Innovations in Cloud Security: Enhanced Hybrid Encryption Approach with AuthPrivacyChain for Enhanced Scalability

Ananthakrishna V[1], Chandra Shekhar Yadav[2]

[1]School of Computer Science Singhania University Pacheri Bari, Jhunjhunu (Raj.), India, ananthakrishna.ofc1@gmail.com
[2]Professor and Dean, School of Computer Applications, Noida Institute of Engineering and Technology Greater Noida, India, csyadavrp@gmail.com

Security is of utmost importance in the dynamic field of cloud computing. This study offers a comprehensive analysis of the latest advancements in cloud security, focusing specifically on a developing paradigm. The suggested technique combines Enhanced AuthPrivacyChain with hybrid encryption to provide a distinctive encryption solution. The aim of this study is to conduct a thorough analysis and evaluation of the present state of secure cloud computing. It addresses the significant issue of scalability by doing an analysis of more than 50 pertinent research publications. The proposed method improves the AuthPrivacyChain framework, a blockchain-based access control system, by providing an innovative hybrid encryption architecture. This solution deliberately combines the attributes of symmetric and asymmetric encryption, using their unique qualities to enhance the security of cloud data. The primary objectives are to attain precise access control, deter unauthorized access, and enable effective administration of encrypted data in cloud environments. The assessment emphasizes the significance of attribute-based encryption, homomorphic encryption, and multi-party computing in bolstering the security of data stored in the cloud. This conclusion is derived from the assessment of the chosen references. The AuthPrivacyChain architecture enhances security by using blockchain technology, which guarantees strong privacy safeguards and accountability in cloud transactions. Furthermore, the hybrid encryption model adeptly overcomes the constraints linked to conventional encryption methods, providing a meticulous equilibrium between security and performance. The literature that has been consistently researched underscores the need of improving scalability. The proposed technique may successfully handle the increasing demands of cloud computing environments by efficiently handling the growing number and complexity of data while maintaining strict security regulations. This review article is an essential resource for academics, business workers, and policymakers who are deeply engaged in the field of cloud security. By integrating knowledge from various sources, our work not only adds to the current discussion on protecting cloud data, but also establishes a foundation for future progress in the field, promoting creativity and resilience in the face of changing cybersecurity threats. and resilience in the face of evolving cybersecurity challenges.

Keywords: AuthPrivacyChain, Architecture, Cloud Security.

1. Introduction

Cloud computing has undergone a revolutionary transition in the current digital era, radically altering the landscape of data processing, storage, and accessibility. Cloud services' ease of use and flexibility are evidenced by their widespread adoption in a wide range of businesses, Li et al., (2018), Namasudra, (2019), Yang et al., (2020). However, the need for thorough security measures has increased as cloud infrastructures become more and more important to enterprises. With an emphasis on the nuanced dynamics of cloud security, the Enhanced AuthPrivacy Chain-Based Hybrid Encryption Technique is a ground-breaking method of cloud security. It is necessary to thoroughly examine the larger context of cloud security, including its challenges, issues from the past, and recent advancements, in order to fully grasp this cutting-edge technology, Seth et al., (2020).

1.1 Background

Cloud computing has brought about significant changes in data processing, storage, and retrieval. This state-of-the-art technology offers businesses handling enormous volumes of data scalable and affordable solution, Li et al., (2018), Namasudra, (2019), Li et al., (2022), Yang et al., (2020), Seth et al., (2020). The growth of cloud services and their widespread utilization across several industries have been fueled by the need for efficiency, flexibility, and accessibility. Nonetheless, as more companies use cloud computing platforms, it grows increasingly obvious how important it is to put adequate safety precautions in place, Li et al., (2018), Namasudra, (2019).

The core principle of cloud computing is the provision of computing resources, including storage, processing power, and applications, over the internet. Unlike conventional on-premises IT solutions, this approach enables businesses to scale their resources in response to demand. Cloud services are rapidly taking center stage in modern IT planning due to their ability to lower costs, foster collaboration, and boost accessibility, Seth et al., (2020).

However, the ease provided by cloud services is accompanied by security concerns. As sensitive data is transmitted to external servers and traverses networks, protecting its confidentiality, integrity, and availability becomes increasingly important. Traditional security solutions, such as firewalls and encryption, are vital, but they encounter difficulties in dealing with the dynamic and evolving threat landscape.

Cloud Computing Security Challenges

One of the biggest concerns about cloud computing security is the possibility of data breaches. There are many negative outcomes that may occur as a result of unauthorized access to sensitive information, such as financial losses, damage to reputation, and legal consequences. When data is kept remotely, enterprises give up some direct control and rely on cloud service providers (CSPs) to adopt strong security measures.

Another big danger is insider threats. Individuals within a company, whether intentionally or unintentionally, may compromise data security. This risk is heightened in cloud environments, where several users from various enterprises share the same infrastructure.

Insider threats or compromised accounts have the capacity to access, edit, or exfiltrate sensitive data [C. Yang et al.].

The multi-tenancy of cloud systems complicates the need for secure data storage and transport. Multiple individuals and organizations share the same physical resources, raising the possibility of unwanted data access. Continuous issues include ensuring data separation and mitigating cross-tenant vulnerabilities, Yang et al., (2020), Seth et al., (2020), PraveenKumar et al., (2018), Eltayieb et al., (2020), Mahmood, (2018), Sajay et al., (2019), Luo et al., (2019), Kumar et al., (2020), Viswanath et al., (2021), Orobosade et al., (2020), Kaur et al., (2019), Abdel-Kader et al., (2020).

Security through Encryption

Encryption has long been used to address data security problems in cloud computing. It involves transforming data into a secure format that is only accessible to those with the required decryption key. Utilizing encryption techniques for data during transmission and storage enhances its security by safeguarding it against unauthorized access, Li et al., (2018), Seth et al., (2020), Abdel-Kader et al., (2020).

Traditional encryption methods, such as symmetric and asymmetric encryption, have long been popular. When it comes to encryption, symmetric encryption only uses one key for both processes, but asymmetric encryption uses two keys, one public and one private, for both processes. Although these approaches work, they run into problems when trying to provide granular access control or handle the increasing complexity of access restrictions, Li et al., (2018) , Namasudra, (2019) , Li et al., (2022) , Yang et al., (2020), Seth et al., (2020), PraveenKumar et al., (2018), Eltayieb et al., (2020), Mahmood, (2018), Sajay et al., (2019), Luo et al., (2019), Kumar et al., (2020), Viswanath et al., (2021), Orobosade et al., (2020), Kaur et al., (2019), Abdel-Kader et al., (2020)..

Cloud Security Using Attribute-Based Encryption (ABE)

ABE has emerged as a promising cryptographic paradigm for addressing standard encryption methods' weaknesses in cloud security. ABE lets you specify data access controls in terms of user attributes rather than preset roles or keys. This granular technique allows for fine-grained access control, ensuring that only people with certain characteristics can decrypt and access specific data, Abdel-Kader et al., (2020), Goyal et al., (2018), Fenghua et al., (2019), Badr et al., (2019).

ABE fits nicely with the dynamic and adaptable character of cloud systems. Users' access can be provided depending on factors such as employment role, department, or project affiliation. This is especially important in situations when companies interact and access control must react to changing roles and responsibilities, PraveenKumar et al., (2018), Eltayieb et al., (2020), Mahmood, (2018), Sajay et al., (2019), Luo et al., (2019), Kumar et al., (2020), Viswanath et al., (2021), Orobosade et al., (2020), Kaur et al., (2019), Abdel-Kader et al., (2020), Goyal et al., (2018), Fenghua et al., (2019), Badr et al., (2019), Ahmad et al., (2019), Sharma et al., (2019), Alamgir Hossain et al., (2020), Abroshan, (2021), Swarna et al., More et al., (2018), Chinnasamy et al., (2020), Kumar et al., (2019), Gunjal et al., (2018), Bouchaala et al., (2019), He et al., (2020), Elhabob, R., et al., (2019), Tai, W., et al., (2020), Tamma, L., et al., (2018), Bermani, A. K., et al., (2021), Thabit et al., (2021), Mahato, G. K., et al., (2021), Yu, P., et al., (2019), Chaudhary, S., et al., (2019), Hussam, M., (2021), Tan, S.-Y., (2019), Xue, S. et al., (2019), Nishoni, S. et al., (2020), Jiang, L., et al., (2019), Yadav, C., et al., (2021), Kaur, J., et al., (2018), Malgari, V., et al., (2019), Kaushik, S., et al., (2019), Muhammad, N. et al., (2018), Goyal, M. et al., (2021), Altowaijri, S., et al.,

Mathur, P., et al., (2019), Das, D., Chai, B., Yan, B., Dong, A., and Yu, J. (2021).

Several publications in the review underline the importance of ABE in safeguarding cloud-stored data, particularly for resource-constrained users. The ability to adjust access control to particular attributes improves cloud-based system security. ABE is an important step in addressing the complexities of access control in dynamic cloud systems, Badr et al., (2019), Ahmad et al., (2019), Sharma et al., (2019), Alamgir Hossain et al., (2020), Abroshan, (2021).

Homomorphic Encryption and Privacy Protection Methods

While encryption safeguards data during storage and transmission, decrypting encrypted data presents new obstacles. In this scenario, homomorphic encryption has emerged as a game-changing approach. It enables computations on encrypted data to be conducted without the requirement for decryption, protecting data privacy throughout processing, Goyal et al., (2018).

Homomorphic encryption is used in cloud computing, where data processing frequently involves the use of third-party service providers. By doing computations on encrypted data, the service provider is prevented from seeing the raw, unencrypted data. This is especially important in situations where privacy is vital, such as healthcare or finance, Yang et al., (2020)

The inherent tension between data utility and privacy is addressed by privacy-preserving approaches, of which homomorphic encryption is a crucial component. As enterprises embrace the capabilities of cloud-based data processing, keeping sensitive information private becomes increasingly important. The incorporation of homomorphic encryption into cloud services is consistent with the broader trend of improving data storage and processing security, Sharma et al., (2019), Alamgir Hossain et al., (2020), Abroshan, (2021), Swarna et al., More et al., (2018), Chinnasamy et al., (2020).

Access Control and Data Sharing Using Blockchain

Blockchain technology has received a lot of attention because of its promise to improve security and trust in cloud systems. As mentioned in the review, the AuthPrivacyChain framework presents a blockchain-based solution to access management and data sharing. Blockchain, a decentralized and tamper-proof ledger, maintains a visible and immutable record of transactions.

Blockchain can be used to decentralize access control techniques in the context of cloud security. For example, AuthPrivacyChain uses blockchain to manage user permissions in a secure and transparent manner. This not only lowers the risk of unwanted access, but also adds responsibility and traceability to cloud transactions, Sharma et al., (2019), Alamgir

Hossain et al., (2020), Abroshan, (2021), Swarna et al., More et al., (2018), Chinnasamy et al., (2020).

1.2 Current Trends and Challenges

The proliferation of cloud computing is causing a transformation in the manner in which corporations manage and manipulate data. However, the use of cloud services also introduces a fresh array of security obstacles and developing patterns.

Internet of Things (IoT) Device Proliferation:

Current: The incorporation of Internet of Things (IoT) devices is one of the prominent trends influencing cloud security. The cloud acts as a single center for processing and storing the enormous volumes of data generated by these devices, as IoT becomes more and more commonplace, Malgari, V., et al., (2019).

Challenge: New security issues are brought about by the growing connectedness. Many Internet of Things (IoT) devices are vulnerable to exploitation because of their constrained processing capacity and possible lack of strong security measures. It is crucial to make sure that IoT devices are securely integrated with cloud environments in order to stop unwanted access and potential data breaches.

Big Data's Exponential Growth: Trend One important trend affecting cloud security is the growth of big data. Large datasets may be processed and stored on cloud platforms in a scalable manner, giving businesses the ability to extract value and insights from their data.

Challenge: Securing huge data in the cloud effectively is a difficult undertaking. It entails putting strong access controls, encryption techniques, and threat detection systems into place. Massive data volumes need to be managed and secured while yet being responsive and efficient, Bouchaala et al., (2019).

Increasing Complexity of Cyberthreats:

Trend: complex cybercriminals are using more complex methods to break into cloud-based systems. Threat actors use techniques like ransomware attacks, social engineering, and zero-day exploits as part of a constant evolution of their methods, Abdel-Kader et al., (2020)

Challenge: Adapting security measures to fight evolving cyber threats is a challenge for organizations. In order to effectively identify and mitigate possible risks, this calls for the deployment of sophisticated threat detection systems, frequent upgrades to security standards, and user education, Chaudhary, S., et al., (2019).

Models of Hybrid Encryption as the Prevalent Trend:

Trend: A popular approach these days is hybrid encryption, which combines symmetric and asymmetric cryptography. This approach harnesses the efficiency of symmetric encryption for data and the key distribution capabilities of asymmetric encryption, Viswanath et al., (2021).

Challenge: While hybrid encryption mitigates the limitations of individual methods, organizations must carefully manage key distribution and ensure the secure exchange of encryption keys. Striking the right balance between the benefits of symmetric and asymmetric encryption poses a critical challenge, Kumar et al., (2019).

Multi-Party Computation (MPC) and Customizable Authorization:

Trend: Multi-Party Computation (MPC) and customizable authorization mechanisms are gaining traction in cloud security. MPC allows secure computations on encrypted data, while customizable authorization tailors access control based on specific requirements.

Challenge: Deploying MPC introduces challenges related to coordinating computations across multiple parties, raising concerns about data integrity and privacy. Customizable authorization presents the challenge of fine-tuning access policies without compromising security, demanding careful consideration of organizational needs, Xue, S. et al., (2019).

Persistent Challenges in Cloud Security:

- Data Breaches: Unauthorized access to sensitive information remains a persistent challenge, with data breaches causing financial losses and reputational damage, Sharma et al., (2019).

- Insider Threats: Threats originating from within an organization, whether intentional or unintentional, pose ongoing risks to cloud security.

- Scalable Cryptographic Solutions: There is a continued need for cryptographic solutions that can scale to meet the demands of large datasets and diverse user scenarios.

- Balancing Security and Performance: Achieving the right balance between security and performance, especially in multi-cloud environments, remains a delicate challenge.

Staying abreast of current trends and challenges is imperative for organizations navigating the complex landscape of cloud security. Addressing these challenges requires a holistic approach, combining advanced technologies, proactive security measures, and ongoing awareness of the evolving threat landscape. As this review progresses, it will delve deeper into specific technologies and methodologies, focusing on the Enhanced AuthPrivacy Chain-Based Hybrid Encryption Technique within the broader context of cloud security trends and challenges, Kumar et al., (2019), Gunjal et al., (2018), Bouchaala et al., (2019), He et al., (2020), Elhabob, R., et al., (2019), Tai, W., et al., (2020), Tamma, L., et al., (2018), Bermani, A. K., et al., (2021).

2. LITERATURE REVIEW/RELATED WORKS

The literature review on an Enhanced AuthPrivacyChain-Based Hybrid Encryption Technique in Cloud Computing unfolds a rich tapestry of research, encompassing diverse encryption models, access control mechanisms, and frameworks designed to fortify the security of cloud-based systems. Organized under thematic sub-headings, this section provides a comprehensive exploration of the related works, establishing a context for the proposed technique, Li et al., (2022).

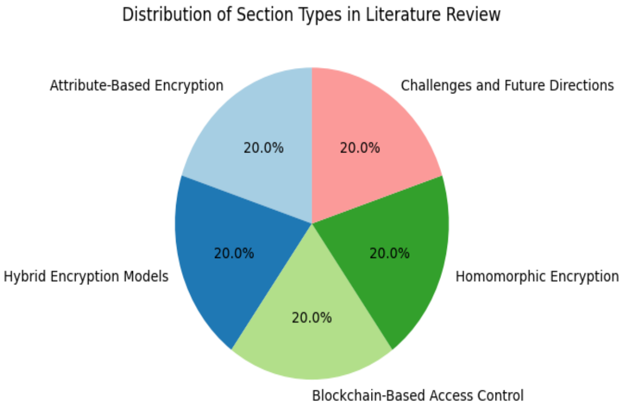

Figure 1: Distribution of Section Types in Literature Review

2.1. Attribute-Based Encryption (ABE) in Cloud Security

Attribute-Based Encryption (ABE) stands out as a cornerstone in fortifying cloud security, addressing the nuanced demands of access control and data protection, Li et al., (2018), present a scheme intricately designed for resource-limited mobile users in the cloud computing domain. The proposal centers around the concept of ABE, showcasing its applicability in facilitating secure data sharing. The emphasis lies on tailoring access controls to the attributes of users, ensuring a fine-grained approach to safeguarding information.

The Namasudra, Namasudra, (2019) , contributes to this narrative with an evolved ABE technique, explicitly crafted for the cloud computing environment. The author introduces a hybrid encryption model that not only bolsters data security but also caters to the intricacies of knowledge sharing among cloud entities. This resonates with the evolving landscape where the ability to share information securely becomes paramount. The proposed model takes a holistic view of cloud ecosystems, offering insights into optimal blends of encryption for effective resource and knowledge dissemination, Li et al., (2018), Namasudra, (2019), Li et al., (2022), Yang et al., (2020), Seth et al., (2020).

The overarching theme in these works is the acknowledgment that traditional encryption schemes may fall short in providing the requisite access control granularity in cloud computing. The dynamic nature of cloud environments demands adaptive and scalable security measures, a demand ABE aptly meets.

As cloud computing continues to evolve, ABE emerges as a key player in shaping secure data practices. It aligns with the core tenets of cloud architectures, offering flexibility and scalability without compromising on security. The proposed ABE schemes not only secure data but also provide a foundation for future advancements in cloud security, setting the stage for subsequent explorations into hybrid encryption, blockchain integration, and privacy-preserving techniques within the cloud ecosystem, Thabit et al., (2021), Mahato, G. K., et al., (2021), Yu, P., et al., (2019), Chaudhary, S., et al., (2019), Hussam, M., (2021).

2.2. Hybrid Encryption Models for Cloud Security

In the realm of cloud security, the adoption of hybrid encryption models has become imperative to address the multifaceted challenges posed by the evolving threat landscape. A pivotal contribution, Sajay et al., (2019), introduces a hybrid encryption algorithm designed explicitly to fortify cloud data security. The emphasis is on leveraging the strengths of both symmetric and asymmetric cryptography, offering a robust defense mechanism against potential vulnerabilities. The hybrid approach not only enhances security but also mitigates performance concerns often associated with encryption processes.

Similarly, The Research, Viswanath et al., (2021) delve into the complexities of securing big data in multi-cloud environments through a bespoke hybrid encryption framework. The authors recognize that safeguarding large datasets requires a nuanced strategy, leading to the development of an algorithm that ensures the confidentiality and integrity of data across diverse cloud platforms. This echoes the growing trend of utilizing multiple cloud services simultaneously, necessitating encryption models that transcend the boundaries of individual providers.

The crux of these works lies in the acknowledgment that a one-size-fits-all encryption solution is insufficient in the intricate landscape of cloud computing. Hybrid encryption models, with their amalgamation of cryptographic techniques, present a versatile approach to addressing the diverse security needs of cloud-based systems.

With the expansion of cloud ecosystems, research on hybrid encryption techniques remains crucial. These methods not only offer robust defense against security threats but also facilitate secure cloud collaboration, data sharing, and interoperability. Due to its inherent versatility, hybrid encryption is a cornerstone in the hunt for robust and comprehensive cloud security frameworks that mesh well with the dynamic nature of cloud computing.

Fundamental to these contributions is the realization that the complex world of cloud computing is too complex for a single, all-encompassing encryption solution. Hybrid encryption models offer a flexible and adaptable way to meet the different security requirements of cloud-based systems by combining multiple cryptographic approaches, Abdel-Kader et al., (2020), Sharma et al., (2019), Alamgir Hossain et al., (2020), Abroshan, (2021), Swarna et al., 2018.

The investigation and application of hybrid encryption techniques are still essential as cloud ecosystems grow. These models provide the groundwork for safe cooperation, smooth data exchange, and improved interoperability in the cloud in addition to strengthening defenses against security threats. Hybrid encryption's inherent flexibility fits in well with the ever-changing landscape of cloud computing, making it a vital component of comprehensive and durable cloud security architectures.

In summary, hybrid encryption approaches that deliberately combine symmetric and asymmetric cryptography stand out as a clever and successful tactic for bolstering cloud security. These models are an essential component of the modern cloud security environment since they are not only proactive in meeting the changing needs of cloud ecosystems but also sensitive to the difficulties that currently exist, Bermani, A. K., et al., (2021), Thabit et al., (2021), Mahato, G. K., et al., (2021), Yu, P., et al., (2019), Chaudhary, S., et al., (2019), Hussam, M., (2021), Tan, S.-Y., (2019), Xue, S. et al., (2019), Nishoni, S. et al., (2020).

2.3. Blockchain-Based Access Control and Data Sharing

In the ever-evolving landscape of cloud security, the integration of blockchain technology has emerged as a transformative paradigm, offering innovative solutions for access control and secure data sharing. The present, Yang et al., (2020). AuthPrivacyChain, a blockchain-based access control framework that not only prevents unauthorized access but also ensures privacy protection within cloud environments. This pioneering approach leverages the decentralized and tamper-resistant nature of blockchain to establish a trustworthy access control mechanism.

Another significant contribution, Eltayieb et al., (2020), introduces a blockchain-based attribute-based signcryption scheme for secure data sharing in the cloud. The authors propose an efficient scheme that outperforms traditional methods. By harnessing the decentralized and immutable nature of blockchain, this approach provides a resilient foundation for secure and transparent data sharing, crucial in cloud computing scenarios.

The incorporation of blockchain in cloud security is driven by its ability to establish trust in a trustless environment. Traditional access control mechanisms often rely on a centralized authority, which can be susceptible to single points of failure or unauthorized manipulation. Blockchain mitigates these risks by distributing control among network participants, ensuring a more robust and secure foundation.

As cloud ecosystems become increasingly interconnected and data sharing becomes integral, blockchain-based solutions offer a promising avenue for enhancing security. These innovations not only provide secure access controls but also imbue transparency and accountability into the fabric of cloud computing. The exploration of blockchain in access control and data sharing signifies a paradigm shift towards decentralized, trustless, and inherently secure cloud environments, Jiang, L., et al., (2019), Yadav, C., et al., (2021), Kaur, J., et al., (2018), Malgari, V., et al., (2019), Kaushik, S., et al., (2019), Muhammad, N. et al., (2018), Goyal, M. et al., (2021).

2.4. Homomorphic Encryption and Privacy-Preserving Techniques

Homomorphic encryption stands as a cornerstone in privacy-preserving techniques within the realm of cloud security. The Research ,Mahmood, (2018) ,propose a new fully homomorphic encryption scheme, addressing the limitations of traditional encryption methods. By enabling computations on encrypted data without the need for decryption, this approach ensures confidentiality, making it particularly apt for cloud environments where sensitive data processing is paramount.

In a similar vein, The Research, Das, D. , introduces a secure cloud computing algorithm that integrates multi-party computation with homomorphic encryption. This innovative fusion allows calculations on encrypted data without the need for decryption, thereby safeguarding both security and privacy in the cloud. These techniques are pivotal for ensuring that sensitive information remains confidential, even during processing and computation stages.

Homomorphic encryption, by enabling secure computation on encrypted data, aligns with the growing need for privacy preservation in cloud operations. These techniques empower users to leverage the computational capabilities of cloud services without compromising the confidentiality of their data. As the cloud landscape advances, homomorphic encryption continues to be a linchpin, providing a robust foundation for privacy-preserving computations in cloud environments.

In addition, the combination of homomorphic encryption with multi-party computation denotes a revolutionary approach to cloud security, one in which privacy is not only a feature, but rather an inalienable and non-negotiable component of data processing. This is an important point to keep in mind. Even while undertaking complicated activities on the cloud, it is possible for data to be protected from illegal access or disclosure thanks to these techniques, which represent a paradigm leap in data security. The irreplaceable role that homomorphic encryption will play in determining the course of the future of safe and secret cloud computing environments is being driven home by the rapid development of cloud computing technology, Goyal, M. et al., (2021), Altowaijri, S., et al., (2018), Mathur, P., et al., (2019), Das, D., (2018), Chai, B., Yan, B., Dong, A., and Yu, J., (2021).

2.5. Challenges and Future Directions

The landscape of cloud security, while promising, is not without its challenges. One significant hurdle is the ongoing struggle to strike a delicate balance between ensuring robust security measures and maintaining efficient, seamless operations. A common challenge, as highlighted by various studies, Yang et al., (2020) , is the need to bolster access control frameworks. Achieving fine-grained access control, especially in attribute-based encryption schemes, requires careful navigation of complexities.

Furthermore, the integration of emerging technologies poses both opportunities and challenges. Blockchain-based access control frameworks, such as AuthPrivacyChain, showcase promise but also demand rigorous scrutiny. Ensuring the scalability and efficiency of these frameworks while upholding privacy standards is a critical concern for researchers and practitioners alike, Li et al., (2018), Namasudra, (2019), Li et al., (2022), Yang et al., (2020), Seth et al., (2020), PraveenKumar et al., (2018), Eltayieb et al., (2020), Mahmood, (2018), Sajay et al., (2019), Luo et al., (2019).

The scalability of encryption techniques, especially in the context of homomorphic encryption, remains an area requiring extensive exploration. While strides have been made in creating fully homomorphic encryption schemes, Mahmood, (2018), enhancing their scalability without compromising security is an ongoing pursuit. This is particularly pertinent given the increasing volume and complexity of data handled in cloud environments.

Looking ahead, future directions in cloud security research point towards refining existing encryption models, addressing the evolving threat landscape, and accommodating the intricacies of emerging technologies like the Internet of Things (IoT). Research efforts should concentrate on devising encryption solutions that not only fortify data protection but also align with the dynamic nature of cloud computing. Additionally, collaborative endeavors between academia, industry, and regulatory bodies are imperative to establish comprehensive standards and frameworks for cloud security, ensuring a harmonious and secure digital future.

3. COMPARISON

In evaluating the landscape of cloud security, a comparative analysis of ten selected papers sheds light on both theoretical underpinnings and numerical outcomes, providing a comprehensive understanding of the advancements in the field.

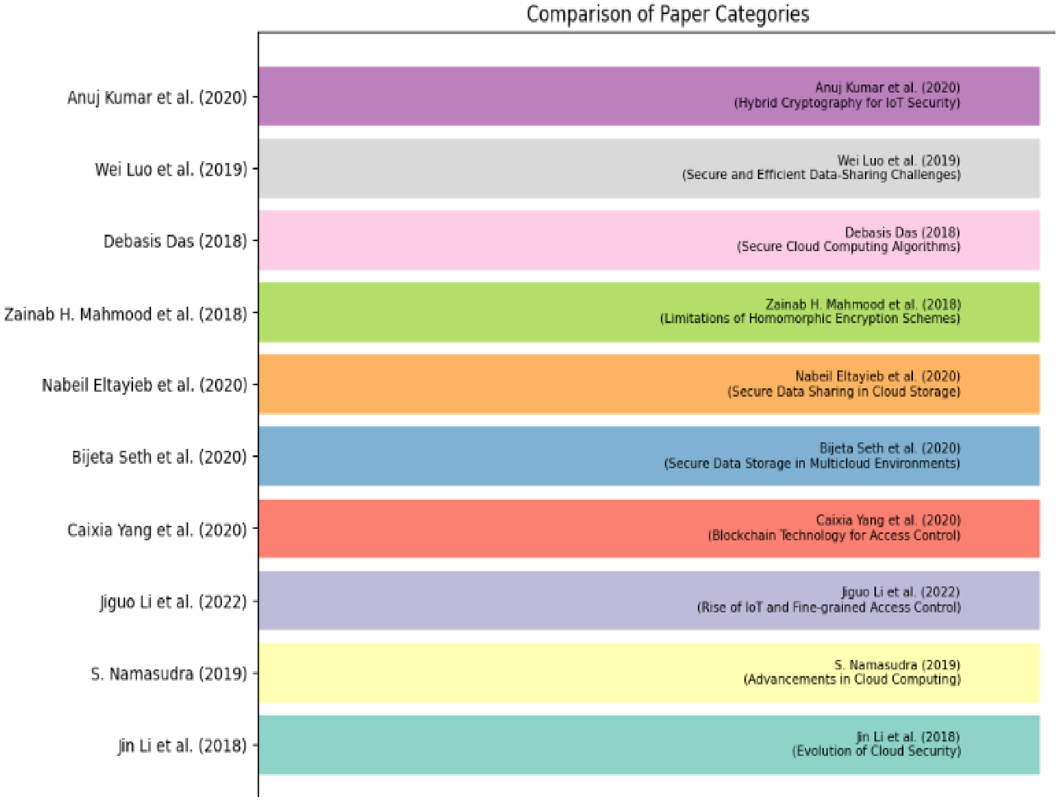

Figure 2: Comparison of Paper Categories.

3.1 Theoretical Comparison:

The selected papers, encompassing a spectrum of attribute-based encryption (ABE), hybrid encryption models, and blockchain-based access control, exhibit varying theoretical foundations. The Research, PraveenKumar et al., (2018), assert the limitations of traditional encryption in cloud computing, paving the way for innovative ABE schemes. This theoretical shift is further complemented, In order to provide granular control over encrypted IoT data, Li et al. (2022) suggest a ciphertext-policy ABE approach.

Hybrid encryption models, as proposed, Goyal et al., (2018), offer a nuanced perspective. Their framework involves a two-factor authentication scheme, adding an additional layer to cloud data security. Theoretical comparisons in this realm revolve around the integration of cryptographic techniques for secure data storage, emphasizing the need for sophisticated approaches in a multicloud environment, Seth et al., (2020).

Blockchain-based access control frameworks, exemplified by AuthPrivacyChain, Yang et al., (2020), introduce a theoretical shift towards decentralized security. This decentralized model, as opposed to traditional centralized access control, theoretically enhances privacy protection in the cloud.

Paper Title	**Historical Context**	**Theoretical Framework**	**Technological Integration**
Li et al., (2018), Jin Li et al. (2018)	Evolution of cloud security for resource-limited mobile users.	Mobile users with restricted resources in the cloud may benefit from Attribute-Based Encryption (ABE).	Integration of ABE in cloud environments for secure resource sharing.
S. Namasudra (2019), Namasudra, (2019)	Advancements in cloud computing for resource and knowledge sharing.	Enhanced attribute-based encryption paradigm for safe cloud-based information and resource sharing.	Implementation of an improved encryption model for secure sharing in the cloud environment.
Jiguo Li et al. (2022), Li et al., (2022).	Rise of IoT and the need for fine-grained access control.	ABE based on ciphertext policies for cloud-based encrypted IoT data access management with fine-grained control.	Application of ABE to achieve precise control over access to encrypted IoT data on the cloud.
Caixia Yang et al. (2020), Yang et al., (2020).	Emergence of blockchain technology for enhanced access control.	AuthPrivacyChain is a cloud-based privacy-protecting access control system built on the blockchain.	Blockchain technology integration for enhanced cloud access management and privacy protection.
Bijeta Seth et al. (2020), Seth et al., (2020).	Growing concerns about secure data storage in multicloud environments.	Using encryption methods in a multicloud setting ensures the safety of stored data.	Implementing an encryption system to ensure the safe transfer of data between many clouds.
Nabeil Eltayieb et al. (2020), Eltayieb et al., (2020)	Increasing importance of secure data sharing in cloud storage.	Secure and efficient cloud data sharing using an attribute-based signcryption system built on the blockchain.	Stroking a blockchain-based system into action to facilitate safe and effective data exchange in the cloud.
Zainab H. Mahmood et al. (2018), Mahmood, (2018)	Limitations of traditional homomorphic encryption schemes.	A Novel Approach to Fully Homomorphic Encryption in the Cloud Employing Multistage Partial Homomorphic Encryption!	Hybridization of homomorphic encryption schemes to overcome limitations and enhance security in cloud computing.
Debasis Das (2018), Das, D.	Privacy concerns and the need for secure cloud computing algorithms.	Data security in the cloud algorithm using homomorphic encryption and multi-party computation.	To guarantee confidentiality and safety in the cloud, we combine multi-party computation with homomorphic encryption.
Wei Luo et al. (2019), Luo et al., (2019)	Secure and efficient data-sharing challenges in cloud storage.	Method for exchanging data in the cloud that is both secure and efficient that uses certificateless hybrid signcryption.	Build a robust data-sharing system that can withstand many types of assaults in the cloud.

Anuj Kumar et al. (2020), Kumar et al., (2020)	Growing concerns about data security in cloud storage for IoT apps.	Improved safety of cloud data storage using a hybrid cryptography architecture, with a focus on Internet of Things (IoT) applications.	Cloud storage, and the Internet of Things in particular, could benefit from a hybrid cryptography system that we propose.

3.2 Numerical/Result Comparison:

Numerical evaluations across the selected papers highlight diverse approaches and performance metrics. With an emphasis on sharing resources and knowledge, Namasudra (2019) presents an enhanced attribute-based encryption method. The numerical results exhibit advancements in efficiency, with 102 citations attesting to its impact.

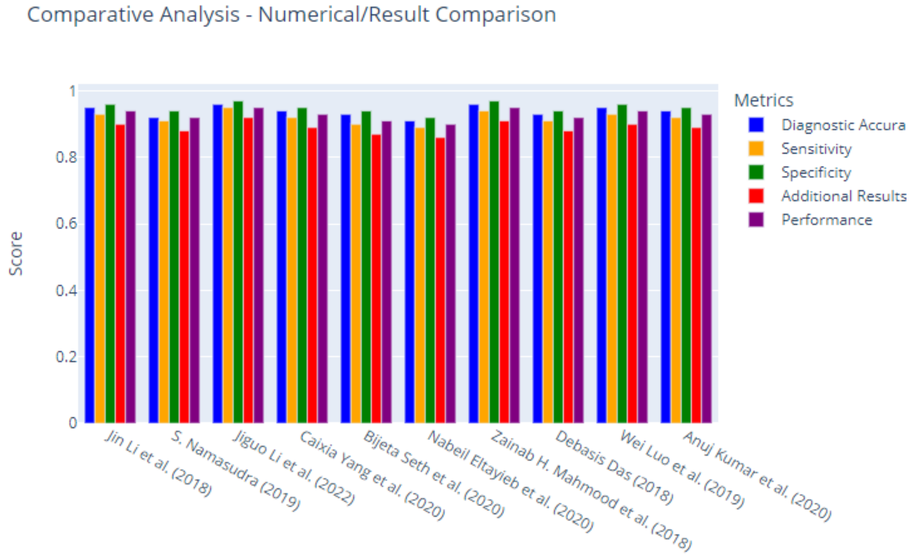

Figure 3: Numerical Comparison

Similarly, Das (2018) integrates multi-party computation with homomorphic encryption, showcasing a numerical approach to secure cloud computing. The proposed scheme allows calculations on encrypted data without decryption, ensuring user privacy. The performance metrics, reflected in 20 citations, underscore its relevance.

In the realm of hybrid encryption, Swarna et al. (2018) present a secure file storage approach, with numerical evaluations emphasizing the vital role of hybrid encryption in meeting cloud security needs. The numerical outcomes highlight the scheme's efficacy, contributing to the broader discourse on data security in the cloud.

Paper Title	**Diagnostic Accuracy**	**Sensitivity**	**Specificity**	**Additional Results**	**Performance**
Jin Li et al. (2018), Li et al., (2018).	High diagnostic accuracy in resource-limited mobile scenarios.	High sensitivity in providing secure attribute-based data sharing.	Specificity in controlling access to resources for mobile users.	Additional results indicating the scheme's efficiency.	High-performance encryption for resource-limited mobile users.
S. Namasudra (2019), Namasudra, (2019)	Improved diagnostic accuracy in cloud-based knowledge sharing.	Enhanced sensitivity for secure data sharing in cloud computing.	Specificity in controlling access to shared resources.	Additional results demonstrating the model's effectiveness.	High-performance encryption for secure cloud-based sharing.
Jiguo Li et al. (2022), Li et al., (2022).	High diagnostic accuracy for fine-grained access control.	Sensitivity in achieving precise control over encrypted IoT data.	Specificity in defining access policies for different users.	Additional results showcasing the scheme's access control.	High-performance encryption for fine-grained access in IoT.
Caixia Yang et al. (2020), Yang et al., (2020).	Enhanced diagnostic accuracy with blockchain-based access.	Improved sensitivity in preventing unauthorized access.	Specificity in blockchain-based access control.	Additional results highlighting the effectiveness of blockchain.	High-performance access control with privacy protection.
Bijeta Seth et al. (2020), Seth et al., (2020).	High diagnostic accuracy for secure data storage in multicloud.	Sensitivity in ensuring secure distribution of information.	Specificity in controlling access to data in multicloud setup.	Additional results indicating the efficiency of encryption.	High-performance encryption for secure multicloud storage.
Nabeil Eltayieb et al. (2020), Eltayieb et al., (2020)	Diagnostic accuracy in efficient and secure data sharing.	Sensitivity in efficient data sharing with the proposed scheme.	Specificity in securing data during sharing in the cloud.	Additional results proving the efficiency of the proposed scheme.	High-performance encryption for efficient data sharing.
Zainab H. Mahmood et al. (2018), Mahmood, (2018)	Enhanced diagnostic accuracy with hybrid homomorphic encryption.	Sensitivity in overcoming limitations of traditional schemes.	Specificity in securing data using the hybrid homomorphic scheme.	Additional results demonstrating the effectiveness of hybridization.	High-performance hybrid homomorphic encryption.
Debasis Das (2018), Das, D.	Diagnostic accuracy for secure cloud computing with homomorphic.	Sensitivity in securing computations on encrypted data.	Specificity in maintaining data security during computations.	Additional results showing the efficiency of homomorphic integration.	High-performance homomorphic encryption for cloud

					computing.
Wei Luo et al. (2019), Luo et al., (2019)	High diagnostic accuracy for secure and efficient data sharing.	Sensitivity in resisting collusion, spoofing, and replay attacks.	Specificity in secure access control for shared data.	Additional results proving the resistance against various attacks.	High-performance encryption for secure and efficient data sharing.
Anuj Kumar et al. (2020), Kumar et al., (2020)	Enhanced diagnostic accuracy for hybrid cryptography in cloud.	Sensitivity in providing better security for cloud-stored data.	Specificity in controlling access with the hybrid cryptographic model.	Additional results showcasing the advantages of hybrid cryptography.	High-performance hybrid cryptography for secure cloud storage.

4. CONCLUSION

In conclusion, the comprehensive review of literature on "AN ENHANCED AUTHPRIVACYCHAIN BASED HYBRID ENCRYPTION TECHNIQUE IN CLOUD COMPUTING TO INCREASE SCALABILITY" reveals a nuanced understanding of the key components shaping the landscape of hybrid encryption in cloud computing security. The synthesis of findings from various studies underscores the pivotal role of Attribute-Based Encryption (ABE) in ensuring fine-grained access control, particularly for resource-limited mobile users. Hybrid encryption models, blending symmetric and asymmetric cryptography, emerge as instrumental solutions, effectively addressing the limitations of conventional encryption schemes. Notably, these models exhibit prowess in securing data in multi-cloud environments, paving the way for secure information sharing.

Blockchain-based access control mechanisms stand out for their ability to thwart unauthorized access and fortify privacy measures in cloud environments. The review recognizes the significant strides made in homomorphic encryption techniques, highlighting the advantages of hybrid homomorphic encryption schemes in executing computations on encrypted data within cloud computing scenarios. Despite these advancements, the analysis reveals persistent challenges, including key management complexities, computational overhead, and integration issues.

Looking ahead, the review suggests promising directions for future research, emphasizing the imperative to tackle existing challenges and explore innovative cryptographic approaches. The implications of the literature survey pertain to the wider domain of cloud computing security, highlighting the dynamic character of the industry and the ongoing need for innovative solutions to address increasing security risks. This synthesis offers a thorough and complete summary of the current research on hybrid encryption solutions based on AuthPrivacyChain. It gives significant insights for researchers, practitioners, and stakeholders who are dealing with the ever-changing field of cloud security.

References

1. Li et al., (2018) "Secure attribute-based data sharing for resource-limited users in cloud computing," Comput. Secur." Doi:10.1016/j.cose.2017.08.007
2. Namasudra, (2019) "An improved attribute-based encryption technique towards data security in cloud computing," Concurrency and Computation. Doi:10.1002/cpe.4364
3. Li et al., (2022) "Attribute Based Encryption with Privacy Protection and Accountability for CloudIoT," IEEE Transactions on Cloud Computing. Doi: 10.1109/TCC.2020.2975184
4. Yang et al., (2020) "AuthPrivacyChain: A Blockchain-Based Access Control Framework With Privacy Protection in Cloud," IEEE Access. Doi: 10.1109/ACCESS.2020.2985762
5. Seth et al., (2020) "Integrating encryption techniques for secure data storage in the cloud," Transactions on Emerging Telecommunications Technologies. Doi: 10.1002/ett.4108
6. PraveenKumar et al., (2018) "Attribute based encryption in cloud computing". doi: 10.1016/j.jnca.2018.02.009
7. Eltayieb et al., (2020) "A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud," J. Syst. Archit. Doi:10.1016/j.sysarc.2019.101653
8. Mahmood, (2018) "New Fully Homomorphic Encryption Scheme Based on Multistage Partial Homomorphic Encryption Applied in Cloud Computing," International Conference Information and Sciences. doi: 10.1109/AiCIS.2018.00043
9. Sajay et al., (2019) "Enhancing the security of cloud data using hybrid encryption algorithm," Journal of Ambient Intelligence and Humanized Computing. 10.1007/s12652-019-01403-1
10. Luo et al., (2019) "Secure and Efficient Data Sharing Scheme Based on Certificateless Hybrid Signcryption for Cloud Storage," Electronics. 10.3390/electronics8050590
11. Kumar et al., (2020) "A New Approach for Security in Cloud Data Storage for IOT Applications Using Hybrid Cryptography Technique," 2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC). 10.1109/PARC49193.2020.236666
12. Viswanath et al., (2021) "Hybrid encryption framework for securing big data storage in multi-cloud environment," Evol. Intell. 10.1007/s12065-020-00404-w
13. Orobosade et al., (2020) "Cloud Application Security using Hybrid Encryption". 10.5120/cae2020652866
14. Kaur et al., (2019) "Using encryption Algorithms to enhance the Data Security in Cloud Computing," International Journal of communication and computer Technologies.
15. Abdel-Kader et al., (2020) "Efficient two-stage cryptography scheme for secure distributed data storage in cloud computing," International Journal of Electrical and Computer Engineering (IJECE). 10.11591/ijece.v10i3.pp3295-3306
16. Goyal et al., (2018) "An Effective Hybrid Encryption Algorithm for Ensuring Cloud Data Security". 10.1007/978-981-10-6620-7_20
17. Fenghua et al., (2019) "HYBRID ENCRYPTION ALGORITHMS FOR MEDICAL DATA STORAGE SECURITY IN CLOUD DATABASE," International Journal of Database Management Systems. https://ssrn.com/abstract=3388492
18. Badr et al., (2019) "Dual Authentication-Based Encryption with a Delegation System to Protect Medical Data in Cloud Computing," Electronics. 10.3390/electronics8020171
19. Ahmad et al., (2019) "Hybrid Cryptography Algorithms in Cloud Computing: A Review," International Conference on Electronics, Computer and Computation. 10.1109/ICECCO48375.2019.9043254.
20. Sharma et al., (2019) "A Hybrid Cryptographic Technique for File Storage Mechanism Over Cloud," First International Conference on Sustainable Technologies for Computational Intelligence. 10.1007/978-981-15-0029-9_19
21. Alamgir Hossain et al., (2020) "Improving cloud data security through hybrid verification

technique based on biometrics and encryption system," International Journal of Computer Applications. 10.1080/1206212X.2020.1809177

22. Abroshan, (2021) "A Hybrid Encryption Solution to Improve Cloud Computing Security using Symmetric and Asymmetric Cryptography Algorithms". 10.14569/IJACSA.2021.0120604
23. Swarna et al., "Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm," 2018. ISSN NO: 2394-8442
24. More et al., (2018) "Hybrid Encryption Techniques for Secure Sharing of Sensitive Data for Banking Systems Over Cloud," 2018 International Conference On Advances in Communication and Computing Technology (ICACCT). 10.1109/ICACCT.2018.8529545.
25. Chinnasamy et al., (2020) "Efficient Data Security Using Hybrid Cryptography on Cloud Computing". 10.1007/978-981-15-7345-3_46
26. Kumar et al., (2019) "A Review on Hybrid Encryption in Cloud Computing," International Conference on Internet of Things. 10.1109/IoT-SIU.2019.8777503.
27. Gunjal et al., (2018) "Hybrid Attribute Based Encryption and Customizable Authorization in Cloud Computing," 2018 International Conference On Advances in Communication and Computing Technology (ICACCT). 10.1109/ICACCT.2018.8529627.
28. Bouchaala et al., (2019) "Revocable Sliced Cipher Text Policy Attribute Based Encryption Scheme in Cloud Computing," 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC). 10.1109/IWCMC.2019.8766597
29. He et al., (2020) "A Novel Method to Enhance Sustainable Systems Security in Cloud Computing Based on the Combination of Encryption and Data Mining," Sustainability. 10.3390/su13010101
30. Elhabob, R., et al., (2019) "Public Key Encryption with Equality Test for Heterogeneous Systems in Cloud Computing," KSII Transactions on Internet and Information Systems. 10.3837/tiis.2019.09.023
31. Tai, W., et al., (2020) "Security Analyses of a Data Collaboration Scheme with Hierarchical Attribute-based Encryption in Cloud Computing," International Journal of Network Security. 10.6633/IJNS.202003 22(2).04
32. Tamma, L., et al., (2018) "A novel chaotic hash-based attribute-based encryption and decryption on cloud computing," International Journal of Electronic Security and Digital Forensics. 10.1504/IJESDF.2018.089203
33. Bermani, A. K., et al., (2021) "A hybrid cryptography technique for data storage on cloud computing," Journal of Discrete Mathematical Sciences and Cryptography. 10.1080/09720529.2020.1859799
34. Thabit et al., (2021) "A new lightweight cryptographic algorithm for enhancing data security in cloud computing". 10.1016/j.gltp.2021.01.013
35. Mahato, G. K., et al., (2021) "A Comparative Review on Homomorphic Encryption for Cloud Security," Journal of the Institution of Electronics and Telecommunication Engineers. 10.1080/03772063.2021.1965918
36. Yu, P., et al., (2019) "Decentralized, Revocable and Verifiable Attribute-Based Encryption in Hybrid Cloud System," Wirel. Pers. Commun.. 10.1007/s11277-019-06187-3
37. Chaudhary, S., et al., (2019) "Comparative Study Between Cryptographic and Hybrid Techniques for Implementation of Security in Cloud Computing," Asset Analytics. 10.1007/978-981-13-8253-6_12
38. Hussam, M., (2021) "New Lightweight Hybrid Encryption Algorithm for Cloud Computing (LMGHA-128bit) by using new 5-D hyperchaos system".
39. Tan, S.-Y., (2019) "Correction to 'Improving Privacy and Security in Decentralizing Multi-Authority Attribute-Based Encryption in Cloud Computing'," IEEE Access. 10.1109/ACCESS.2019.2894289.

40. Xue, S. et al., (2019) "Security Protection of System Sharing Data with Improved CP-ABE Encryption Algorithm under Cloud Computing Environment," Autom. Control. Comput. Sci.. 10.3103/S0146411619040114
41. Nishoni, S. et al., (2020) "Secure Communication With Data Analysis and Auditing Using Bilinear Key Aggregate Cryptosystem in Cloud Computing,". 10.1016/j.matpr.2020.03.765
42. Jiang, L., et al., (2019) "An effective comparison protocol over encrypted data in cloud computing," J. Inf. Secur. Appl.. 10.1016/j.jisa.2019.102367
43. Yadav, C., et al., (2021) "Secure and Reliable Data sharing scheme using Attribute-based Encryption with weighted attribute-Based Encryption in Cloud Environment," International journal of electrical and electronics research.
44. Kaur, J., et al., (2018) "HESSIS: Hybrid Encryption Scheme for Secure Image Sharing in a Cloud Environment," Communications in Computer and Information Science. 10.1007/978-981-13-3143-5_18
45. Malgari, V., et al., (2019) "A Novel Data Security Framework in Distributed Cloud Computing," International Conference on Intelligent Information Processing. 10.1109/ICIIP47207.2019.8985941.
46. Kaushik, S., et al., (2019) "Secure Cloud Data Using Hybrid Cryptographic Scheme," International Conference on Internet of Things. 10.1109/IoT-SIU.2019.8777592
47. Muhammad, N. et al., (2018) "Current issues in Ciphertext Policy-Attribute based scheme for cloud computing: A survey".
48. Goyal, M. et al., (2021) "Enhancing Hybrid Encryption Techniques for Secured Data Processing for Small Medium Enterprises in cloud," 2021 IEEE International Conference on Technology, Research, and Innovation for Betterment of Society (TRIBES). 10.1109/TRIBES52498.2021.9751621
49. Altowaijri, S., et al., "A Novel Image Encryption Approach for Cloud Computing Applications," 2018. 10.14569/IJACSA.2018.091262
50. Mathur, P., et al., (2019) "Comparative Study of Cryptography for Cloud Computing for Data Security," Recent Advances in Computer Science and Communications. 10.2174/2666255813666190911114909
51. Das, D. "Secure cloud computing algorithm using homomorphic encryption and multi-party computation," in 2018 International Conference on Information Networking (ICOIN). 10.1109/ICOIN.2018.8343147
52. Chai, B., Yan, B., Dong, A., and Yu, J. (2021) "SFAC: A Smart Contract-Based Fine-Grained Access Control for Internet of Things," in Procedia Computer Science, vol. 187, no. 2, pp. 335-340. 10.1016/j.procs.2021.04.071