post-hoc explanation methods, the paper underscores the need for more robust and reliable explainability mechanisms to improve the effectiveness and trustworthiness of network in- trusion detection systems [19].This paper explores methods for enhancing the fairness and performance of edge cameras using Explainable AI (XAI) techniques. It addresses the challenge of ensuring that edge cameras, which are critical for applications such as surveillance and monitoring, operate fairly and efficiently across diverse scenarios. The use of XAI helps in interpreting and understanding the decision-making processes of AI models deployed in edge devices, allowing for greater transparency and accountability. By applying XAI, the paper aims to improve the accuracy and fairness of camera-based systems, ensuring that they provide reliable and unbiased performance while maintaining high operational standards in real-time environments [20]. The integration of Explainable AI (XAI) into Intrusion Detection Systems (IDS) enhances their effectiveness and transparency in cloud environments and addresses the challenge of making IDS more effective and transparent by incorporating explainability into AI-driven detection mechanisms. By leveraging XAI, the paper aims to improve the interpretability of AI models used in IDS, allowing security analysts to better understand and trust the system's decisions. This approach not only enhances the detection of malicious activities but also aids in the inves- tigation and response processes by providing clear, actionable insights into how decisions are made. The integration of XAI into IDS is presented as a crucial step toward more reliable and understandable security solutions for protecting cloud infrastructures [21]. The potential of using Explainable

AI (XAI) to enhance the security of energy systems against cyberattacks. It focuses on how XAI can improve the un- derstanding and interpretation of AI-driven security measures by providing clear, interpretable insights into decision-making processes. By applying XAI techniques, the paper aims to make AI-based threat detection and response mechanisms more transparent and reliable, enabling better identification of vulnerabilities and more effective responses to attacks. This approach enhances the overall security posture of energy systems by bridging the gap between complex AI algorithms and actionable security insights, ultimately leading to more resilient and adaptive defense strategies [22]. This paper eval- uates black-box explainable AI (XAI) frameworks specifically designed for network intrusion detection. It examines various XAI methods that provide transparency into the decision- making processes of complex machine-learning models used for detecting network threats. By focusing on the effective- ness of these frameworks in elucidating model predictions, the paper aims to enhance the interpretability of intrusion detection systems, which is crucial for understanding and trusting automated security measures. The evaluation includes a comparison of different XAI techniques in terms of their ability to reveal insights into model behavior, improve threat detection accuracy, and support security analysts in interpret- ing and responding to detected intrusions. This analysis helps in identifying the most effective approaches for integrating explainability into network intrusion detection systems [23]. By use of explainable models to enhance the interpretation of malware detection results. It focuses on employing agnostic methods that do not rely on specific model architectures but instead provide general frameworks for explaining how detection decisions are made. By leveraging explainability techniques, the paper aims to improve the transparency of malware detection systems, allowing security professionals to understand and trust the model's predictions. This approach is crucial for identifying and addressing potential issues or biases in detection algorithms, ultimately enhancing the effectiveness and reliability of malware detection tools [24].

III. Proposed System

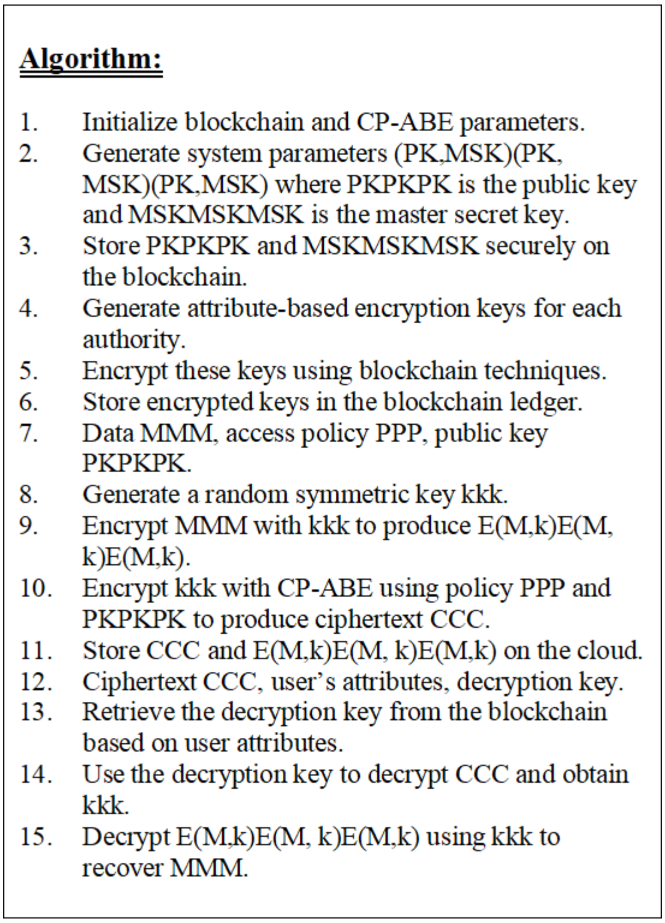
The proposed system addresses critical challenges in secur- ing and managing sensitive data across cloud environments and smart cities by leveraging advanced encryption techniques and innovative technologies. By integrating Ciphertext-Policy Attribute-Based Encryption (CP-ABE) with enhancements such as blockchain technology, multiple authority frameworks, and keyword search capabilities, the system aims to provide a comprehensive solution to privacy and security concerns. The inclusion of blockchain ensures a decentralized and tamper- proof method for key management, while the multi-authority approach and hidden policies safeguard user attributes and access controls.

Additionally, the incorporation of efficient keyword search techniques facilitates secure and swift data retrieval. This combination of features ensures that sensi- tive data remains protected from unauthorized access while remaining accessible to authorized users, balancing privacy, usability, and efficiency effectively. This component enhances the traditional CP-ABE model by incorporating blockchain technology. Blockchain provides a decentralized, tamper-proof framework for key management, which is crucial for main- taining secure and controlled access to encrypted data in cloud environments. This approach mitigates key management challenges and ensures that data remains protected while accessible only to authorized users.

A. Algorithm

This approach integrates blockchain technology with Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to enhance the security and privacy of cloud-stored data using Elliptic Curve Cryptography (ECC). ECC is a public-key encryption technique that provides strong security with smaller key sizes, making it efficient and suitable for cloud environ- ments. The blockchain serves as a decentralized, tamper-proof ledger for managing cryptographic keys, ensuring that only authorized users can access the data. This combination of ECC and blockchain ensures secure, efficient, and scalable key management, crucial for protecting sensitive information in the cloud. Next one of enhances cloud data sharing security by using an online/offline multi-authority CP-ABE scheme with hidden policies. The algorithm divides tasks between an offline phase, where heavy computations are handled in advance, and an online phase, where lighter, quicker opera- tions occur. The hidden policy feature protects user privacy by concealing access control rules during encryption and decryption, preventing the exposure of sensitive information. Additionally, multiple authorities manage different user at- tributes, distributing control and making the system more secure against attacks, as compromising the system requires breaching multiple authorities. The paper presents a privacy- preserving mechanism designed for information sharing in On- line Social Networks (OSNs) using a real-world social network dataset. The mechanism leverages privacy situation awareness to dynamically adjust privacy settings based on the context and relationships between users. By analyzing user behavior and interactions within the network, the system can identify potential privacy risks and automatically apply appropriate privacy controls. This approach helps users maintain control over their information while participating in social networks, reducing the likelihood of unintended data exposure or privacy breaches. The integration of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) with searchable encryption to secure data sharing in smart cities. The algorithm allows data to be encrypted with hidden sensitive policies, ensuring that the access structure remains confidential. Additionally, it enables keyword search functionality within the encrypted data, allow- ing authorized users to efficiently retrieve relevant information without exposing the underlying content or search queries. This combination enhances both privacy and usability, making it a robust solution for managing and protecting sensitive data in smart city environments.

This system introduces an advanced CP-ABE scheme that employs multiple authorities and hidden policies. The use of multiple authorities helps distribute the control of attributes, thereby increasing security by reducing the risk of system compromise. The online/offline functionality improves effi- ciency by handling certain computational tasks offline, speed- ing up the encryption and decryption processes. Tailored for smart city applications, this system employs CP-ABE with hidden sensitive policies to manage vast amounts of data securely. Concealing access structures enhances privacy. Additionally, it integrates keyword search techniques, enabling efficient data retrieval without exposing the content or search queries, which is essential for maintaining both security and usability. In Ciphertext-Policy Attribute-Based Encryption (CP-ABE), the encryption process involves defining an access policy based on user attributes. The data to be encrypted is first encrypted with a symmetric key, which is then encrypted using the CP-ABE scheme based on the specified policy and public key. The resulting ciphertext combines both the encrypted data and the encrypted symmetric key. During decryption, the system retrieves the decryption key associated with the user's attributes from a secure source, such as a blockchain ledger. This key is then used to decrypt the symmetric key, which in turn decrypts the data. This approach ensures that data can only be decrypted by users whose attributes satisfy the access policy, thus providing fine-grained access control and data security.



Algorithm:

```
1.  Initialize blockchain and CP-ABE parameters.
2.  Generate system parameters (PK,MSK)(PK, MSK)(PK,MSK) where PKPKPK is the public key and MSKMSKMSK is the master secret key.
3.  Store PKPKPK and MSKMSKMSK securely on the blockchain.
4.  Generate attribute-based encryption keys for each authority.
5.  Encrypt these keys using blockchain techniques.
6.  Store encrypted keys in the blockchain ledger.
7.  Data MMM, access policy PPP, public key PKPKPK.
8.  Generate a random symmetric key kkk.
9.  Encrypt MMM with kkk to produce E(M,k)E(M, k)E(M,k).
10. Encrypt kkk with CP-ABE using policy PPP and PKPKPK to produce ciphertext CCC.
11. Store CCC and E(M,k)E(M, k)E(M,k) on the cloud.
12. Ciphertext CCC, user's attributes, decryption key.
13. Retrieve the decryption key from the blockchain based on user attributes.
14. Use the decryption key to decrypt CCC and obtain kkk.
15. Decrypt E(M,k)E(M, k)E(M,k) using kkk to recover MMM.
```

Figure 1. Algorithm of CP-ABE.

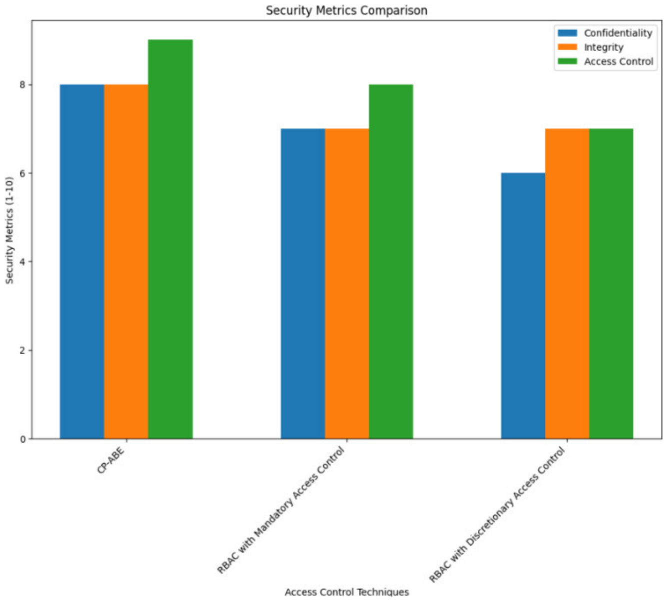


Figure 2. Security Comparison of CP-ABE.

doi:10.20944/preprints202408.1992.v1

The integration of Ciphertext-Policy Attribute-Based En- cryption (CP-ABE) with Role-Based Access Control (RBAC) enhances security by combining two complementary ap- proaches. CP-ABE provides fine-grained access control based on user attributes and policies, ensuring that data remains confidential and accessible only to those who meet the specific criteria. Adding RBAC to CP-ABE introduces an additional layer of access control by defining roles and their permissions within the system. This layered approach reduces the likeli- hood of unauthorized access and improves overall data security by restricting access not only based on attributes but also on the defined roles, which can further segment and protect sensitive information. While CP-ABE offers strong security, its efficiency can be affected by the complexity of attribute-based policies and the need for extensive computational resources. The addition of RBAC can improve efficiency by simplifying access control through predefined roles, which reduces the complexity of managing numerous attributes and policies. This combination streamlines the encryption and decryption processes, making them more manageable and faster compared to a purely attribute-based system. In contrast, standard RBAC alone is highly efficient due to its simplicity, relying on role assignments for access control without the overhead of complex attribute-based encryption. This graph compares various security metrics—confidentiality, integrity, and access control—across different techniques including XAI with CP- ABE and traditional RBAC models. XAI with CP-ABE is shown to provide higher scores in confidentiality, integrity, and access control compared to RBAC with mandatory or discretionary access control. This indicates that the integration of Explainable AI with Ciphertext-Policy Attribute-Based En- cryption enhances security by ensuring better protection and management of sensitive data. The efficiency metrics graph evaluates encryption time, decryption time, and scalability for XAI with CP-ABE compared to RBAC methods. XAI with CP-ABE demonstrates better performance in encryption time and scalability while maintaining competitive decryption time. This suggests that XAI combined with CP-ABE not only pro- vides superior security but also achieves efficient performance in handling encrypted data, making it a robust choice for sce- narios requiring both high security and efficiency. Combining security and efficiency metrics, the comparison highlights that XAI with CP-ABE stands out in terms of both security and performance. It effectively addresses confidentiality, integrity, and access control challenges while also delivering efficient encryption and decryption times and scalability. This makes XAI with CP-ABE a promising approach for modern systems needing strong security and efficient data management, out- performing traditional RBAC models in these aspects.

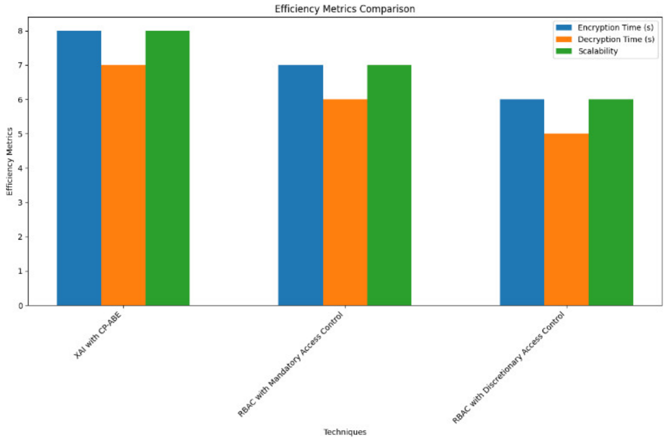


Figure 3. Efficiency Comparison of CP-ABE.

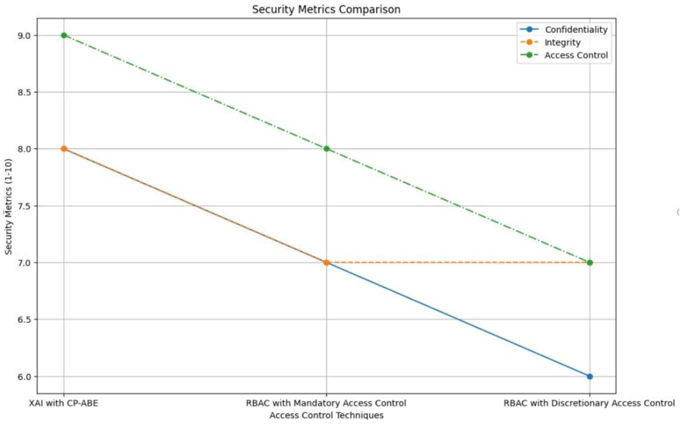


Figure 4. Security Comparison of Explainable AI with CP-ABE.

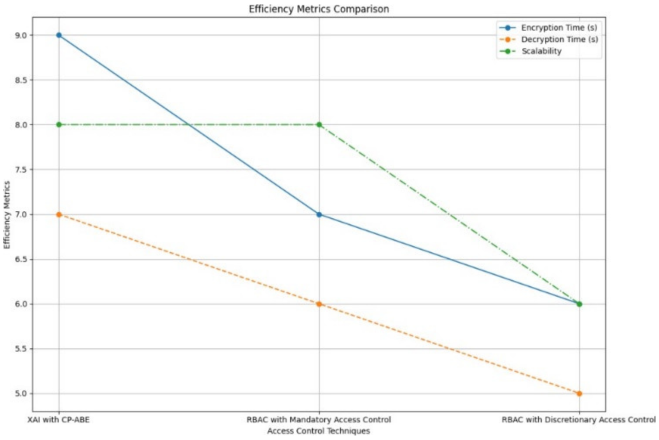


Figure 5. Efficiency Comparison of Explainable AI with CP-ABE.

IV. Dataset Collection

Clearly define the purpose of the dataset and identify the specific data attributes needed. Determine the sources of data, such as sensors or IoT devices in smart cities, ensuring accessibility and permission for data collection. Decide on the collection methods, whether manual or automated and establish the frequency of data collection. Ensure compliance with privacy laws and consider anonymizing data to protect sensitive information. Validate and clean the data to ensure accuracy and consistency. Choose suitable storage solutions, like cloud storage, and implement security measures to pro- tect the dataset from unauthorized access or breaches Label and annotate the data as needed, using appropriate tools to maintain accuracy. Document the metadata and provide clear usage guidelines, ensuring the dataset is well-prepared for future analysis or applications. The Kaggle Fall Detection dataset by Kumarkandagatla is a meticulously curated dataset designed for training and evaluating machine learning models in the context of fall detection. The dataset comprises sensor data captured from accelerometers and gyroscopes, providing time-series readings that record movements during differ- ent activities such as walking, standing, sitting, and falling. Each activity is carefully labeled, distinguishing between falls and other non-fall activities, making the dataset ideal for supervised learning applications in fall detection. This dataset offers a variety of scenarios and activities, simulating real-life conditions where falls can occur. The inclusion of data from different movements allows for the development of models that can accurately detect falls amid everyday activities. This is crucial for building reliable systems that can identify falls in diverse environments and situations. By using the Kumarkandagatla Fall Detection dataset, researchers and developers can create fall detection systems that contribute to safety and health monitoring, particularly in healthcare and elder care. These systems can improve the quality of life for at-risk individuals by providing timely alerts and assistance in the event of a fall. The KDD Cup 99 and NSL-KDD datasets are widely used for research in intrusion detection systems (IDS). The KDD Cup 99 dataset, created for the 1999 KDD Cup competition, is based on data from a DARPA dataset containing simulated network traffic. It includes a large number of records labeled as either normal or an attack, covering various types of network intrusions. However, the KDD Cup 99 dataset has been criticized for its redundancy and imbalance, leading to biased evaluation results. To address these issues, the NSL-KDD dataset was developed as an improved version. It removes duplicate records, reducing bias and making it more suitable for developing and testing IDS models. The NSL-KDD dataset is also more balanced and con- tains a more manageable number of records, facilitating more accurate and realistic performance evaluation. Both datasets have become benchmarks in the field, with the KDD Cup 99 often criticized for its shortcomings, and the NSL-KDD serving as a preferred alternative due to its enhancements. Designed for object detection, segmentation, and captioning tasks. Contains over 200,000 labeled images with 1.5 million object instances spread across 80 object categories. Widely used for training and benchmarking machine learning models due to its diverse and complex annotations. Primarily used for image classification tasks. Includes over 14 million labeled im- ages across more than 20,000 categories. Played a pivotal role in advancing deep learning, particularly through the ImageNet Large Scale Visual Recognition Challenge (ILSVRC), which spurred innovation in convolutional neural networks (CNNs).

V. Result Analysis

The decentralized nature of blockchain ensures secure key distribution and minimizes trust in a central authority. The system effectively mitigates key escrow issues and enhances data security in cloud environments. The scheme allows for efficient data sharing while concealing access policies, enhancing both security and privacy. The online/offline ap- proach significantly reduces computational overhead, making the scheme practical for real-world applications. The proposed scheme hides sensitive policies during encryption, ensuring privacy while enabling keyword searches over encrypted data. This approach is particularly useful in smart city applications where data confidentiality and accessibility are crucial. The scheme enhances privacy by concealing the access policy, making it difficult for unauthorized users to infer sensitive information. The keyword search functionality allows users to search encrypted data without revealing the keyword itself, improving the system's efficiency and security. The focus is on balancing security with practicality in large-scale smart city environments. improved security in data access and reduced risk of policy exposure, making it suitable for smart city applications. The feasibility and effectiveness of CP-ABE in securing MQTT communications in resource-constrained IoT devices. The system maintains low latency and efficient data transmission, making it practical for real-time IoT applica- tions. The non-interactive nature of the model reduces com- munication overhead, making it suitable for environments with limited bandwidth. Results highlight the model's ability to verify computations without revealing sensitive data, ensuring data privacy and security. The simulation results of executing the provided script involve the detection of objects within input images or videos using the YOLO V7 model. Upon execution, the script loads the specified model weights and processes the input data, which could be either images or video streams. Utilizing the capabilities of the YOLO V7 model, the script detects objects within the potentially saves the annotated results to designated directories. During the simulation, users can visualize the detection process in real time if the view image option is enabled. This visualization provides immediate feedback on the model's performance, displaying the input data with overlaid bounding boxes and labels. Furthermore, the script offers flexibility through various command-line options, allowing users to customize the simulation according to their requirements. These options include specifying the input data source, model weights, and output directories for saving re- sults, as well as controlling parameters like confidence thresh- olds and augmentation techniques. It highlights how advanced deep learning techniques can be effectively employed to en- hance UAV security, particularly in identifying and mitigating vulnerabilities. The study also discusses the challenges of implementing ZTA in UAV systems, such as the need for continuous authentication and the complexity of managing dynamic access controls.

It demonstrates how adversaries can manipulate inputs to deceive these XAI methods, leading to incorrect explanations and potentially bypassing the IDS. The study emphasizes the need for more resilient and secure XAI methods that can withstand adversarial attacks. The analysis shows that edge cameras often face biases in image recog- nition tasks, which can be mitigated through explainability, leading to more accurate and equitable outcomes. It also discusses the implications of these improvements for real- time surveillance and security applications. It highlights how explainability can improve the detection of sophisticated cyber threats by providing clearer insights into the decision-making process of IDS. The study also discusses the challenges of integrating XAI with cloud security, including scalability and maintaining performance without compromising security. The vulnerabilities in energy infrastructure and how explainable AI can provide actionable insights to prevent and mitigate attacks. And examines the balance between transparency and security, advocating for the careful implementation of XAI in critical energy systems.

VI. Conclusion

Enhancing secure and privacy-preserving data sharing in cloud and smart city environments using Ciphertext-Policy Attribute-Based Encryption (CP-ABE). A common theme is the integration of advanced techniques to improve key man- agement, privacy, and efficiency. The first paper explores the use of blockchain technology to decentralize and secure key management in CP-ABE, ensuring transparency and eliminat- ing single points of failure. The next two papers introduce an online/offline multi-authority CP-ABE scheme with hidden policies, which conceals sensitive attribute values, reduces computational overhead, and is geared toward practical cloud deployment. The final paper applies CP-ABE with hidden policies in smart cities, leveraging keyword search techniques to ensure secure data retrieval while protecting sensitive policy information. Together, these works contribute to the development of more secure, efficient, and privacy-aware data-sharing systems in the cloud and smart city contexts. By highlighting key advancements in enhancing security and efficiency through Ciphertext-Policy Attribute-Based Encryption (CP-ABE) in various applications. One study introduces a CP-ABE scheme that hides sensitive policies during keyword searches in smart city contexts, thereby safeguarding data confidentiality and user privacy. Another paper demonstrates the integration of CP-ABE with MQTT protocols for IoT systems using Raspberry Pi, addressing security challenges while maintaining performance in resource-constrained environments. Addition- ally, a non-interactive verifiable computation model based on CP-ABE is proposed for the perceptual layer in IoT systems, ensuring data integrity and computational efficiency without requiring constant interaction between entities. These advancements collectively contribute to strengthening security and operational effectiveness in smart cities and IoT networks. Looking ahead, future enhancements could focus on further optimizing the integration of these technologies to improve the scalability, efficiency, and accuracy of fall detection systems. This could involve exploring novel approaches for data aug- mentation, fine-tuning algorithms, and enhancing the interop- erability of edge computing solutions with other IoT devices. Additionally, ongoing research and development efforts could prioritize expanding the scope of fall detection systems to address specific challenges faced by different demographics and environments. Collaboration with healthcare professionals, caregivers, and end-users will be crucial in tailoring these sys- tems to meet the diverse needs of individuals and communities. Ultimately, the continuous advancement of technology coupled with interdisciplinary collaboration holds the potential to sig- nificantly enhance the safety and well-being of seniors and other vulnerable populations through innovative fall detection solutions. Integrating Zero Trust principles with deep learning can significantly enhance UAV security by applying rigorous access controls and continual verification of network activities, which reduces potential vulnerabilities. Post-hoc explainable AI methods in network intrusion detection can be deceived, underscoring the need for resilient AI techniques that prevent exploitation. Improvements in fairness and performance of edge cameras require advanced algorithms to ensure unbiased and accurate data processing, thereby boosting system relia- bility. Additionally, understanding cyberattack methodologies is essential for securing energy systems, as it enables the development of advanced techniques to interpret and respond to attack patterns. In the cloud environment, effective defense relies on sophisticated intrusion detection systems that can better identify and mitigate threats, ensuring robust cloud security.

References

1. Liu, S., Yu, J., Chen, L., & Chai, B. (2022). Blockchain-assisted comprehensive key management in CP-ABE for cloud-stored data. IEEE Transactions on Network and Service Management, *20*(2), 1745-1758.
2. Zhao, C., Xu, L., Li, J., Fang, H., & Zhang, Y. (2022). Toward secure and privacy-preserving cloud data sharing: Online/offline multiauthority CP-ABE with hidden policy. IEEE Systems Journal, *16*(3), 4804-4815.
3. Yi, Y., He, J., Zhu, N., Ma, X., & Luo, Y. (2022, December). A Privacy-Preserving Mechanism Based on Privacy Situation Awareness for Information Sharing in OSNs. In 2022 3rd International Conference on Electronics, Communications and Information Technology (CECIT) (pp. 285-290). IEEE.
4. Meng, F., Cheng, L., & Wang, M. (2021). Ciphertext-policy attribute- based encryption with hidden sensitive policy from keyword search techniques in smart city. EURASIP Journal on Wireless Communications and Networking, *2021*, 1-22.
5. Mendoza-Cardenas, F., Leon-Aguilar, R. S., & Quiroz-Arroyo, J. L. (2022, March). CP-ABE encryption over MQTT for an IoT system with Raspberry Pi. In 2022 56th Annual Conference on Information Sciences and Systems (CISS) (pp. 236-239). IEEE.
6. Zhao, J., Miao, W., & Zeng, Z. (2022, January). A non-interactive verifiable computation model of perceptual layer data based on CP- ABE. In *2022 2nd International Conference on Consumer Electronics and Computer Engineering (ICCECE)* (pp. 799-803). IEEE.
7. Mosteiro-Sanchez, A., Barcelo, M., Astorga, J., & Urbieta, A. (2021, June). Multi-Layered CP-ABE Scheme for Flexible Policy Update in Industry 4.0. In 2021 10th Mediterranean Conference on Embedded Computing (MECO*)* (pp. 1-4). IEEE.
8. Zhang, L., Chen, Y., & Qian, X. (2022, August). Data Confirmation Scheme based on Auditable CP-ABE. In 2022 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics) (pp. 439-443). IEEE.
9. Zhang, L., Chen, Y., & Qian, X. (2022, August). Data Confirmation Scheme based on Auditable CP-ABE. In 2022 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics) (pp. 439-443). IEEE.
10. Huang, Q. (2022, September). A CP-ABE method base on reused sub- policy. In 2022 International Conference on Cloud Computing, Big Data Applications and Software Engineering (CBASE) (pp. 168-173). IEEE.
11. Kamel, M. B., Van Oosterhout, J., Ligeti, P., & Reich, C. (2023, June). Distributed Cryptography for Lightweight Encryption in Decentralized CP-ABE. In 2023 19th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) (pp. 476-480). IEEE.
12. Wang, Q., Zhang, L., Lu, X., & Wang, K. (2022, December). A Multi-authority CP-ABE Scheme based on Cloud-Chain Fusion for SWIM. In 2022 IEEE Intl Conf on Parallel & Distributed Pro- cessing with Applications, Big Data & Cloud Computing, Sustain- able Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom) (pp. 213-219). IEEE.
13. Haque, E., Hasan, K., Ahmed, I., Alam, M. S., & Islam, T. (2024). Enhancing UAV Security Through Zero Trust Architecture: An Ad- vanced Deep Learning and Explainable AI Analysis. arXiv preprint arXiv:2403.17093.
14. Shindo, Takahiro, Taiju Watanabe, Kein Yamada, and Hiroshi Watanabe. Accuracy improvement of object detection in VVC coded video using YOLO-v7 features. In 2023 IEEE International Conference on Artificial Intelligence in Engineering and Technology (IICAIET), pp. 247-251. IEEE, 2023.
15. Wu, Y., Tang, Y., & Yang, T. (2023, February). An improved nighttime people and vehicle detection algorithm based on YOLO v7. In 2023 3rd International Conference on Neural Networks, Information and Communication Engineering (NNICE) (pp. 266-270). IEEE.
16. Wang, S. (2023, November). Environmental Target Detection Technol- ogy for Autonomous Driving Based on Improved YOLO v7. In 2023 China Automation Congress (CAC) (pp. 7621-7626). IEEE.
17. Khan, Y. A., Imaduddin, S., Ahmad, A., & Rafat, Y. (2023, January). Image-based Foreign Object Detection using YOLO v7 Algorithm for Electric Vehicle Wireless Charging Applications. In 2023 5th Interna- tional Conference on Power, Control & Embedded Systems (ICPCES) (pp. 1-6). IEEE.
18. Chen, C. C., Novianda, N. R., Guan, Y. H., Lin, Y. X., & Yen, M.H. (2023, December). A real time driving emotion detection based on yolov7 neural network. In 2023 IEEE/ACIS 8th International Conference on Big Data, Cloud Computing, and Data Science (BCD) (pp. 349-352). IEEE.

19. Senevirathna, T., Siniarski, B., Liyanage, M., & Wang, S. (2024, January). Deceiving Post-hoc Explainable AI (XAI) Methods in Network Intrusion Detection. In 2024 IEEE 21st Consumer Communications & Networking Conference (CCNC) (pp. 107-112). IEEE.
20. Nguyen, T. T. H., Nguyen, V. T. K., Cao, Q. H., Nguyen, Q. K., & Cao, H. (2024, January). Enhancing the fairness and performance of edge cameras with explainable ai. In 2024 IEEE International Conference on Consumer Electronics (ICCE) (pp. 1-4). IEEE.
21. Upadhyay, U., Kumar, A., Roy, S., Rawat, U., & Chaurasia, S. (2023, November). Defending the Cloud: Understanding the Role of Explain- able AI in Intrusion Detection Systems. In 2023 16th International Conference on Security of Information and Networks (SIN) (pp. 1-9). IEEE.
22. Paul, S., Vijayshankar, S., & Macwan, R. (2024, February). Demystify- ing Cyberattacks: Potential for Securing Energy Systems With Explain- able AI. In 2024 International Conference on Computing, Networking and Communications (ICNC) (pp. 430-434). IEEE.
23. Arreche, O., Guntur, T. R., Roberts, J. W., & Abdallah, M. (2024). E- XAI: Evaluating Black-Box Explainable AI Frameworks for Network Intrusion Detection. IEEE Access.
24. Al Masud, A., Abdullah, A. B., & Chowdhury, L. (2024, March). Explainable Models to Interpret Malware Detection Using Agnostic Method. In 2024 International Conference on Advances in Computing, Communication, Electrical, and Smart Systems (iCACCESS) (pp. 1-5). IEEE.
25. Nicodeme, C. (2020, June). Build confidence and acceptance of AI- based decision support systems-Explainable and liable AI. In *2020 13th international conference on human system interaction (HSI)* (pp. 20-23). IEEE.
26. Liu, Y., & Li, S. (2023, December). Hybrid cyber threats detection using explainable AI in Industrial IoT. In 2023 International Conference on Human-Centered Cognitive Systems (HCCS) (pp. 1-6). IEEE.
27. Tyagi, S., Pingulkar, S., & Tiwary, A. (2023, October). Detecting Diabetic Retinopathy using ResNet50 and Explainable AI. In 2023 IEEE International Carnahan Conference on Security Technology (ICCST) (pp. 1-6). IEEE.
28. Rani, J. V., Ali, H. A. S., & Jakka, A. (2023, December). IoT Network Intrusion Detection: An Explainable AI Approach in Cybersecurity. In 2023 4th International Conference on Communication, Computing and Industry 6.0 (C216) (pp. 1-6). IEEE.
29. Yan, B., Dong, A., Chai, B., Han, Y., Zhou, G., & Zhao, F. (2021). Blockchain-assisted collaborative service recommendation scheme with data sharing. IEEE Access, *9*, 40871-40883.
30. Liu, L., Wang, H., & Zhang, Y. (2019). Secure iot data outsourcing with aggregate statistics and fine-grained access control. IEEE Access, *8*, 95057-95067.
31. Sharaf, S., & Shilbayeh, N. F. (2019). A secure G-cloud-based frame- work for government healthcare services. IEEE Access, *7*, 37876-37882.
32. Sun, J., Ren, L., Wang, S., & Yao, X. (2019). Multi-keyword searchable and data verifiable attribute-based encryption scheme for cloud storage. IEEE Access, *7*, 66655-66667.
33. Malamas, V., Kotzanikolaou, P., Dasaklis, T. K., & Burmester, M. (2020). A hierarchical multi blockchain for fine grained access to medical data. IEEE Access, *8*, 134393-134412.
34. Li, H., & Han, D. (2019). EduRSS: A blockchain-based educational records secure storage and sharing scheme. IEEE access, *7*, 179273- 179289.
35. Wang, Q., Peng, L., Xiong, H., Sun, J., & Qin, Z. (2017). Ciphertext- policy attribute-based encryption with delegated equality test in cloud computing. IEEE Access, *6*, 760-771.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.