Anonymization and Revocation of CP-ABE Based Ring Networks

Dr. B. Ravinder Reddy[1], Desharaju Sai Satwik[2], Koushik Gurichettu[3], Venkatesh Cheerala[4]

Assistant Professor[1], Under Graduate Student[234], Department of Computer Science and Engineering, Anurag University

Abstract. In today's digital landscape, ensuring the privacy and security of user identities has become more critical than ever, given the increasing threats to data confidentiality and integrity. The project titled "Anonymization and Revocation of User Identity in CPABE-Based Ring Networks" addresses these concerns by integrating Ciphertext-Policy Attribute-Based Encryption (CPABE) into a ring network environment. This novel approach effectively hides user identities during communications, mitigating risks of unauthorized data access and preventing potential misuse of sensitive information. A key feature of this project is the implementation of a secure revocation mechanism that ensures once a user's permissions are revoked, they no longer have access to protected data, thereby strengthening the overall security framework. By combining CPABE's robust access control with the anonymity provided by ring signatures, the project establishes a solution that guarantees both privacy preservation and secure data access control in networked environments. The successful integration of anonymization and secure revocation into CPABE-based systems represents a significant contribution to the field of secure communication networks, offering a reliable method for safeguarding user identities and maintaining data integrity. This approach can greatly enhance the security and privacy aspects of digital communications in a world where privacy breaches are increasingly prevalent.

1 INTRODUCTION

In healthcare systems, the confidentiality and privacy of sensitive medical records are critical concerns. Patient data, including diagnoses, treatments, medications, and personal identifiers, must be protected to prevent unauthorized access and ensure patient trust. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is an encryption technique that provides a flexible and robust means of enforcing access control policies based on user attributes. In CP-ABE, access to encrypted data is granted only to those users whose attributes satisfy specific policy conditions defined by the data owner. However, while CP-ABE effectively addresses access control, it does not inherently preserve the anonymity of the users accessing the data, which may be a significant concern in healthcare scenarios. For instance, a healthcare worker accessing sensitive patient information may need to remain anonymous, especially in situations where privacy violations could result in serious legal or ethical consequences.

To overcome this limitation, a combination of CP-ABE and ring signatures can be employed to protect user anonymity. Ring signatures, a cryptographic technique that allows a group member to sign a message without revealing their identity, offer an effective solution to this challenge. By incorporating ring signatures into the CP-ABE framework, it is possible to ensure that the identity of the user accessing the healthcare data remains concealed, while still ensuring that the access control policies based on attributes are enforced. This hybrid solution enables healthcare systems to balance the need for stringent access control with the need for protecting the identities of authorized users.

The proposed system integrates these two cryptographic techniques—CP-ABE for defining and enforcing access policies based on user attributes, and ring signatures for preserving the anonymity of users. This solution is implemented using the Charm-crypto library, which provides a cryptographic framework for implementing elliptic curve-based operations. By leveraging elliptic curve cryptography, the system can perform encryption and decryption operations efficiently, ensuring fast processing times even in large-scale healthcare environments. The use of elliptic curve cryptography also enhances the security of the system, as elliptic curve-based algorithms offer strong security guarantees with relatively small key sizes, which helps improve overall system efficiency.

To evaluate the effectiveness of the proposed solution, we implement the system on healthcare datasets and perform an extensive analysis of its performance in terms of key generation, encryption, and decryption times. The evaluation demonstrates that the hybrid CP-ABE and ring signature approach not only provides robust access control and privacy preservation but also performs well in terms of computational efficiency. This

makes the system viable for real-world applications in healthcare environments where both data security and user privacy are paramount. By using this combined approach, healthcare organizations can secure sensitive patient data while ensuring that authorized users can access the data without exposing their identities. This method significantly contributes to advancing privacy-preserving techniques in healthcare data management systems, which are essential for the growing need for secure and anonymous data sharing.

2 LITERATURE

The 2007 paper by Bethencourt, Sahai, and Waters, titled Ciphertext-Policy Attribute-Based Encryption (CP-ABE), introduces a cryptographic technique that enables flexible, policy-based control over access to encrypted data. Unlike traditional encryption schemes that rely on direct key exchange between sender and receiver, CP-ABE allows data owners to encrypt information based on an "access policy." This access policy, expressed as a logical combination of attributes (e.g., roles, department names), determines who can decrypt the data. In essence, the data owner defines the access criteria, and only users possessing the required attributes in their cryptographic keys can decrypt the data.

2.1 Key Concepts and Mechanism

CP-ABE is part of the broader Attribute-Based Encryption (ABE) family. In ABE, each user is associated with a set of attributes, and keys are generated based on those attributes. However, CP-ABE flips the traditional model by embedding the access policy directly into the ciphertext, while user keys are associated with attributes. This separation offers two advantages:

1. Fine-Grained Access Control

Access to data can be flexibly restricted to only those users who meet the specified attribute-based criteria. For example, in a medical records system, access can be limited to users with attributes such as "Doctor," "Nurse," and "Emergency Access."

2. Policy Flexibility

Policies are expressed using logical operators (e.g., AND, OR, threshold gates) over attributes, making it easy to define complex conditions for access.

2.2 The Process of CP-ABE

The encryption process in CP-ABE consists of four main steps:

1. *Setup*

A central authority generates a master public key and a master private key. These keys are used in later stages to generate user-specific keys and to encrypt data.

2. Key Generation

For each user, the authority issues a private key based on the user's attributes. Each private key is tied to a set of attributes relevant to the user, like "Role: Researcher" or "Department: HR."

3. Encryption

The data owner specifies an access policy based on attributes and encrypts the data using the public key, embedding the policy in the ciphertext. For example, a policy might state that only users with attributes "Department: Finance" AND "Role: Manager" can access the data.

4. Decryption

When a user attempts to access the encrypted data, their attributes (encoded in their private key) are checked against the policy embedded in the ciphertext. If the user's attributes satisfy the policy, decryption proceeds; otherwise, access is denied.

5. Applications and Advantages

CP-ABE is particularly valuable in scenarios where centralized control over users is impractical, such as cloud storage, IoT environments, and large, decentralized organizations. It provides scalable access control without the need for a continuous exchange of encryption keys.

2.3 Challenges and Limitations

While CP-ABE offers powerful access control, challenges remain. Key revocation is difficult to manage since user keys are tied to attributes rather than unique identities. Additionally, as access policies become complex, the computational load of encryption and decryption increases, potentially impacting system performance.

In conclusion, CP-ABE represents a significant advancement in cryptographic access control, balancing flexibility, security, and scalability. The technique allows data owners to manage access to sensitive information in a highly customizable way, suiting diverse applications across sectors that require secure, attribute-based access.

3 PRELIMINARIES

3.1 Pairing based Cryptography

Pairing-Based Cryptography (PBC) is a cryptographic technique that utilizes mathematical pairings, specifically bilinear maps, to enable efficient and secure cryptographic protocols. A pairing is a bilinear map

$Q \in G$

$$e : G_1 \times G_2 \rightarrow G_T$$

, where G_1, G_2, and G_T are groups of points on elliptic curves

The bilinearity property means that for any points P and Q , and any integers a,b the pairing satisfies

$$e(aP, bQ) = e(P, Q)^{\{a\ b\}}$$

This property makes PBC especially useful for advanced cryptographic tasks such as:

Identity-Based Encryption (IBE): This allows the public key to be derived from a`n identity (e.g., email address), eliminating the need for a traditional public-key infrastructure.

Attribute-Based Encryption (ABE): Enables fine-grained access control, where users can decrypt data if they satisfy specific attribute-based policies.

Group Signatures: Allows a group of users to sign messages without revealing the identity of the signer.

Secure Multi-party Computation: Facilitates the computation of a function over inputs from multiple parties without revealing those inputs.

The strength of pairing-based cryptography lies in its reliance on the difficulty of problems such as the Discrete Logarithm Problem (DLP) and the Computational Diffie-Hellman Problem (CDHP) on elliptic curves. These problems are believed to be hard and form the security basis for many PBC protocols.

For efficient PBC, the choice of elliptic curve is critical. Curves that are pairing-friendly—meaning they allow efficient pairing computations—are typically used. These curves, such as Barreto-Naehrig (BN) and Barreto-Lynn-Scott (BLS) curves, are chosen because they have specific properties that optimize pairing computations, like a small embedding degree, which is the number of times the group order needs to be embedded into a larger field.

Pairing-based cryptography has become a significant tool for modern cryptographic systems, especially in scenarios where sophisticated encryption and access control are necessary. However, while it provides powerful cryptographic capabilities, the efficiency and security depend heavily on the selection of appropriate elliptic curves and the proper implementation of the pairing operations.

3.2 Bilinear maps

A bilinear pairing is a mathematical map defined between two groups, typically elliptic curve groups, that satisfies specific properties essential for cryptographic applications. Formally, a bilinear pairing is a map

$$e : G_1 \times G_2 \rightarrow G_T$$

are groups defined over elliptic curves, and the map itself is bilinear. This means that it is linear in each argument; for any scalars a and b, and any elements

$$P \in G_1,$$

$$Q \in G_2$$

The map satisfies $e(aP, bQ) = e(P, Q)^{\{a\,b\}}$

The bilinearity property is important because it allows the pairing to link the group elements in a way that makes cryptographic protocols, like identity-based encryption and attribute-based encryption, possible.

In addition to being bilinear, the pairing must also be non-degenerate, meaning that there exist points

$$P \in G_1,$$

$$Q \in G_2$$

This ensures that the pairing is useful for distinguishing different elements in the groups and forms the basis for constructing cryptographic schemes that rely on it for security.

A key feature of bilinear pairings in cryptography is that they allow for more complex and flexible cryptographic constructions than traditional cryptography, enabling secure key exchange, data encryption, and digital signatures without the need for a central trusted authority. For example, in identity-based encryption, public keys can be derived from user identities, reducing the need for a traditional public key infrastructure. These properties make bilinear pairings central to modern cryptographic systems, as they enable new functionalities and enhance security, particularly in systems that require fine-grained access control, multi-party computation.

The Tate pairing is a bilinear map defined on elliptic curves that takes two elements, one from each of two groups G1 and G2, and maps them to a third group GT. It is bilinear, meaning it satisfies the property

$$e(aP, bQ) = e(P, Q)^{\{a\ b\}}$$

for all scalars a,b and points $P \in G1$, $Q \in G2$. The pairing is non-degenerate, ensuring that it can distinguish different elements in the groups, which is crucial for its cryptographic applications. Efficient computation of the Tate pairing makes it suitable for various cryptographic protocols, such as identity-based encryption (IBE) and attribute-based encryption (ABE), where its bilinearity allows for key management and fine-grained access control. Its efficiency and non-degeneracy make it an essential tool in secure communication systems, enabling constructions like short signatures and secure multi-party computation. The Tate pairing serves as a foundation for more advanced pairings, such as the Ate pairing, which optimizes it for specific types of elliptic curves

3.3 Attribute based access control (ABAC)

Attribute-Based Access Control (ABAC) is an advanced and dynamic model for controlling access to resources based on attributes associated with users, resources, and the context of the access request. Unlike traditional models that rely on roles or fixed permissions, ABAC offers more flexibility by allowing access decisions to be based on a combination of attributes, such as a user's department, role, clearance level, or the time of day. ABAC is typically implemented through two main models: Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and Key-Policy Attribute-Based Encryption (KP-ABE), each addressing different aspects of data security. CP-ABE has gained significant attention in secure data access and encryption systems because it directly associates access control policies with encrypted data, making it ideal for scenarios where data confidentiality and fine-grained control are paramount. In CP-ABE, the data is encrypted with an access control policy that specifies the required attributes needed to decrypt the data. This policy, which can be defined by the data owner, is enforced on the ciphertext itself. A user’s private key is tied to a specific set of attributes, and the decryption process is only possible if the user’s attributes satisfy the conditions specified in the encryption policy. For example, in a healthcare system, a patient’s medical records may be encrypted such that only doctors with specific qualifications, such as "specialist" or "oncologist," are able to access certain records. This ensures that only users who meet the necessary criteria can access the data, maintaining privacy and preventing unauthorized access.

CP-ABE is particularly beneficial in environments where access control must be adaptable and responsive to dynamic conditions, such as in cloud storage services or distributed systems. These systems often require policies that change over time, and CP-ABE's ability to enforce policies based on attributes makes it a powerful tool for protecting sensitive data in scenarios where multiple parties with varying levels of access need to collaborate. Healthcare systems, for example, benefit from CP-ABE because it allows for secure data sharing while ensuring that patient confidentiality is upheld and only authorized personnel have access to sensitive information. The flexibility of CP-ABE also makes it highly relevant in government, finance, and corporate sectors, where access to confidential documents or financial data needs to be carefully managed and monitored. While KP-ABE also falls under the ABAC model, it differs in that the access control policy is associated with the user’s private key rather than the encrypted data itself. In KP-ABE, decryption is allowed only if the user's key attributes meet the access policy. While KP-ABE can be useful in some cases, CP-ABE’s approach of attaching the policy directly to the data itself makes it more suitable for applications where data owners want to maintain control over who accesses their encrypted information, independent of the user’s key attributes. Therefore, CP-ABE's more widespread adoption in practical applications, such as securing sensitive healthcare data, is due to its robust, flexible, and secure design that integrates easily into systems requiring fine-grained access control.

1. Cipher text attribute-based Encryption (CP-ABE)

Blockchain based CP-ABE

In data-sharing systems, especially those involving sensitive or private information, secure access control and data integrity are paramount. Traditional data-sharing models often rely on centralized servers for

storing data and controlling access, but this introduces risks related to single points of failure and potential unauthorized data exposure. To address these concerns, advanced data-sharing architectures now leverage blockchain technology combined with attribute-based cryptographic methods, creating a decentralized and highly secure framework for managing access and ensuring data integrity.

Blockchain's decentralized ledger and immutable nature provide a robust platform for logging and verifying access to data. By distributing records across multiple nodes, blockchain removes the need for a central authority and makes it difficult for any unauthorized entity to alter data records. This immutable, decentralized system not only bolsters security but also provides transparency, as every access attempt and transaction is recorded in a way that is visible to authorized parties.

Attribute-Based Signatures (ABS) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) play a critical role within this architecture, strengthening authentication and access control. ABS allows entities to authenticate and verify data based on specific attributes rather than identities, a method that maintains privacy while still ensuring that only authorized users with the required attributes can generate or verify signatures. This attribute-centric approach to authentication is particularly useful in systems where identities may need to be concealed or where user roles are defined by specific characteristics rather than individual names.

CP-ABE further enhances access control by enabling data encryption tied to predefined access policies. In CP-ABE, data is encrypted with an access structure based on attributes, allowing only users with matching attributes to decrypt and access the information. This approach enables granular access control, ensuring that data is only accessible to authorized users without requiring a central server to manage access rights. For instance, sensitive data in a financial system could be encrypted in a way that only users with particular roles or qualifications can access it, thus providing security that aligns precisely with organizational access policies.

Blockchain integration in this model ensures transparency and tamper resistance. As access records and permission logs are recorded on the blockchain, they are securely distributed and resistant to manipulation. Additionally, employing Practical Byzantine Fault Tolerance (PBFT) as the consensus mechanism allows the system to achieve secure agreement among nodes efficiently without requiring the energy-intensive proof-of-work (PoW) mechanism. PBFT ensures that the blockchain remains operational and secure even if some nodes fail or act maliciously, thereby supporting data integrity and availability.

Together, ABS, CP-ABE, and blockchain create a comprehensive, privacy-preserving, and efficient framework for secure data sharing. This integration addresses the need for strong, decentralized access control mechanisms and provides a secure alternative to centralized data management, offering both fine-grained access control and enhanced transparency in data-sharing systems.

2. Multi-Authority CP-ABE

In cloud-based data-sharing environments, ensuring data privacy and implementing effective access control mechanisms are paramount for maintaining security. While traditional encryption schemes like Ciphertext-Policy Attribute-Based Encryption (CP-ABE) have been widely used for this purpose, they come with certain limitations. CP-ABE allows data owners to define encryption policies based on user attributes, ensuring that only users whose attributes match the specified access policies can decrypt the data. This makes it an effective solution for managing fine-grained access control in scenarios like cloud storage. However, CP-ABE often struggles with issues related to efficient revocation and resistance to collusion attacks. Without proper mechanisms for revoking access, both at the user and attribute levels, there is a risk that users who should no longer have access may continue to do so. Additionally, collusion attacks, where users combine their keys to gain unauthorized access, can undermine the effectiveness of the encryption system.

A promising approach to address these challenges is the Proxy-Based and Collusion Resistant Multi-Authority Revocable CP-ABE (PCMR-CPABE) framework. This framework incorporates a proxy server to improve revocation processes and reduce the computational load typically associated with CP-ABE schemes. In PCMR-CPABE, the decryption key is divided into two components: a user-specific secret key and a proxy-generated key. This division ensures that, during decryption, only the correct combination of these keys can enable access to the data. By introducing a proxy server, the framework strengthens resistance to collusion attacks, as even if multiple users share their keys, they cannot successfully decrypt the data without the corresponding proxy key. Furthermore, in the event that a user's access is revoked, the proxy server can

invalidate the proxy key associated with that user, preventing them from decrypting any further data without the need for re-encrypting the data or updating keys for other users. This approach not only enhances security but also significantly reduces the computational burden on the cloud infrastructure.

The PCMR-CPABE framework handles two types of revocation mechanisms: user-level revocation and attribute-level revocation. In the case of user-level revocation, a revoked user loses access to all data that is encrypted under the existing attribute-based policies, making it an efficient means of controlling access when a user's permissions need to be completely removed. Attribute-level revocation, on the other hand, allows for more granular control, revoking only specific attributes while maintaining access for other users who retain the necessary attributes. This flexibility enables dynamic adjustments to access control policies without compromising the overall security or privacy of the system. Additionally, the system guarantees both forward and backward secrecy, ensuring that revoked users cannot access any past or future data that they were authorized to access.

To implement the PCMR-CPABE framework, elliptic curve cryptography (ECC) is leveraged to enhance security while maintaining computational efficiency. The Charm-Crypto library, a popular open-source library for cryptographic operations, is used to streamline the implementation of this framework. By using elliptic curve-based schemes, the system ensures that the cryptographic operations are both secure and efficient, which is crucial in cloud environments where computational resources are shared among multiple users. The proxy server plays a crucial role in offloading some of the cryptographic computations, reducing the computational load on the cloud infrastructure, and simplifying the decryption process for users. This makes the system more scalable and efficient, ensuring that it can handle large-scale cloud-based environments with a dynamic user base and frequently changing access policies.

In conclusion, the PCMR-CPABE framework offers a robust solution for secure and efficient data sharing in cloud-based environments. By combining multi-authority attribute management, collusion resistance, and proxy-based revocation, this framework addresses the critical challenges of efficient revocation, data privacy, and access control. It is a scalable and secure solution designed to meet the demands of modern, dynamic cloud computing environments, ensuring that sensitive data remains protected and accessible only to authorized users, while minimizing computational overhead. This makes it an ideal choice for securing data in a variety of cloud-based applications, from healthcare systems to enterprise data sharing platforms.

3. CP-ABE in Healthcare

In healthcare, protecting sensitive medical data such as Electronic Health Records (EHRs) is critical for patient privacy and maintaining trust in healthcare systems. Ciphertext-Policy Attribute-Based Encryption (CPABE) offers a robust solution for securing EHRs by enabling access control policies based on the attributes of users, ensuring that only authorized individuals can decrypt and access patient data. CPABE allows healthcare institutions like hospitals or clinics to define access control policies that are tied to user attributes, such as roles, credentials, or department affiliations. For example, a doctor with the proper medical license and access rights for a specific department might be granted access to a patient's records, while other individuals, such as administrative staff, may be denied access to sensitive information, ensuring that privacy is maintained.

One of the key strengths of CPABE in healthcare is its ability to enforce fine-grained access control, which is essential for protecting patient confidentiality. Unlike traditional access control mechanisms that are static and rigid, CPABE provides a flexible, dynamic framework for managing permissions. Healthcare environments are often large, complex, and constantly evolving, with numerous stakeholders involved—doctors, nurses, lab technicians, insurance agents, and patients—who require varying levels of access to different types of medical data. CPABE allows healthcare organizations to manage these permissions in real time, adjusting access policies as roles and responsibilities change, without the need for manual intervention or extensive reconfiguration of access systems. For instance, if a nurse moves to a new department or a doctor's credentials are updated, the CPABE framework can immediately adjust the data access rights according to these changes, all while ensuring that sensitive information remains protected.

Additionally, CPABE is particularly well-suited for modern healthcare systems where data sharing across multiple platforms, such as cloud-based services, is necessary. Cloud computing has revolutionized healthcare data management by enabling data to be accessible remotely to various healthcare providers, insurance companies, and patients. However, it also raises concerns about data security and unauthorized access.

CPABE addresses these challenges by encrypting data with policies that only permit access to authorized users under specific conditions. As a result, CPABE enables secure sharing of critical health information—such as diagnostic images, lab reports, treatment plans, and patient histories—across different healthcare entities, ensuring that the data remains confidential while being accessible to those who need it. In a cloud environment, where data may be accessed by multiple entities over different networks, CPABE ensures that even if data is intercepted, it remains unreadable to unauthorized parties.

Moreover, CPABE eliminates the need for traditional, centralized access control mechanisms that could potentially become single points of failure. In large, distributed healthcare organizations, centralized systems may be vulnerable to attacks or failures, but CPABE's decentralized nature provides enhanced security, as access control is distributed across the system based on user attributes. This decentralized approach improves both security and efficiency, as it reduces the reliance on a single, centralized server that could be targeted by malicious actors.

Overall, CPABE offers an ideal solution for safeguarding sensitive health information in a modern, dynamic healthcare environment. Its flexibility, scalability, and ability to enforce granular access controls make it an essential tool for maintaining the privacy and security of electronic health records, especially as healthcare data becomes more interconnected and shared across multiple platforms. By providing a secure, efficient, and flexible means of controlling access, CPABE plays a crucial role in enabling healthcare organizations to share information securely, all while maintaining stringent privacy standards that are vital to patient trust and regulatory compliance.

4 RESEARCH METHODOLOGY

This methodology provides a robust framework for securing user identities within Ciphertext-Policy Attribute-Based Encryption (CP-ABE) networks, effectively combining CP-ABE for access control with ring signatures to ensure user anonymity. In CP-ABE, data encryption is governed by attribute-based access policies, meaning that only those users who possess the appropriate set of attributes are granted the ability to decrypt the data. This ensures that sensitive information remains accessible only to authorized users based on predefined conditions, maintaining a high level of data confidentiality.

To further enhance privacy, this approach integrates ring signatures, a cryptographic technique that enables a group of users to collaboratively sign data or perform actions without disclosing their individual identities. This is particularly important in scenarios where multiple users from a trusted group need to access or process encrypted data, but individual identification is not desired. Ring signatures allow users to prove membership in a group while ensuring that no external party can distinguish the actual signer, thereby preserving anonymity.

Additionally, a crucial feature of this methodology is the incorporation of a revocation mechanism. This ensures that if a user's permissions are revoked—either due to security concerns or the user leaving the system—they can no longer access the encrypted data. The revocation process is integrated seamlessly into the CP-ABE system, ensuring that the data remains secure even as users come and go from the network. This mechanism prevents unauthorized access, even by users who may have previously been authorized but no longer hold the required attributes or permissions.

The implementation of this methodology leverages the Charm-crypto library and elliptic curve cryptography (ECC), which provide a secure and efficient foundation for the cryptographic operations involved. The Charm-crypto library supports a wide range of cryptographic protocols, making it an ideal choice for implementing CP-ABE and ring signatures. Elliptic curve cryptography, known for its efficiency and strong security properties, is used to handle the mathematical operations required by these encryption schemes.

By combining CP-ABE for precise access control, ring signatures for anonymity, and a robust revocation mechanism, this approach effectively addresses some of the key challenges in encrypted ring networks, including privacy, secure access, and user revocation. It ensures that sensitive data remains protected, accessible only to authorized users, and that users' identities are shielded, all while maintaining the flexibility required in dynamic, user-driven environments.

4.1 Ciphertext-Policy Attribute-Based Encryption (CP-ABE)

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is a powerful encryption method used to enforce access control policies based on user attributes, which is particularly useful in sensitive environments like healthcare systems. In CP-ABE, healthcare records or any sensitive data are encrypted under an access policy that defines which attributes are required for decryption. For example, an access policy might specify that only users with specific roles (e.g., doctor or nurse) and specialties (e.g., cardiology or oncology) can access the data. The access policy, in this case, would be expressed as a logical combination of attributes such as "((doctor or nurse) and (cardiology or oncology))". Only those users whose attributes satisfy this condition will be able to decrypt and access the medical records.

The setup for this system involves the generation of two essential cryptographic components by a trusted authority: a master secret key (MSK) and a public key (PK). The MSK is kept private by the trusted authority, while the public key is distributed to the users in the system. When a user joins the system, their decryption key is generated based on their specific attributes (for instance, the user's role, department, and level of access). This process ensures that each user's decryption key is tied to their attributes, enabling the system to enforce fine-grained access control. In the encryption phase, the data is encrypted under a specific access policy, meaning that only those whose attributes match the policy will have the ability to decrypt and view the data. This ensures that even if the encrypted data is accessed by unauthorized parties, it remains protected, as they cannot meet the decryption conditions.

By tying encryption to user attributes, CP-ABE enhances security by ensuring that only users with the appropriate roles, qualifications, and affiliations can access sensitive information, such as patient health records. The system also offers the flexibility to update or modify access control policies as the roles or attributes of users change, which is particularly beneficial in dynamic environments like healthcare, where staff roles and responsibilities may frequently change. This combination of attribute-based encryption and access control policies provides an efficient, scalable, and secure way to protect sensitive data while ensuring that authorized users have timely access to the information they need for effective decision-making and patient care.

4.2 Ring Signatures

Ring signatures are a cryptographic technique that enables a member of a group to sign a message on behalf of the entire group, while maintaining the anonymity of the individual signer. In the context of our system, ring signatures are employed to anonymize the identities of users who access encrypted healthcare data. When a user decrypts and accesses healthcare data, their identity is concealed, as the system only knows that a member of an authorized group (such as doctors, nurses, or medical professionals) accessed the data. However, it does not reveal which specific individual in the group performed the decryption.

The process of creating a ring signature begins by selecting a random element from the set of possible signers, such as members of the healthcare team authorized to access the data. This element is then used to generate a signature that proves the signer belongs to the authorized group, without revealing the specific identity of the individual. The signature is constructed in such a way that it's computationally infeasible to determine which member of the group created the signature, thus ensuring anonymity. The cryptographic design behind ring signatures ensures that the signer cannot later be identified, but the data can still be trusted because it has been signed by someone with the correct group membership.

In healthcare systems, where privacy is paramount, this approach is crucial. It allows healthcare professionals to access sensitive patient information in an encrypted format while preserving their anonymity. For instance, in a hospital setting, if a doctor or nurse accesses a patient's medical records, their actions are recorded through a ring signature that proves their authorization to view the data, but does not expose their personal identity. This enhances privacy and security, reducing the risk of unauthorized tracking or profiling of individuals based on their interactions with sensitive healthcare data. By combining ring signatures with CP-ABE, this solution ensures that access control policies are upheld while safeguarding user privacy and maintaining the integrity of the data.

4.3 Integration of CP-ABE and Ring Signatures

The proposed system integrates CP-ABE with ring signatures by first encrypting the data using CP-ABE based on the user's attributes, and then generating a ring signature to ensure anonymity during data access. This two-step process ensures that access control policies are enforced, and the identities of users who access the data remain anonymous.

5 THEORY AND CALCULATION

5.1 CP-ABE Calculations

1. Key Generation

For each attribute tt_i, the key generation algorithm produces a decryption key component:

$$K_{att_i} = g^{\alpha} \cdot H(att_i)^t \quad \text{.....(1)}$$

where g is a generator of an elliptic curve group, α is the master secret, and $H(att_i)^t$is a hash of the attribute.

Encryption:

To encrypt a message M, a random secret sss is chosen and the ciphertext is generated as:

$$C = (C_0 = g^s, C_1 = M \cdot e(g,g)^{\alpha s}, C_x) \quad \text{.....(2)}$$

where C_x represents components related to the attributes in the access policy.

2. Decryption

The decryption process reconstructs the secret s by using the decryption key components corresponding to the user's attributes. If the user's attributes satisfy the policy, the message M can be recovered:

$$M = \frac{C_1}{e}(C_0, K_{att_i}) \quad \text{.....(3)}$$

4.2 Ring Signature Calculations

3. Signature Generation

For a group G of users, the signer generates a ring signature by selecting a random value x and computing:

$$\sigma = (x, \{y_1, y_2, \dots, y_n\}) \quad \text{.....(4)}$$

where y_i are values computed for each member of the group. The signature ensures that the identity of the specific signer remains unknown while still proving that the signer belongs to the group.

4. Signature Verification

The verifier checks that the signature corresponds to a valid member of the group but cannot determine which member signed the message.

5. Mathematical Expressions and Symbols

CP-ABE Key Generation

The key generation for each attribute attiatt_iatti is defined by:

$$K_{att_i} = g^{\alpha} \cdot H(att_i)^t \quad \text{.....(5)}$$

where:

g is a generator of the elliptic curve group,

α is the master secret,

$H(att_i)^t$ is the hash of the attribute,

t is a randomly chosen exponent.

CP-ABE Encryption

The encryption of a message M under a specified policy is given by:

$$C = (C_0 = g^s, C_1 = M \cdot e(g,g)^{\alpha s}, C_x) \quad \text{.....(6)}$$

where:

s is a randomly selected secret,

$e(g,g)$ is the bilinear pairing function,

C_x represents the components related to the attributes specified in the access policy.

CP-ABE Decryption

The decryption process is defined by:

$$M = \frac{C_1}{e}(C_0, K_{att_i}) \quad \text{.....(7)}$$

if the user's attributes satisfy the access policy.

Ring Signature Generation

The generation of a ring signature σ\sigmaσ by a user in a group G is expressed as:

$$\sigma = (x, \{y_1, y_2, \ldots, y_n\})$$

where:

x is a randomly chosen secret,

y_i are values computed for each member of the group, ensuring anonymity for the signer.

6 RESULTS AND DISCUSSION

For the performance evaluation of the proposed system, several critical variables were utilized to assess the efficiency and effectiveness of the cryptographic operations involved. Key Generation Time is defined as the time required to generate decryption keys for users based on their attributes in the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) scheme. This metric is essential for understanding the system's responsiveness in generating keys for new users and enabling timely access control. Encryption Time refers to the time taken to encrypt healthcare data stored in a CSV file, a key factor when evaluating the scalability and performance of the system, especially in the context of large datasets. Decryption Time denotes the time required for authorized users to decrypt the encrypted data, which is a critical measure of the system's usability and efficiency in providing quick and secure access to encrypted information. Lastly, Ring Signature Overhead represents the additional computational time incurred by generating and verifying ring signatures, which are employed to preserve user anonymity. While ring signatures provide privacy benefits, this overhead must be evaluated to ensure that the anonymity feature does not significantly degrade system performance. Collectively, these variables offer a comprehensive framework for assessing the system's overall performance in terms of security, efficiency, and usability in encrypted healthcare data management.

6.1 Performance Metrics

The performance of the system was evaluated using several key metrics:

- **Key Generation Time:** The time required to generate decryption keys for users based on their attributes.
- **Encryption Time:** The time taken to encrypt healthcare data stored in a CSV file.
- **Decryption Time:** The time taken for authorized users to decrypt the encrypted data.

6.2 Evaluation Results

The results indicate that the encryption and decryption times are linearly proportional to the number of attributes involved in the access policy. The ring signature introduces a small overhead, but this is minimal compared to the overall benefits of maintaining user anonymity. The system is suitable for real-world healthcare applications, providing both privacy and security without significant computational overhead.

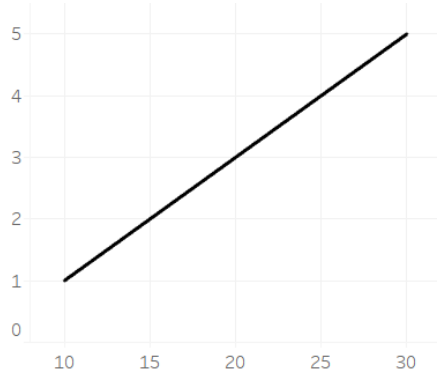

FIGURE 1 Encryption time vs number of attributes

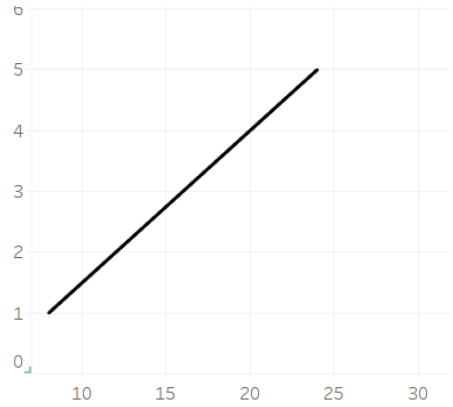

FIGURE 2 Decryption time vs number of attributes

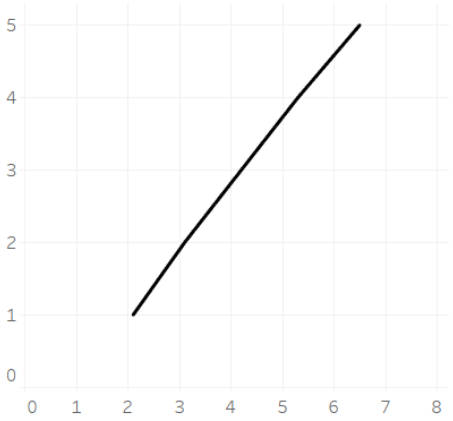

FIGURE 3 Key generation time vs number of attributes

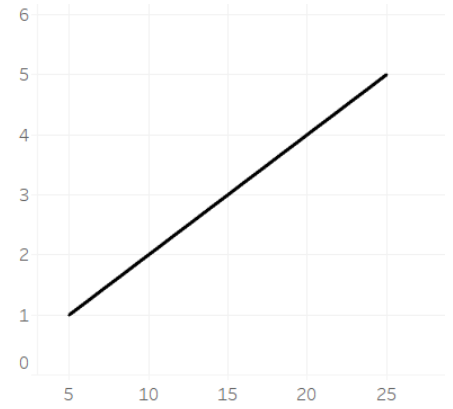

FIGURE 4 Ring signature overhead vs number of attributes

User cases and sequences

The collusion-resistant CP-ABE (Ciphertext-Policy Attribute-Based Encryption) scheme significantly improves security in cloud-based systems, particularly in sensitive domains such as e-health data management, by addressing key vulnerabilities like unauthorized data access and inadequate user revocation mechanisms. In such systems, users are granted decryption rights based on their attributes (such as role, department, or security clearance), and an access policy governs the conditions under which encrypted data can be decrypted. This model is especially useful in settings where it is essential to ensure that only authorized individuals can access protected information.

One of the major challenges in implementing CP-ABE systems is the risk of collusion attacks. In a collusion attack, users with different attributes might combine their decryption keys to circumvent access controls and gain unauthorized access to encrypted data. The CP-ABE scheme in question effectively prevents such attacks by integrating advanced mechanisms that make it computationally infeasible for unauthorized users to combine keys in a way that would bypass the access policy. This feature is crucial in environments like healthcare, where sensitive data—such as medical records—must remain protected from malicious access.

In addition to collusion resistance, the scheme incorporates accountability features that track and log user actions. This ensures that any malicious behavior or unauthorized attempts to access data can be traced back to the responsible individual. In environments like healthcare, where trust is essential, accountability mechanisms help to maintain transparency and prevent misuse of sensitive information. These mechanisms also support the auditing of data access, providing a critical layer of security for compliance with privacy regulations such as HIPAA (Health Insurance Portability and Accountability Act) or GDPR (General Data Protection Regulation).

Another essential component of this scheme is its efficient and secure revocation process. User revocation is necessary when an individual's access rights change, such as when they switch roles, leave the organization, or when a security breach occurs. Traditional CP-ABE schemes often struggle with slow or cumbersome revocation procedures, which could result in delayed data protection. The proposed scheme addresses these issues by offering a revocation mechanism that ensures unauthorized users are quickly removed from the system and can no longer decrypt data. This ensures that access control remains effective, even in dynamic environments where roles and permissions change frequently.

Moreover, the system employs privacy-preserving techniques that allow users to access encrypted data without revealing their identities. This is particularly critical in healthcare, where patient privacy is not just a legal obligation, but a moral imperative. By combining CP-ABE with privacy-preserving methods, the system allows healthcare providers to access critical patient information while maintaining confidentiality and ensuring that personal details are kept anonymous.

By integrating collusion resistance, accountability, secure revocation, and privacy preservation into a unified framework, this CP-ABE scheme offers a comprehensive and effective solution for managing sensitive data in cloud-based environments. It addresses the complex challenges of maintaining data confidentiality, enforcing access control policies, ensuring user accountability, and facilitating efficient revocation processes, all while respecting user privacy. This approach is particularly valuable in industries like healthcare, where the integrity of data security systems is crucial to ensuring the confidentiality and privacy of patient information.

REFERENCES

1. Mukiri, R. R., Kumar, B. S., & Prasad, B. V. V. (2019, February). Effective Data Collaborative Strain Using RecTree Algorithm. In *Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India*.
2. Rao, B. T., Prasad, B. V. V. S., & Peram, S. R. (2019). Elegant Energy Competent Lighting in Green Buildings Based on Energetic Power Control Using IoT Design. In *Smart Intelligent Computing and Applications: Proceedings of the Second International Conference on SCI 2018, Volume 1* (pp. 247-257). Springer Singapore.
3. Someswar, G. M., & Prasad, B. V. V. S. (2017, October). USVGM protocol with two layer architecture for efficient network management in MANET'S. In *2017 2nd International Conference on Communication and Electronics Systems (ICCES)* (pp. 738-741). IEEE.
4. Alapati, N., Prasad, B. V. V. S., Sharma, A., Kumari, G. R. P., Veeneetha, S. V., Srivalli, N., ... & Sahitya, D. (2022, November). Prediction of Flight-fare using machine learning. In *2022 International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP)* (pp. 134-138). IEEE.
5. Alapati, N., Prasad, B. V. V. S., Sharma, A., Kumari, G. R. P., Bhargavi, P. J., Alekhya, A., ... & Nandini, K. (2022, November). Cardiovascular Disease Prediction using machine learning. In *2022*

International Conference on Fourth Industrial Revolution Based Technology and Practices (ICFIRTP) (pp. 60-66). IEEE.

6. Narayana, M. S., Babu, N., Prasad, B. V. V. S., & Kumar, B. S. (2011). Clustering Categorical Data--Study of Mining Tools for Data Labeling. *International Journal of Advanced Research in Computer Science*, *2*(4).
7. Shankar, G. S., Onyema, E. M., Kavin, B. P., Gude, V., & Prasad, B. S. (2024). Breast Cancer Diagnosis Using Virtualization and Extreme Learning Algorithm Based on Deep Feed Forward Networks. *Biomedical Engineering and Computational Biology*, *15*, 11795972241278907.
8. Kulkarni, R., & Prasad, B. S. (2022). Predictive Modeling Of Heart Disease Using Artificial Intelligence. *Journal of Survey in Fisheries Sciences*, 791-801.
9. Gowda, B. M. V., Murthy, G. V. K., Upadhye, A. S., & Raghavan, R. (1996). Serotypes of Escherichia coli from pathological conditions in poultry and their antibiogram.
10. Balasubbareddy, M., Murthy, G. V. K., & Kumar, K. S. (2021). Performance evaluation of different structures of power system stabilizers. *International Journal of Electrical and Computer Engineering (IJECE)*, *11*(1), 114-123.
11. Murthy, G. V. K., & Sivanagaraju, S. (2012). S. Satyana rayana, B. Hanumantha Rao," Voltage stability index of radial distribution networks with distributed generation,". *Int. J. Electr. Eng*, *5*(6), 791-803.
12. Anuja, P. S., Kiran, V. U., Kalavathi, C., Murthy, G. N., & Kumari, G. S. (2015). Design of elliptical patch antenna with single & double U-slot for wireless applications: a comparative approach. *International Journal of Computer Science and Network Security (IJCSNS)*, *15*(2), 60.
13. Murthy, G. V. K., Sivanagaraju, S., Satyanarayana, S., & Rao, B. H. (2015). Voltage stability enhancement of distribution system using network reconfiguration in the presence of DG. *Distributed Generation & Alternative Energy Journal*, *30*(4), 37-54.
14. Reddy, C. N. K., & Murthy, G. V. (2012). Evaluation of Behavioral Security in Cloud Computing. *International Journal of Computer Science and Information Technologies*, *3*(2), 3328-3333.
15. Madhavi, M., & Murthy, G. V. (2020). Role of certifications in improving the quality of Education in Outcome Based Education. *Journal of Engineering Education Transformations*, *33*(Special Issue).
16. Varaprasad Rao, M., Srujan Raju, K., Vishnu Murthy, G., & Kavitha Rani, B. (2020). Configure and management of internet of things. In *Data Engineering and Communication Technology: Proceedings of 3rd ICDECT-2K19* (pp. 163-172). Springer Singapore.
17. Murthy, G. V. K., Suresh, C. H. V., Sowjankumar, K., & Hanumantharao, B. (2019). Impact of distributed generation on unbalanced radial distribution system. *International Journal of Scientific and Technology Research*, *8*(9), 539-542.
18. Balram, G., & Kumar, K. K. (2022). Crop field monitoring and disease detection of plants in smart agriculture using internet of things. *International Journal of Advanced Computer Science and Applications*, *13*(7).
19. Balram, G., & Kumar, K. K. (2018). Smart farming: Disease detection in crops. *Int. J. Eng. Technol*, *7*(2.7), 33-36.
20. Balram, G., Rani, G. R., Mansour, S. Y., & Jafar, A. M. (2001). Medical management of otitis media with effusion. *Kuwait Medical Journal*, *33*(4), 317-319.
21. Balram, G., Anitha, S., & Deshmukh, A. (2020, December). Utilization of renewable energy sources in generation and distribution optimization. In *IOP Conference Series: Materials Science and Engineering* (Vol. 981, No. 4, p. 042054). IOP Publishing.
22. Hnamte, V., & Balram, G. (2022). Implementation of Naive Bayes Classifier for Reducing DDoS Attacks in IoT Networks. *Journal of Algebraic Statistics*, *13*(2), 2749-2757.
23. Prasad, P. S., & Rao, S. K. M. (2017). HIASA: Hybrid improved artificial bee colony and simulated annealing based attack detection algorithm in mobile ad-hoc networks (MANETs). *Bonfring International Journal of Industrial Engineering and Management Science*, *7*(2), 01-12.
24. Prasad, PVS Siva, and S. Krishna Mohan Rao. "A Survey on Performance Analysis of ManetsUnder Security Attacks." *network* 6, no. 7 (2017).

25. Reddy, B. A., & Reddy, P. R. S. (2012). Effective data distribution techniques for multi-cloud storage in cloud computing. *CSE, Anurag Group of Institutions, Hyderabad, AP, India*.
26. Srilatha, P., Murthy, G. V., & Reddy, P. R. S. (2020). Integration of Assessment and Learning Platform in a Traditional Class Room Based Programming Course. *Journal of Engineering Education Transformations*, *33*(Special Issue).
27. Reddy, P. R. S., & Ravindranadh, K. (2019). An exploration on privacy concerned secured data sharing techniques in cloud. *International Journal of Innovative Technology and Exploring Engineering*, *9*(1), 1190-1198.
28. Reddy, P. R. S., Bhoga, U., Reddy, A. M., & Rao, P. R. (2017). OER: Open Educational Resources for Effective Content Management and Delivery. *Journal of Engineering Education Transformations*, *30*(3).
29. Madhuri, K., Viswanath, N. K., & Gayatri, P. U. (2016, November). Performance evaluation of AODV under Black hole attack in MANET using NS2. In *2016 international conference on ICT in Business Industry & Government (ICTBIG)* (pp. 1-3). IEEE.
30. Kovoor, M., Durairaj, M., Karyakarte, M. S., Hussain, M. Z., Ashraf, M., & Maguluri, L. P. (2024). Sensor-enhanced wearables and automated analytics for injury prevention in sports. *Measurement: Sensors*, *32*, 101054.
31. Rao, N. R., Kovoor, M., Kishor Kumar, G. N., & Parameswari, D. V. L. (2023). Security and privacy in smart farming: challenges and opportunities. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(7 S).
32. Madhuri, K. (2023). Security Threats and Detection Mechanisms in Machine Learning. *Handbook of Artificial Intelligence*, 255.
33. Madhuri, K. (2022). A New Level Intrusion Detection System for Node Level Drop Attacks in Wireless Sensor Network. *Journal of Algebraic Statistics*, *13*(1), 159-168.
34. DASTAGIRAIAH, D. (2024). A SYSTEM FOR ANALYSING CALL DROP DYNAMICS IN THE TELECOM INDUSTRY USING MACHINE LEARNING AND FEATURE SELECTION. *Journal of Theoretical and Applied Information Technology*, *102*(22).
35. Sukhavasi, V., Kulkarni, S., Raghavendran, V., Dastagiraiah, C., Apat, S. K., & Reddy, P. C. S. (2024). Malignancy Detection in Lung and Colon Histopathology Images by Transfer Learning with Class Selective Image Processing.
36. Sudhakar, R. V., Dastagiraiah, C., Pattem, S., & Bhukya, S. (2024). Multi-Objective Reinforcement Learning Based Algorithm for Dynamic Workflow Scheduling in Cloud Computing. *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, *12*(3), 640-649.
37. PushpaRani, K., Roja, G., Anusha, R., Dastagiraiah, C., Srilatha, B., & Manjusha, B. (2024, June). Geological Information Extraction from Satellite Imagery Using Deep Learning. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-7). IEEE.
38. Rani, K. P., Reddy, Y. S., Sreedevi, P., Dastagiraiah, C., Shekar, K., & Rao, K. S. (2024, June). Tracking The Impact of PM Poshan on Child's Nutritional Status. In *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-4). IEEE.
39. Sravan, K., Gunakar Rao, L., Ramineni, K., Rachapalli, A., & Mohmmad, S. (2023, July). Analyze the Quality of Wine Based on Machine Learning Approach. In *International Conference on Data Science and Applications* (pp. 351-360). Singapore: Springer Nature Singapore.
40. LAASSIRI, J., EL HAJJI, S. A. Ï. D., BOUHDADI, M., AOUDE, M. A., JAGADISH, H. P., LOHIT, M. K., ... & KHOLLADI, M. (2010). Specifying Behavioral Concepts by engineering language of RM-ODP. *Journal of Theoretical and Applied Information Technology*, *15*(1).
41. Ramineni, K., Harshith Reddy, K., Sai Thrikoteshwara Chary, L., Nikhil, L., & Akanksha, P. (2024, February). Designing an Intelligent Chatbot with Deep Learning: Leveraging FNN Algorithm for Conversational Agents to Improve the Chatbot Performance. In *World Conference on Artificial Intelligence: Advances and Applications* (pp. 143-151). Singapore: Springer Nature Singapore.
42. Samya, B., Archana, M., Ramana, T. V., Raju, K. B., & Ramineni, K. (2024, February). Automated Student Assignment Evaluation Based on Information Retrieval and Statistical Techniques.

In *Congress on Control, Robotics, and Mechatronics* (pp. 157-167). Singapore: Springer Nature Singapore.

43. Sekhar, P. R., & Sujatha, B. (2020, July). A literature review on feature selection using evolutionary algorithms. In *2020 7th International Conference on Smart Structures and Systems (ICSSS)* (pp. 1-8). IEEE.
44. Sekhar, P. R., & Sujatha, B. (2023). Feature extraction and independent subset generation using genetic algorithm for improved classification. *Int. J. Intell. Syst. Appl. Eng*, *11*, 503-512.
45. Sekhar, P. R., & Goud, S. (2024). Collaborative Learning Techniques in Python Programming: A Case Study with CSE Students at Anurag University. *Journal of Engineering Education Transformations*, *38*(Special Issue 1).
46. Pesaramelli, R. S., & Sujatha, B. (2024, March). Principle correlated feature extraction using differential evolution for improved classification. In *AIP Conference Proceedings* (Vol. 2919, No. 1). AIP Publishing.
47. Amarnadh, V., & Moparthi, N. R. (2023). Comprehensive review of different artificial intelligence-based methods for credit risk assessment in data science. *Intelligent Decision Technologies*, *17*(4), 1265-1282.
48. Amarnadh, V., & Moparthi, N. R. (2024). Prediction and assessment of credit risk using an adaptive Binarized spiking marine predators' neural network in financial sector. *Multimedia Tools and Applications*, *83*(16), 48761-48797.
49. Amarnadh, V., & Moparthi, N. R. (2024). Range control-based class imbalance and optimized granular elastic net regression feature selection for credit risk assessment. *Knowledge and Information Systems*, 1-30.
50. Amarnadh, V., & Akhila, M. (2019, May). RETRACTED: Big Data Analytics in E-Commerce User Interest Patterns. In *Journal of Physics: Conference Series* (Vol. 1228, No. 1, p. 012052). IOP Publishing.
51. Ravinder Reddy, B., & Anil Kumar, A. (2020). Survey on access control mechanisms in cloud environments. In *Advances in Computational Intelligence and Informatics: Proceedings of ICACII 2019* (pp. 141-149). Springer Singapore.
52. Reddy, M. B. R., Nandini, J., & Sathwik, P. S. Y. (2019). Handwritten text recognition and digital text conversion. *International Journal of Trend in Research and Development*, *3*(3), 1826-1827.
53. Reddy, B. R., & Adilakshmi, T. (2023). Proof-of-Work for Merkle based Access Tree in Patient Centric Data. *structure*, *14*(1).
54. Reddy, B. R., Adilakshmi, T., & Kumar, C. P. (2020). Access Control Methods in Cloud Enabledthe Cloud-Enabled Internet of Things. In *Managing Security Services in Heterogenous Networks* (pp. 1-17). CRC Press.
55. Reddy, M. B. R., Akhil, V., Preetham, G. S., & Poojitha, P. S. (2019). Profile Identification through Face Recognition.
56. Dutta, P. K., & Mitra, S. (2021). Application of agricultural drones and IoT to understand food supply chain during post COVID-19. *Agricultural informatics: automation using the IoT and machine learning*, 67-87.
57. Matuka, A., Asafo, S. S., Eweke, G. O., Mishra, P., Ray, S., Abotaleb, M., ... & Chowdhury, S. (2022, December). Analysing the impact of COVID-19 outbreak and economic policy uncertainty on stock markets in major affected economies. In *6th Smart Cities Symposium (SCS 2022)* (Vol. 2022, pp. 372-378). IET.
58. Saber, M., & Dutta, P. K. (2022). Uniform and Nonuniform Filter Banks Design Based on Fusion Optimization. *Fusion: Practice and Applications*, *9*(1), 29-37.
59. Mensah, G. B., & Dutta, P. K. (2024). Evaluating if Ghana's Health Institutions and Facilities Act 2011 (Act 829) Sufficiently Addresses Medical Negligence Risks from Integration of Artificial Intelligence Systems. *Mesopotamian Journal of Artificial Intelligence in Healthcare*, *2024*, 35-41.
60. Aydın, Ö., Karaarslan, E., & Gökçe Narin, N. (2023). Artificial intelligence, vr, ar and metaverse technologies for human resources management. *VR, AR and Metaverse Technologies for Human Resources Management (June 15, 2023)*.

61. Thamma, S. R. (2025). Transforming E-Commerce with Pragmatic Advertising Using Machine Learning Techniques.
62. Thamma, S. R. T. S. R. (2024). Optimization of Generative AI Costs in Multi-Agent and Multi-Cloud Systems.
63. Thamma, S. R. T. S. R. (2024). Revolutionizing Healthcare: Spatial Computing Meets Generative AI.
64. Thamma, S. R. T. S. R. (2024). Cardiovascular image analysis: AI can analyze heart images to assess cardiovascular health and identify potential risks.
65. Thamma, S. R. T. S. R. (2024). Generative AI in Graph-Based Spatial Computing: Techniques and Use Cases.
66. Harinath, D., Bandi, M., Patil, A., Murthy, M. R., & Raju, A. V. S. (2024). Enhanced Data Security and Privacy in IoT devices using Blockchain Technology and Quantum Cryptography. *Journal of Systems Engineering and Electronics (ISSN NO: 1671-1793)*, *34*(6).
67. Harinath, D., Patil, A., Bandi, M., Raju, A. V. S., Murthy, M. R., & Spandana, D. (2024). Smart Farming System–An Efficient technique by Predicting Agriculture Yields Based on Machine Learning. *Technische Sicherheit (Technical Security) Journal*, *24*(5), 82-88.
68. Masimukku, A. K., Bandi, M., Vallu, S., Patil, A., Vasundhara, K. L., & Murthy, M. R. (2025). Innovative Approaches in Diabetes Management: Leveraging Technology for Improved Healthcare Outcomes. *International Meridian Journal*, *7*(7).
69. Bandi, M., Masimukku, A. K., Vemula, R., & Vallu, S. (2024). Predictive Analytics in Healthcare: Enhancing Patient Outcomes through Data-Driven Forecasting and Decision-Making. *International Numeric Journal of Machine Learning and Robots*, *8*(8), 1-20.
70. Moreb, M., Mohammed, T. A., & Bayat, O. (2020). A novel software engineering approach toward using machine learning for improving the efficiency of health systems. *IEEE Access*, *8*, 23169-23178.
71. Ravi, P., Batta, G. S. H. N., & Yaseen, S. (2019). Toxic comment classification. *International Journal of Trend in Scientific Research and Development (IJTSRD)*.
72. Pallam, R., Konda, S. P., Manthripragada, L., & Noone, R. A. (2021). Detection of Web Attacks using Ensemble Learning. *learning*, *3*(4), 5.
73. Reddy, P. V., Ravi, P., Ganesh, D., Naidu, P. M. K., Vineeth, N., & Sameer, S. (2023, July). Detection and Evaluation of Cervical Cancer by Multiple Instance Learning. In *2023 2nd International Conference on Edge Computing and Applications (ICECAA)* (pp. 627-633). IEEE.
74. Ravi, P., Haritha, D., & Niranjan, P. (2018). A Survey: Computing Iceberg Queries. *International Journal of Engineering & Technology*, *7*(2.7), 791-793.
75. Chidambaram, R., Balamurugan, M., Senthilkumar, R., Srinivasan, T., Rajmohan, M., Karthick, R., & Abraham, S. (2013). Combining AIET with chemotherapy–lessons learnt from our experience. *J Stem Cells Regen Med*, *9*(2), 42-43.
76. Karthick, R., & Sundhararajan, M. (2014). Hardware Evaluation of Second Round SHA-3 Candidates Using FPGA. *International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)*, *2*(2).
77. Sudhan, K., Deepak, S., & Karthick, R. (2016). SUSTAINABILITY ANALYSIS OF KEVLAR AND BANANA FIBER COMPOSITE.
78. Karthick, R., Gopalakrishnan, S., & Ramesh, C. (2020). Mechanical Properties and Characterization of Palmyra Fiber and Polyester Resins Composite. *International Journal of Emerging Trends in Science & Technology*, *6*(2).
79. Karthick, R., Pandi, M., Dawood, M. S., Prabaharan, A. M., & Selvaprasanth, P. (2021). ADHAAR: A RELIABLE DATA HIDING TECHNIQUES WITH (NNP2) ALGORITHMIC APPROACH USING X-RAY IMAGES. *3C Tecnologia*, 597-608.
80. Deepa, R., Karthick, R., Velusamy, J., & Senthilkumar, R. (2025). Performance analysis of multiple-input multiple-output orthogonal frequency division multiplexing system using arithmetic optimization algorithm. *Computer Standards & Interfaces*, *92*, 103934.
81. Selvan, M. Arul, and S. Miruna Joe Amali. "RAINFALL DETECTION USING DEEP LEARNING TECHNIQUE." (2024).
82. Selvan, M. Arul. "Fire Management System For Indutrial Safety Applications." (2023).

83. Selvan, M. A. (2023). A PBL REPORT FOR CONTAINMENT ZONE ALERTING APPLICATION.
84. Selvan, M. A. (2023). CONTAINMENT ZONE ALERTING APPLICATION A PROJECT BASED LEARNING REPORT.
85. Selvan, M. A. (2021). Robust Cyber Attack Detection with Support Vector Machines: Tackling Both Established and Novel Threats.
86. Reddy, A. S., Prathap, P., Subbaiah, Y. V., Reddy, K. R., & Yi, J. (2008). Growth and physical behaviour of Zn1− xMgxO films. *Thin Solid Films*, *516*(20), 7084-7087.
87. Ambujam, S., Audhya, M., Reddy, A., & Roy, S. (2013). Cutaneous angiosarcoma of the head, neck, and face of the elderly in type 5 skin. *Journal of Cutaneous and Aesthetic Surgery*, *6*(1), 45-47.
88. Reddy, K. R., Prathap, P., Revathi, N., Reddy, A. S. N., & Miles, R. W. (2009). Mg-composition induced effects on the physical behavior of sprayed Zn1− xMgxO films. *Thin Solid Films*, *518*(4), 1275-1278.
89. Prathap, P., Reddy, A. S., Reddy, G. R., Miles, R. W., & Reddy, K. R. (2010). Characterization of novel sprayed Zn1− xMgxO films for photovoltaic application. *Solar energy materials and solar cells*, *94*(9), 1434-1436.
90. Babbar, R., Kaur, A., Vanya, Arora, R., Gupta, J. K., Wal, P., ... & Behl, T. (2024). Impact of Bioactive Compounds in the Management of Various Inflammatory Diseases. *Current Pharmaceutical Design*, *30*(24), 1880-1893.
91. Lokhande, M., Kalpanadevi, D., Kate, V., Tripathi, A. K., & Bethapudi, P. (2023). Study of Computer Vision Applications in Healthcare Industry 4.0. In *Healthcare Industry 4.0* (pp. 151-166). CRC Press.
92. Parganiha, R., Tripathi, A., Prathyusha, S., Baghel, P., Lanjhiyana, S., Lanjhiyana, S., ... & Sarkar, D. (2022). A review of plants for hepatic disorders. *J. Complement. Med. Res*, *13*(46), 10-5455.
93. Tripathi, A. K., Soni, R., & Verma, S. (2022). A review on ethnopharmacological applications, pharmacological activities, and bioactive compounds of Mimosa pudica (linn.). *Research Journal of Pharmacy and Technology*, *15*(9), 4293-4299.
94. Tripathi, A. K., Dwivedi, C. P., Bansal, P., Pradhan, D. K., Parganiha, R., & Sahu, D. An Ethnoveterinary Important Plant Terminalia Arjuna. *International Journal of Health Sciences*, (II), 10601-10607.
95. Mishra, S., Grewal, J., Wal, P., Bhivshet, G. U., Tripathi, A. K., & Walia, V. (2024). Therapeutic potential of vasopressin in the treatment of neurological disorders. *Peptides*, *174*, 171166.
96. Koliqi, R., Fathima, A., Tripathi, A. K., Sohi, N., Jesudasan, R. E., & Mahapatra, C. (2023). Innovative and Effective Machine Learning-Based Method to Analyze Alcoholic Brain Activity with Nonlinear Dynamics and Electroencephalography Data. *SN Computer Science*, *5*(1), 113.
97. Tripathi, A. K., Diwedi, P., Kumar, N., Yadav, B. K., & Rathod, D. (2022). Trigonella Foenum Grecum L. Seed (Fenugreek) Pharmacological Effects on Cardiovascular and Stress Associated Disease. *NeuroQuantology*, *20*(8), 4599.
98. Sahu, P., Sharma, G., Verma, V. S., Mishra, A., Deshmukh, N., Pandey, A., ... & Chauhan, P. (2022). Statistical optimization of microwave assisted acrylamide grafting of Linum usitatissimum Gum. *NeuroQuantology*, *20*(11), 4008.
99. Biswas, D., Sharma, G., Pandey, A., Tripathi, A. K., Pandey, A., Sahu, P., ... & Chauhan, P. (2022). Magnetic Nanosphere: Promising approach to deliver the drug to the site of action. *NeuroQuantology*, *20*(11), 4038.
100. Ramya, S., Devi, R. S., Pandian, P. S., Suguna, G., Suganya, R., & Manimozhi, N. (2023). Analyzing Big Data challenges and security issues in data privacy. *International Research Journal of Modernization in Engineering Technology and Science*, *5*(2023), 421-428.
101. Pandian, P. S., & Srinivasan, S. (2016). A Unified Model for Preprocessing and Clustering Technique for Web Usage Mining. *Journal of Multiple-Valued Logic & Soft Computing*, *26*.
102. Muthukumar, K. K. M., & Pandian, S. Analyzing and Improving the Performance of Decision Database with Enhanced Momentous Data Types. *Asia Journal of Information Technology*, *16*(9), 699-705.

103. Pandian, P. S. (2023). RETRACTED: Adopting security checks in business transactions using formal-oriented analysis processes for entrepreneurial students. *International Journal of Electrical Engineering & Education*, *60*(1_suppl), 1357-1365.
104. Karthick, R., & Pragasam, J. (2019). D "Design of Low Power MPSoC Architecture using DR Method" Asian Journal of Applied Science and Technology (AJAST) Volume 3, Issue 2.
105. Karthick, R. (2018). Deep Learning For Age Group Classification System. *International Journal Of Advances In Signal And Image Sciences*, *4*(2), 16-22.
106. Karthick, R., Akram, M., & Selvaprasanth, P. (2020). A Geographical Review: Novel Coronavirus (COVID-19) Pandemic. *A Geographical Review: Novel Coronavirus (COVID-19) Pandemic (October 16, 2020). Asian Journal of Applied Science and Technology (AJAST)(Quarterly International Journal) Volume*, *4*, 44-50.
107. Karthick, R. (2018). Integrated System For Regional Navigator And Seasons Management. *Journal of Global Research in Computer Science*, *9*(4), 11-15.
108. Kavitha, N., Soundar, K. R., Karthick, R., & Kohila, J. (2024). Automatic video captioning using tree hierarchical deep convolutional neural network and ASRNN-bi-directional LSTM. *Computing*, *106*(11), 3691-3709.
109. Selvan, M. A. (2023). INDUSTRY-SPECIFIC INTELLIGENT FIRE MANAGEMENT SYSTEM.
110. Selvan, M. Arul. "PHISHING CONTENT CLASSIFICATION USING DYNAMIC WEIGHTING AND GENETIC RANKING OPTIMIZATION ALGORITHM." (2024).
111. Selvan, M. Arul. "Innovative Approaches in Cardiovascular Disease Prediction Through Machine Learning Optimization." (2024).
112. Kumar, T. V. (2024). A Comparison of SQL and NO-SQL Database Management Systems for Unstructured Data.
113. Kumar, T. V. (2024). A Comprehensive Empirical Study Determining Practitioners' Views on Docker Development Difficulties: Stack Overflow Analysis.
114. Kumar, T. V. (2024). Developments and Uses of Generative Artificial Intelligence and Present Experimental Data on the Impact on Productivity Applying Artificial Intelligence that is Generative.
115. Kumar, T. V. (2024). A New Framework and Performance Assessment Method for Distributed Deep Neural NetworkBased Middleware for Cyberattack Detection in the Smart IoT Ecosystem.
116. Sharma, S., & Dutta, N. (2024). Examining ChatGPT's and Other Models' Potential to Improve the Security Environment using Generative AI for Cybersecurity.
117. Sharma, S., & Dutta, N. (2016). Analysing Anomaly Process Detection using Classification Methods and Negative Selection Algorithms.
118. Sakshi, S. (2023). Development of a Project Risk Management System based on Industry 4.0 Technology and its Practical Implications.
119. Arora, P., & Bhardwaj, S. (2021). Methods for Threat and Risk Assessment and Mitigation to Improve Security in the Automotive Sector. *Methods*, *8*(2).
120. Arora, P., & Bhardwaj, S. (2020). Research on Cybersecurity Issues and Solutions for Intelligent Transportation Systems.
121. Arora, P., & Bhardwaj, S. (2019). The Suitability of Different Cybersecurity Services to Stop Smart Home Attacks.
122. Arora, P., & Bhardwaj, S. (2017). A Very Safe and Effective Way to Protect Privacy in Cloud Data Storage Configurations.
123. Arora, P., & Bhardwaj, S. (2017). Investigation and Evaluation of Strategic Approaches Critically before Approving Cloud Computing Service Frameworks.
124. Arora, P., & Bhardwaj, S. (2017). Enhancing Security using Knowledge Discovery and Data Mining Methods in Cloud Computing.
125. Arora, P., & Bhardwaj, S. (2019). Safe and Dependable Intrusion Detection Method Designs Created with Artificial Intelligence Techniques. *machine learning*, *8*(7).
126. Sharma, S., & Dutta, N. (2024). Examining ChatGPT's and Other Models' Potential to Improve the Security Environment using Generative AI for Cybersecurity.

127. Sakshi, S. (2023). Development of a Project Risk Management System based on Industry 4.0 Technology and its Practical Implications.
128. Sharma, S., & Dutta, N. (2018). Development of New Smart City Applications using Blockchain Technology and Cybersecurity Utilisation. *Development*, *7*(11).
129. Sharma, S., & Dutta, N. (2017). Classification and Feature Extraction in Artificial Intelligence-based Threat Detection using Analysing Methods.
130. Sharma, S., & Dutta, N. (2017). Development of Attractive Protection through Cyberattack Moderation and Traffic Impact Analysis for Connected Automated Vehicles. *Development*, *4*(2).
131. Sharma, S., & Dutta, N. (2016). Analysing Anomaly Process Detection using Classification Methods and Negative Selection Algorithms.
132. Sharma, S., & Dutta, N. (2015). Evaluation of REST Web Service Descriptions for Graph-based Service Discovery with a Hypermedia Focus. *Evaluation*, *2*(5).
133. Sharma, S., & Dutta, N. (2015). Cybersecurity Vulnerability Management using Novel Artificial Intelligence and Machine Learning Techniques.
134. Sharma, S., & Dutta, N. (2015). Distributed DNN-based Middleware for Cyberattack Detection in the Smart IOT Ecosystem: A Novel Framework and Performance Evaluation Technique.
135. Sakshi, S. (2024). A Large-Scale Empirical Study Identifying Practitioners' Perspectives on Challenges in Docker Development: Analysis using Stack Overflow.
136. Sakshi, S. (2023). Advancements and Applications of Generative Artificial Intelligence and show the Experimental Evidence on the Productivity Effects using Generative Artificial Intelligence.
137. Bhat, S. (2024). Building Thermal Comforts with Various HVAC Systems and Optimum Conditions.
138. Bhat, S. (2020). Enhancing Data Centre Energy Efficiency with Modelling and Optimisation of End-To-End Cooling.
139. Bhat, S. (2016). Improving Data Centre Energy Efficiency with End-To-End Cooling Modelling and Optimisation.
140. Bhat, S. (2015). Deep Reinforcement Learning for Energy-Saving Thermal Comfort Management in Intelligent Structures.
141. Bhat, S. (2015). Design and Function of a Gas Turbine Range Extender for Hybrid Vehicles.
142. Bhat, S. (2023). Discovering the Attractiveness of Hydrogen-Fuelled Gas Turbines in Future Energy Systems.
143. Bhat, S. (2019). Data Centre Cooling Technology's Effect on Turbo-Mode Efficiency.
144. Bhat, S. (2018). The Impact of Data Centre Cooling Technology on Turbo-Mode Efficiency.
145. Bhat, S. (2015). Technology for Chemical Industry Mixing and Processing. *Technology*, *2*(2).
146. Bauri, K. P., & Sarkar, A. (2016). Flow and scour around vertical submerged structures. *Sādhanā*, *41*, 1039-1053.
147. Bauri, K. P., & Sarkar, A. (2020). Turbulent bursting events within equilibrium scour holes around aligned submerged cylinder. *Journal of Turbulence*, *21*(2), 53-83.
148. Bauri, K. P., & Sarkar, A. (2019). Turbulent burst-sweep events around fully submerged vertical square cylinder over plane bed. *Environmental Fluid Mechanics*, *19*, 645-666.
149. Bauri, K. P. (2022). Coherent structures around submerged circular and square cylinders due to change of orientation angle in steady current over plane bed. *Acta Geophysica*, *70*(5), 2223-2250.
150. Polamarasetti, A. (2024, November). Research developments, trends and challenges on the rise of machine learning for detection and classification of malware. In *2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC)* (pp. 1-5). IEEE.
151. Polamarasetti, A. (2024, November). Machine learning techniques analysis to Efficient resource provisioning for elastic cloud services. In *2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC)* (pp. 1-6). IEEE.
152. Polamarasetti, A. (2024, November). Role of Artificial Intelligence and Machine Learning to Enhancing Cloud Security. In *2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC)* (pp. 1-6). IEEE.

153. Gollangi, H. K., Bauskar, S. R., Madhavaram, C. R., Galla, E. P., Sunkara, J. R., & Reddy, M. S. (2020). Echoes in Pixels: The intersection of Image Processing and Sound detection through the lens of AI and Ml. *International Journal of Development Research*, *10*(08), 39735-39743.
154. Reddy, M. S., Sarisa, M., Konkimalla, S., Bauskar, S. R., Gollangi, H. K., Galla, E. P., & Rajaram, S. K. (2021). Predicting tomorrow's Ailments: How AI/ML Is Transforming Disease Forecasting. *ESP Journal of Engineering & Technology Advancements*, *1*(2), 188-200.
155. Boddapati, V. N., Sarisa, M., Reddy, M. S., Sunkara, J. R., Rajaram, S. K., Bauskar, S. R., & Polimetla, K. (2022). Data migration in the cloud database: A review of vendor solutions and challenges. *Available at SSRN 4977121*.
156. Boddapati, V. N., Sarisa, M., Reddy, M. S., Sunkara, J. R., Rajaram, S. K., Bauskar, S. R., & Polimetla, K. (2022). Data migration in the cloud database: A review of vendor solutions and challenges. *Available at SSRN 4977121*.
157. Patra, G. K., Rajaram, S. K., Boddapati, V. N., Kuraku, C., & Gollangi, H. K. (2022). Advancing Digital Payment Systems: Combining AI, Big Data, and Biometric Authentication for Enhanced Security. *International Journal of Engineering and Computer Science*, *11*(08), 10-18535.
158. Patra, G. K., Rajaram, S. K., & Boddapati, V. N. (2019). Ai And Big Data In Digital Payments: A Comprehensive Model For Secure Biometric Authentication. *Educational Administration: Theory and Practice*.
159. Boddapati, V. N., Galla, E. P., Sunkara, J. R., Bauskar, S., Patra, G. K., Kuraku, C., & Madhavaram, C. R. (2021). Harnessing the Power of Big Data: The Evolution of AI and Machine Learning in Modern Times. *ESP Journal of Engineering & Technology Advancements*, *1*(2), 134-146.
160. Singh, K., & Neeru, N. (2023). A COMPREHENSIVE STUDY OF THE IOT ATTACKS ON DIFFERENT LAYERS. *Journal Punjab Academy of Sciences*, *23*, 140-155.
161. Singh, K., & Neeru, N. (2023). A COMPREHENSIVE STUDY OF THE IOT ATTACKS ON DIFFERENT LAYERS. *Journal Punjab Academy of Sciences*, *23*, 140-155.
162. Ravi, P., Haritha, D., & Obulesh, A. (2022). Average Iceberg Queries Computation Using Bitmap Indexes On Health Care Data. *Journal of Pharmaceutical Negative Results*, 3724-3731.
163. Singh, V., Sharma, M. P., Jayapriya, K., Kumar, B. K., Chander, M. A. R. N., & Kumar, B. R. (2023). Service quality, customer satisfaction and customer loyalty: A comprehensive literature review. *Journal of Survey in Fisheries Sciences*, *10*(4S), 3457-3464.