International Journal of Engineering Research and Science & Technology

IJERST

ISSN : 2319-5991

www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2021.v17.i3.pp18-28

Vol. 17, Issue 3, 2021

Cloud-Based Attribute-Based Encryption and Big Data for Safeguarding Financial Data

Rama Krishna Mani Kanta Yalla,

AWS Developer, OQ Point LLC, Redmond, WA.

Email ID: ramakrishnayalla207@gmail.com

Abstract

The potential to improve the security of financial data in the digital era is presented by the convergence of big data analytics, cloud computing, and attribute-based encryption (ABE). Innovative solutions are essential to protecting sensitive data as the banking industry battles more complex cyber attacks. In order to strengthen the security of financial data, this article investigates the integration of ABE with big data analytics within cloud computing systems. It starts by going over the basics of ABE, such as ciphertext-policy ABE (CP-ABE) and key-policy ABE (KP-ABE), and clarifies how ABE allows for fine-grained access control over encrypted data. The paper then explores the use of ABE in cloud computing, highlighting its function in guaranteeing data scalability and confidentiality. Additionally, the integration of big data analytics with an emphasis on anomaly detection, predictive analytics, real-time transaction monitoring, and better security measures is covered in relation to financial institutions. The significance of using big data analytics to detect fraud, control risks, and adhere to legal obligations is emphasized in the article. To further illustrate the usefulness of these technologies, case studies illustrating the application of big data analytics and ABE in actual financial institutions are provided. Financial businesses can maintain legal and ethical standards while improving data security through iterative improvement and compliance verification. In summary,this article offers valuable perspectives on how ABE, cloud computing, and big data analytics may protect financial information and reduce cyber threats in the contemporary banking industry.

Keywords: Attribute-based encryption (ABE), real-time monitoring, anomaly detection, fraud detection, risk management, key policy ABE (KP-ABE), ciphertext policy ABE (CP-ABE).

1 Introduction

Attribute-based encryption (ABE), cloud computing, and big data analytics together are transforming the security of financial data. Sophisticated security measures are becoming more and more necessary for the financial industry in the digital age to safeguard confidential data. In order to address these issues, the confluence of various technologies presents encouraging

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2021.v14.i3.pp18-28

Vol. 14, Issue 3, 2021

options. According to Allioui and Mourdi (2023), there is a lot of promise for the Internet of Things (IoT) in financial management. IoT can improve data management, productivity, efficiency, and decision-making. IoT has a huge impact on both traditional and modern organizations, as demonstrated by their thorough study of 84 academic publications, which also highlights future research prospects and problems. In their analysis of the importance of blockchain technology, Dong et al. (2023) pay particular attention to aspects like security,consensus processes, and decentralization. A comprehensive synopsis of blockchain's evolution and uses is given, emphasizing how it can potentially overcome the drawbacks of traditional financial institutions and how government agencies, tech companies, and financial intermediaries are beginning to embrace it. Ometov et al. look at privacy and security concerns in Cloud, Edge, and Fog computing ecosystems (2022). Their analysis highlights the significance of strongsecurity measures to reduce risks in this heterogeneous environment by identifying the main assaults, differences, and convergences among various paradigms.

A security framework called IoTAttest is introduced by Dirin (2023) to guarantee data and device integrity in Internet of Things systems. It does this by utilizing Trusted Platform Module 2.0 and remote attestation. Evidence of the framework's efficacy in creating safe Internet of Things systems comes from proof-of-concept applications that verify its usability, scalability, extensibility, and security. Within a digital marketing framework, Cui (2023) offers an enhanced homomorphic encryption technique for categorizing internet use data. Using cutting-edge encryption methods and machine learning models, the study demonstrates the framework's effectiveness and security in focusing on certain markets and enhancing digital marketing tactics. The importance of co-produced participatory research is emphasized in Montgomery's (2022) examination of the function and experiences of peer researchers in adult safeguarding policy. The research emphasizes how important it is to collaborate more and provide more funds in order to improve the influence of this kind of study on policy formation. Australian genetic specialists' opinions about who owns patient data are examined by Malakar (2024). While stressing the necessity of a strong health system infrastructure to oversee and promote this ownership, the study finds a consensus in favor of patient ownership of genetic data.

The difficulties encountered in child protection and safeguarding procedures during the COVID-19 epidemic are examined by Driscoll (2022). The research delineates the flexible strategies utilized by experts to mitigate changing risks and sustain efficient exchange of information and cooperation. Using a case study, Lawrence (2022) examines financial elder abuse and neglect, highlighting the vital need for strong legal protections to shield vulnerable groups from these types of crimes. In order to handle expected faults with high-alert drugs in healthcare organizations, Booth (2024) creates a thorough framework of safeguarding techniques. Hospitalscan lower risks and enhance patient safety by using the framework's tools and visual aids. Lastly, an in-depth analysis of attribute-based encryption (ABE) techniques and their uses in the Internetof Things is given by Shruti Rani (2023). The report makes recommendations for future research to improve the efficacy of ABE in securing IoT environments and emphasizes the significance ofenhanced security and privacy measures in cloud and fog computing platforms.

The rising frequency of cyber threats and data breaches in the modern banking sector has made protecting sensitive data a top priority. The dynamic and intricate nature of today's cyberecosystem often proves to be too much for standard security solutions, especially for financial

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2021.v14.i3.pp18-28

Vol. 14, Issue 3, 2021

organizations handling massive volumes of data. Novel techniques like Cloud-Based Attribute-Based Encryption (ABE) have surfaced as viable remedies to reduce these hazards. Characteristic-Based Public-key cryptography, which includes encryption, enables fine-grained access control over encrypted data. This implies that information can be encrypted according to particular traits or regulations, guaranteeing that only individuals who are permitted and possess the necessary attributes can decode and retrieve the data. When combined with cloud computing, ABE provides a scalable and effective way to secure big datasets that are frequently encountered in the banking industry.

By combining ABE with big data technology, financial organizations can take use of cloud computing's potential while still upholding strict security measures. Making informed decisions requires having insights into market trends, customer behavior, and risk management, all of which are provided by big data analytics. These advantages do, however, come with a risk: safeguarding the enormous volumes of private data processed and kept on cloud servers. The potential of big data technology and cloud-based attribute-based encryption to improve thesecurity of financial data is examined in this article. It explores the workings of ABE, the benefits of storing and processing data on cloud platforms, and the use of big data in the financialsector. The paper looks at these components in order to give readers a thorough grasp of how these technologies can be used to protect financial data and guarantee data integrity and privacy in an increasingly digital world.

1.1 Attribute-Based Encryption (ABE)

ABE is a kind of public-key encryption in which the ciphertext and the user's secret key rely on many factors (such as roles, user identification, or other descriptive properties). The user's qualities must match those listed in the access policy in order for access to the encrypted data to be authorized.

1.2 Types of ABE

Key-Policy ABE (KP-ABE): This approach encrypts data using a set of attributes and embeds the access policy into the secret key of the user. If the characteristics of the ciphertext meet the requirements of the key's access policy, decryption can occur. The roles are inverted in Ciphertext-Policy ABE (CP-ABE). Users are assigned secret keys linked to specific attributes, and the access policy is contained inside the ciphertext. If the user's characteristics match the ciphertext's access policy, decryption can be achieved.

1.3 Application in Cloud Computing

Data Confidentiality: Guarantees that the data can only be decrypted and accessed by authorized individuals who have the necessary qualities. Cloud service providers can implementcomplicated access control policies with fine-grained access control, which eliminates the needto keep user-specific keys. Scalability: Because of its attribute-based methodology, it is appropriate for systems with a high user count and data access policies.

1.4 Process Overview

Configuration: Public parameters and master keys are generated from a reliable source. Key Generation: Depending on a user's qualities, the authority gives them secret keys. Data encryption: An access policy that outlines the attributes needed for decryption is applied to

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2021.v14.i3.pp18-28

Vol. 14, Issue 3, 2021

encrypted data. Decryption: If the ciphertext's access policy is satisfied by the users' attributes, the data can be decrypted.

1.5 Data Collection and Integration

Data is gathered by financial institutions from a variety of sources, such as social media, market feeds, customer interactions, and transactions. A thorough picture of financial activity is provided by integrating this data, which aids in the identification of irregularities and possible security risks.

1.6 Real-Time Analytics

Real-time financial transaction monitoring and analysis is made possible by big data analytics. This facilitates the prompt mitigation of risks by assisting in the early discovery of fraudulent activity.

1.7 Predictive Analytics

Predictive models are able to predict possible security lapses and fraudulent efforts by examining past data. Based on these forecasts, financial institutions can take preemptive steps to stop these kinds of things from happening.

1.8 Enhanced Security Measures

Large data sets can be analyzed by big data techniques to find trends and abnormalities that point to potential security risks. Algorithms that use machine learning have the capacity to continuously learn from fresh data, which enhances their capacity to identify and address security risks.

2 Literature Survey

Mittal (2017) In order to provide secure data access in cloud contexts, this study investigates attribute-based encryption (ABE). Using characteristics to manage access to encrypted data and improve security and privacy in cloud storage and sharing are two important features. Instead of using more conventional techniques like usernames or passwords, ABE provides fine-grained access control, enabling people to access data based on specified criteria. By guaranteeing safe data management and sharing procedures, this method allays worries about data confidentiality and illegal access in cloud computing.

Gai (2015) In mobile cloud environments, the study presents a proactive attribute-based safe data schema designed specifically for the banking sector. The use of characteristics for strict data access control, which strengthens security in financial transactions, is one of the key highlights. This schema makes it possible to take preventative steps to protect sensitive data, guaranteeing adherence to industry rules and reducing possible risks related to using mobile clouds.

Moghadam (2019) Examining current approaches and identifying unresolved problems, this study explores the path toward cloud-based data analytics security. Analyzing existing security measures, identifying security holes, and talking about unsolved issues are some of the highlights. The study is to promote additional research in this developing subject and to deepen understanding of security issues in cloud-based data analytics.

Morales-Sandoval (2020) An attribute-based encryption (ABE) strategy designed for safe cloud storage, sharing, and retrieval of encrypted data is presented in this study. Highlights include

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2021.v14.i3.pp18-28

Vol. 14, Issue 3, 2021

improving security and privacy in cloud storage and sharing, and controlling access to encrypted data by utilizing attributes. Fine-grained data access management is ensured via the ABE framework, which makes variable access control policies based on user traits possible. This method helps to enable safe data management procedures in the cloud by addressing issues with data confidentiality and illegal access in cloud computing.

Qiu (2018) Specifically designed for mobile clouds in the financial industry, this paper offers a proactive, user-centric secure data method that uses attribute-based semantic access controls. Proactive security procedures that use attribute-based access controls to guarantee strict data protection are among the key aspects. By improving adherence to industry rules and reducing the risks connected with mobile cloud usage, the program is intended to address specific security concerns within the financial sector.

Sameera (2023) With a focus on industrial cloud environments, this study presents an effective attribute-based encryption (ABE) technique with privacy-preserving key generation. One of the main achievements is the creation of a strong encryption system that protects user privacy during key generation and guarantees data security. The plan improves security in industrial cloud environments by enabling user-attribute-based, fine-grained access management. Secure data management and sharing in industrial cloud infrastructures are made easier by this strategy, which addresses privacy concerns and offers effective encryption techniques.

Song (2019) The difficulties of privacy and security that arise from processing data in industrial big data and Internet of Things (IoT) ecosystems are examined in this investigation. Analyzing weaknesses and possible risks within these networked systems, suggesting measures to protect sensitive data, and addressing industry rules' compliance are some of the highlights. The goal of the conversation is to improve knowledge of the intricate issues related to security and privacy in industrial data processing, which will aid in the creation of strong defenses against threats to vital infrastructure.

Kumar (2018) In addition to providing a gap analysis and suggesting future research areas, this thorough survey evaluates attribute-based encryption (ABE) in cloud computing. Highlights include assessing current ABE schemes, pointing out security and implementation issues, and making recommendations for future development paths. The purpose of the survey is to improve knowledge of ABE's function in cloud security, provide direction for next studies, and encourage creativity in this developing area.

Yang (2020) Examining data security and privacy protection tactics for cloud storage, this survey provides information on existing practices as well as potential future developments. Examining encryption methods, access control systems, and privacy legislation compliance are some of the highlights. The purpose of the survey is to raise public awareness of the risks associated with data security in cloud storage, point out weaknesses in security protocols, and suggest ways to improve security and privacy in cloud-based data storage systems.

Joshi (2018) To ensure safe access to cloud-based Electronic Health Record (EHR) systems, this study focuses on attribute-based encryption (ABE). The use of ABE to restrict access to private medical data and improve security and privacy in EHR administration are two noteworthyfeatures. By enabling user-attribute-based, fine-grained access control, the method protects

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2021.v14.i3.pp18-28

Vol. 14, Issue 3, 2021

patient privacy and complies with healthcare standards. By addressing important security issues in cloud-based healthcare systems, our research makes it easier to maintain electronic health records securely and effectively.

Koo (2013) In cloud storage environments, this study investigates safe and effective data retrieval over encrypted data using attribute-based encryption (ABE). The use of ABE to providesafe data access while maintaining confidentiality and improving privacy in cloud storage systems are two noteworthy features. By providing user-attribute-based fine-grained accesscontrol, the method ensures effective data retrieval without sacrificing security. Through tacklingprivacy issues and refining data retrieval procedures, our research advances the development of safe and effective cloud storage solutions.

Deepika (2020) Through the prism of attribute-based encryption (ABE), this review offersinsights into data privacy. Examining ABE's contribution to improving data privacy, its applications in a variety of fields, and its efficiency in maintaining secrecy while permitting adaptable access control are some of the key points. In addition to highlighting areas for further study and advancement in this vital sector, the review attempts to enhance knowledge of the role that ABE plays in protecting data privacy.

3 Methodology

3.1 Selection of Sources

A thorough analysis of scholarly literature is essential to fully comprehend how Cloud-Based Attribute-Based Encryption (ABE) and Big Data are integrated for the protection of financial data. Examining several peer-reviewed papers, articles, and journals on pertinent technologies and their uses in financial data security is part of this process. The overview first examines the mechanisms and uses of attribute-based encryption, or ABE. Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE) are compared in order to see which is a better method for protecting sensitive information.

The analysis then moves on to Big Data Analytics, looking into how these tools improve data security, identify fraud, and control risks in financial institutions. Applications for machine learning, predictive modeling, and real-time analytics fall under this category. The influence of the Internet of Things (IoT) on data security, operational efficiency, and financial management is examined through an analysis of research, with a particular emphasis on IoT security frameworks and protocols. The literature review delves into the evolution and uses of Blockchain Technology in the financial industry. This entails evaluating the consensus processes, decentralization, and security characteristics of blockchain technology in order to overcome the shortcomings of conventional financial systems. Lastly, Cloud Computing is reviewed, analyzing how cloud- based models handle, store, and protect massive datasets. ABE integration is given particular focus in order to improve data security.

3.2 Sources of Data

Data collection from financial institutions, including banks and investment businesses, is the focus of this task. The information consists of market feeds, client interactions, and transaction records. These documents offer insightful information about consumer behavior, market trends, and financial activity.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2021.v14.i3.pp18-28

Vol. 14, Issue 3, 2021

Making Use of Public and Proprietary Datasets: This refers to making use of both publicly accessible datasets and datasets that are owned and supplied by certain organizations. These datasets are necessary in order to conduct thorough and precise analysis.

3.3 Integration of Data

Combining Diverse Data Sources: This refers to techniques for combining different datasets into a coherent, single dataset. It makes sure that all pertinent data is gathered from various sources.

Preserving Data Accuracy and Consistency: This describes the methods used to make sure that the combined data is consistent, accurate, and dependable across all sources. To preserve the integrity of the data, this may entail data validation, cleaning, and transformation procedures.

3.4 Implementation of Attribute-Based Encryption (ABE)

3.4.1 Selection of ABE Scheme

KP-ABE and CP-ABE comparison: This is a comparison of the two main categories of attribute-based encryption methods. Whereas Ciphertext-Policy ABE (CP-ABE) embeds the access policies directly in the ciphertext, Key-Policy ABE (KP-ABE) enables data owners to establish access policies and embed them in users' private keys.

Selecting the Correct ABE Scheme: The unique security needs for financial data should be the basis for choosing which ABE scheme to employ. This could involve taking the data's sensitivity, scalability, and adaptability into account.

3.4.2 Setup and Configuration

Configuring Master Keys and Public Parameters: In this stage, the ABE system's initial master keys and public parameters are configured. For the system to function and be secure, these are necessary.

Producing and Sharing Cryptocurrency: This covers the processes for generatingcryptocurrencies based on user characteristics. These keys are distributed safely to authorized users thanks to the distribution method.

3.4.3 Encryption and Decryption Processes

Procedure for Encrypting Financial Data: The processes for encrypting financial data with the chosen ABE scheme are described in this section. It involves using encryption methods and establishing the access rules.

Methods for Decryption: The latter covers the procedures required to decode the information. Ensuring secure and allowed access, the data can only be decrypted and accessed by users whose attributes meet the access policy encoded in the ciphertext.

3.5 Big Data Analytics Integration

3.5.1 Real-Time Data Analysis

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2021.v14.i3.pp18-28

Vol. 14, Issue 3, 2021

Putting in place systems that continuously track financial transactions as they happen is known as "implementing real-time monitoring." These technologies give users immediate access to information about current events.

Techniques for Anomaly and Fraud Detection: These involve the use of Big Data analytics to spot odd patterns and behaviors that might point to fraud. These irregularities are detected in real time by sophisticated algorithms that examine massive amounts of data.

3.5.2 Predictive Analytics Models

Predictive model development is the process of building models that have the ability to foresee possible security vulnerabilities before they happen. Advanced statistical and machine learning methods are used in the construction of these models.

Leveraging Historical Data: By training these predictive models on historical data, the accuracy of the algorithms is increased. The models can more accurately predict future threats and vulnerabilities by examining prior instances.

3.5.3 Enhanced Security Measures

Using machine learning to assess new data on a continual basis is known as "deploying machine learning algorithms." The ability of these algorithms to recognize and react to security risks is enhanced over time as they learn and adapt.

Developing techniques to improve the capacity to recognize and neutralize security threats is part of the process of improving threat identification and mitigation. These tactics are continuously improved upon by fresh data, which gradually increases their efficacy.

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2021.v14.i3.pp18-28
Vol. 14, Issue 3, 2021

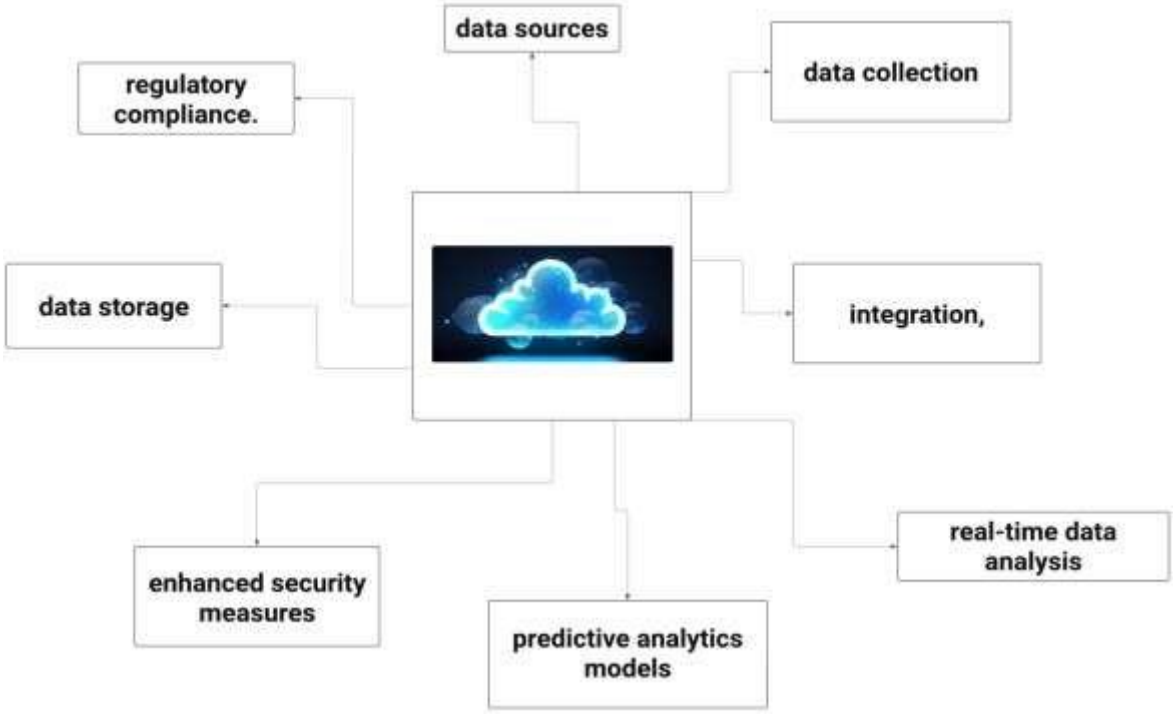

Figure 1: Big Data Analytics Integration with ABE

4 RESULTS AND DISCUSSION

The security and efficiency of financial data have been significantly enhanced by the combination of Attribute-Based Encryption (ABE) with big data analytics and cloud computing. Large data volumes were difficult for traditional ways to handle, but ABE makes sure that only authorized individuals may access important data. Data processing and analysis have beenimproved by utilizing Hadoop's distributed file system (HDFS) and cutting-edge machine learning methods. Financial institutions can quickly identify and stop fraud thanks to real-time monitoring and predictive analytics, which also lessens the likelihood of data breaches and unauthorized access occurrences. In the banking sector, this technological synergy has enhanced data integrity, operational efficiency, and regulatory compliance.

5 Conclusion

To sum up, the combination of attribute-based encryption (ABE), cloud computing, and big data analytics presents a number of promising avenues for enhancing the security of financial data. Cloud-based solutions can guarantee data confidentiality and scalability by utilizing ABE's fine-grained access control, which is important for managing large datasets in the banking industry. Additionally, big data analytics improves security measures by providing real-time monitoring, anomaly detection, and predictive analytics, which enable proactive risk management and regulatory compliance. Finally, through iterative refinement and stakeholder feedback, these

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2021.v14.i3.pp18-28

Vol. 14, Issue 3, 2021

technologies can continually adapt to new threats while upholding moral and legal standards. Attribute-based encryption (ABE), cloud computing, and big data analytics will all continue to be refined and integrated for future improvements in the field of financial data security. Potential directions for ABE technology development could be to increase flexibility and scalability so that even more precise access control over sensitive data is possible. Furthermore, data confidentiality should be prioritized along with resilience against new cyber threats in cloud- based solution optimization. This can be achieved by implementing strong encryption techniques and safe data storage protocols. To help financial institutions keep ahead of possible security breaches, big data analytics should develop to use cutting-edge machine learning algorithms and artificial intelligence approaches for more precise anomaly identification and predictive analytics. Future initiatives should also place a higher priority on ethical and legal compliance, guaranteeing that user consent and data protection continue to be at the forefront of security procedures. By means of ongoing technological innovation and iterative refinement prompted by stakeholder feedback, these integrated solutions can securely protect financial data in the digital age while adhering to legal and ethical requirements. Enhancing data security can be achieved byextending predictive analytics to encompass more financial metrics. Resilient encryption and access restrictions will be necessary to guarantee adherence to changing data privacy standards.If these technologies keep improving, financial data security could undergo a revolution that benefits all parties involved and improves operational sustainability.

6 References

1) Mittal, A. (2017). Attribute based encryption for secure data access in cloud.
2) Gai, K., Qiu, M., Thuraisingham, B., & Tao, L. (2015, August). Proactive attribute-based secure data schema for mobile cloud in financial industry. In 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems (pp. 1332-1337). IEEE.
3) Moghadam, S. S., & Fayoumi, A. (2019). Toward securing cloud-based data analytics: A discussion on current solutions and open issues. IEEE Access, 7, 45632-45650.
4) Morales-Sandoval, M., Cabello, M. H., Marin-Castro, H. M., & Compean, J. L. G. (2020). Attribute-based encryption approach for storage, sharing and retrieval of encrypted data in the cloud. IEEE Access, 8, 170101-170116.
5) Qiu, M., Gai, K., Thuraisingham, B., Tao, L., & Zhao, H. (2018). Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry. Future generation computer systems, 80, 421-429.
6) Sameera, M., & Rani, K. U. (2023). Enhancement of Cloud Data Protection using Attribute Based Encryption with Multiple Keys: A Survey. Mathematical Statistician and Engineering Applications, 72(1), 1952-1967.
7) Song, Y., Wang, H., Wei, X., & Wu, L. (2019). Efficient attribute-based encryption with privacy-preserving key generation and its application in industrial cloud. Security and communication networks, 2019.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2021.v14.i3.pp18-28

Vol. 14, Issue 3, 2021

8) Kumar, P., & Alphonse, P. J. A. (2018). Attribute based encryption in cloud computing: A survey, gap analysis, and future directions. Journal of Network and Computer Applications, 108, 37-52.
9) Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. Ieee Access, 8, 131723-131740.
10) Joshi, M., Joshi, K., & Finin, T. (2018, July). Attribute based encryption for secure access to cloud based EHR systems. In 2018 IEEE 11th International Conference on CloudComputing (CLOUD) (pp. 932-935). IEEE.
11) Koo, D., Hur, J., & Yoon, H. (2013). Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage. Computers & Electrical Engineering, 39(1), 34-46.
12) Deepika, D., Malik, R., Kumar, S., Gupta, R., & Singh, A. K. (2020, May). A review on data privacy using attribute-based encryption. In Proceedings of the International Conference on Innovative Computing & Communications (ICICC).