JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Literature Survey on Different Data Encryption and Decryption Techniques

[1]Mohit Kumar Malviya, [2]Prof. Manish Kumar Singhal
[1]M.tech Scholar, [2]Associate Professor & H.O.D
[1,2]Department of Information Technology (IT)
[1,2]NRI Institution of Information Science & Technology (NIIST)-BHOPAL,(M.P), INDIA,

Abstract : In this survey paper discuss the different Data Encryption and Decryption Techniques. With the exponential growth of data exchange over digital platforms, ensuring the security and privacy of information has become critical. Encryption and decryption techniques play a pivotal role in safeguarding sensitive data from unauthorized access and cyber threats. This literature survey explores various data encryption and decryption methods, analyzing their strengths, weaknesses, and applications. The survey also discusses emerging trends such as homomorphic encryption, which allows computations on encrypted data without decryption. This survey provides insights into selecting appropriate encryption techniques based on performance, security requirements, and specific use cases.

Keyword **- Encryption, Decryption, Cryptography, Symmetric Encryption, Asymmetric Encryption, Data Security, Algorithms, etc.**

I. INTRODUCTION

Encryption and decryption are essential processes in securing data in today's digital world. Encryption refers to the conversion of data into a coded format, making it unreadable to unauthorized users. This ensures that sensitive information, such as financial transactions, personal details, and confidential communications, is protected from potential threats. The encryption process uses algorithms and keys to transform plain text into ciphertext. Decryption, on the other hand, is the reverse process, where the encrypted data (ciphertext) is converted back to its original form (plaintext) using a corresponding key. This allows authorized users to access the data. The use of encryption and decryption enhances data security, privacy, and integrity, especially in fields like banking, healthcare, and cloud computing, where data breaches could have significant consequences. As cyber threats continue to evolve, encryption remains a vital tool in safeguarding digital information.

Encryption and decryption play a crucial role in both protecting data at rest (stored data) and data in transit (data being transmitted over networks). Various encryption methods, such as symmetric key encryption, where the same key is used for both encryption and decryption, and asymmetric key encryption, which uses a pair of public and private keys, are employed depending on the use case and security requirements. Symmetric encryption is faster and is often used for large volumes of data, while asymmetric encryption is more secure and typically used in activities like digital signatures and secures communications.

In the realm of cybersecurity and information protection, symmetric cryptography stands as a foundation, stimulating the data and upholding the purity of confidentiality [19]. At its core, symmetric cryptography revolves around the pivotal process of secret key generation elemental procedure that reinforces secure communication and data encryption. This paper delves into the complex domain of symmetric cryptography, unraveling the essence of secret key generation and its indispensable role in safeguarding digital information [1]. Symmetric cryptography relies on a single shared key for both encrypting and decrypting data. The genesis of this shared key lies within the meticulous procedure of key generation. This essential process initiates with the utilization of a random number generator, employed to craft a unique cryptographic key. This key serves as the linchpin of data security, furnishing the mechanism to transform plaintext into ciphertext and vice versa. Ensuring that this key remains clandestine and impervious to unauthorized access is paramount to preserving the integrity and confidentiality of encrypted data [2]. The significance of the secret key within symmetric cryptography cannot be overstated. Serving as the conduit through which information is shielded from prying eyes, the secret key encapsulates the essence of secure communication. Its generation algorithm is meticulously crafted to thwart adversarial attempts at guessing or reverse-engineering the key. This algorithmic sophistication ensures that the key remains resilient against cryptographic attacks, thereby bolstering the security posture of the encrypted data. Once the secret key emerges from the crucible of key generation, it assumes a mantle of confidentiality, shared solely between the sender and the intended recipient. This secret key exchange embodies the cornerstone of symmetric cryptography, orchestrating a symbiotic relationship between security and accessibility [4]. By entrusting the secret key exclusively to authorized entities, the

sanctity of encrypted data is preserved, shielding it from the prying eyes of malevolent adversaries. Symmetric cryptography epitomizes a delicate balance between robust security measures and operational efficiency. The clandestine exchange of secret keys engenders a realm of trust between communicative entities, fostering an environment conducive to secure data transmission. However, this symbiotic relationship is contingent upon the impregnability of the secret key testament to the pivotal role of key generation in fortifying data security

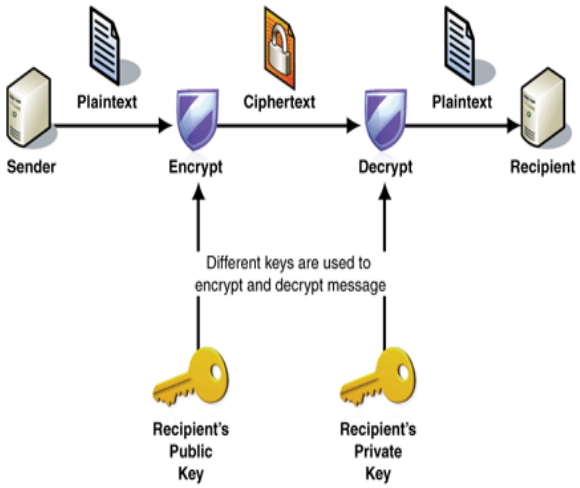

Fig 1 Data Encryption and Decryption Techniques

.

II. Type Style and Fonts

Naseemuddin Mohammaj, et.al (2024), Author are presented It takes some time to put the security framework for big data in cloud computing into practice. For complete security, the current cryptosystem is insufficiently useful. The encrypted data saved on cloud big data server storages cannot be searched at all if conventional encryption techniques are used. One amazing method that can assist the encrypted search is the fully homographic encryption technology. The cooperating encryption method covered in this work can be used to implement this. Another main topic of this article is realtime encryption of data moving via cloud networks Collaboration between cloud-to-cloud servers makes this possible. A few years later, significant technological advancements cause standard encryption methods to no longer meet security requirements. This work presents a distributed, parallel encryption solution that lessens the need for secure storage of sensitive data. Encrypting the various data components at different places and combining them at one place is helpful [01].

Narendra Shyam Joshi ,et.al,(2024), Author are analysis performance analysis Encryption is becoming more and more crucial for protecting user privacy as cloud services gain popularity. It is essential to provide dependable methods for quick and safe data recovery. This study suggests a brand-new method for searching encrypted cloud data. The proposed technique uses a greedy depth-first search (DFS) algorithm combined with an advanced grading system to optimise queries including multiple words and synonyms. Users are assumed to search using a large number of keywords, some of which may be synonyms for article terms, according to the recommended architecture. To address this issue, a search algorithm that makes use of synonyms from user queries was developed. Greedy search techniques assist us in locating the most relevant data even if the search universe is constantly expanding. Our depth-first search approach increases [02].

LE L, et.al, (2023), Author are study a n the current era of information explosion, users' demand for data storage is increasing, and data on the cloud has become the first choice of users and enterprises. Cloud storage facilitates users to backup and share data, effectively reducing users' storage expenses. As the duplicate data of different users are stored multiple times, leading to a sudden decrease in storage utilization of cloud servers. Data stored in plaintext form can directly remove duplicate data, while cloud servers are semi-trusted and usually need to store data after encryption to protect user privacy. In this paper, we focus on how to achieve secure de-duplication and recover data in ciphertext for different users, and determine whether the indexes of public key searchable encryption and the matching relationship of trapdoor are equal in ciphertext to achieve secure de-duplication. For the duplicate file, the data user's re-encryption key about the file is appended to the ciphertext chain table of the stored copy [03].

M. Suganya et.al, (2023), Researcher are Comparative analysis is presented here of the increasing rise of distributed system technologies, one of the most pressing problems facing the digital world is ensuring the security of sensitive and confdential data during transport and storage, which is also regarded as one of the most critical difculties facing cloud computing. Numerous techniques exist for enhancing data security in the cloud computing storage environment. Encryption is the most important method of data protection. Consequently, several accessible encryption strategies are utilized to provide security, integrity, and authorized access by employing modern cryptographic algorithms. Cloud computing is an innovative paradigm widely accepted as a platform for storing and analysing user data [04].

Bijeta Seth, et. al (2022), Authors presented Cloud computing has emerged as one of the most groundbreaking technologies to have redefined the bounds of conventional computing techniques. It has ushered in a paradigm shift and pushed

the frontiers of how computing assets, inclusive of infrastructure resources, software, and applications can be used, adopted, and purchased. The economic benefits or rather the fundamental economic shift offered by cloud computing in reducing capital expenditure and converting it to operational expenditure has been a primary motivating factor for early adopters. However, despite its inherent advantages that include better access and control, there exist several reservations around cloud computing that have impeded its growth. The control, elasticity, and ease of use that cloud computing is associated with also engender many security issues. Security is considered to be the topmost hurdle out of the nine identified challenges of cloud computing as underlined by the study conducted by the International Data Corporation [05].

Udochukwu Iheanacho Erondu, et.al, (2022), Author are study the advancement of network and multimedia technologies in recent years, multimedia data, particularly picture, audio, and video data, has become increasingly frequently used in human civilization. Some multimedia data, such as entertainment, politics, economics, militaries, industries, and education, requires secrecy, integrity, and ownership or identity protection. Cryptology, which looks to be a viable method for information security, has been used in many practical applications to safeguard multimedia data in this regard. Traditional ciphers based on number theory or algebraic ideas, such as data encryption standard (DES), advanced encryption standard (AES), and other similar algorithms, which are most commonly employed for text or binary data, do not appear to be appropriate for multimedia applications. As a result, this research examines effective algorithms for data security [06].

Muhammad Bilal Qureshi, et.al, (2022), With technological advancement, cloud computing paradigms are gaining massive popularity in the ever-changing technological advancement. The main objective of the cloud computing system is to provide on-demand storage and computing resources to the users on the pay-per-use policy. It allows small businesses to use top-notch infrastructure at low expense. However, due to the cloud resource sharing property, data privacy and security are significant concerns and barriers for smart systems to constantly transfer generated data to the cloud computing resources, which a third-party provider manages. Many encryption techniques have been proposed to cope with data security issues. In this paper, different existing data protection and encryption techniques based on common parameters have been critically analyzed and their workflows are graphically presented [07].

Sultan Almakdi, (2021) – This paper reviews has presented the database users have begun to use cloud database services to outsource their databases. The reason for this is the high computation speed and the huge storage capacity that cloud owners provide at low prices. However, despite the attractiveness of the cloud computing environment to database users, privacy issues remain a cause for concern for database owners since data access is out of their control. Encryption is the only way of assuaging users' fears surrounding data privacy, but executing Structured Query Language (SQL) queries over encrypted data is a challenging task, especially if the data are encrypted by a randomized encryption algorithm. Many researchers have addressed the privacy issues by encrypting the data using deterministic, onion layer, or homomorphic encryption. Nevertheless, even with these systems, the encrypted data can still be subjected to attack [08].

.

III. TYPE OF DATA ENCRYPTION AND DECRYPTION DATA

Data encryption and decryption are crucial techniques for safeguarding information in the digital world. **Encryption** is the process of converting plaintext data into an unreadable format, known as ciphertext, to prevent unauthorized access. This transformation is done using algorithms and encryption keys. There are two main types of encryption: symmetric and asymmetric. In symmetric encryption, the same key is used to both encrypt and decrypt data, making it fast but requiring secure key exchange. Asymmetric encryption, on the other hand, uses a pair of keys: a public key to encrypt data and a private key to decrypt it. While this method is more secure, it is slower and often used for smaller datasets.

Decryption is the reverse process of encryption, where ciphertext is converted back into its original plaintext form. Only authorized users with the correct decryption key can access the data. Encryption ensures confidentiality, while decryption restores accessibility when needed. These processes are widely used in securing communication, financial transactions, and personal data online, protecting it from hackers and unauthorized entities.

Encryption and decryption are not only essential for protecting sensitive data but also play a key role in maintaining data integrity and authenticity. For instance, encryption ensures that data remains unchanged during transmission, and even if it is intercepted, it cannot be altered without detection. This is critical in sectors like banking, healthcare, and government, where the security of personal and confidential information is paramount.

Beyond symmetric and asymmetric encryption, there are different algorithms used, such as AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), and ECC (Elliptic Curve Cryptography). AES is commonly used for symmetric encryption, offering a strong level of security with relatively fast processing speeds. RSA and ECC are used in asymmetric encryption, with RSA being one of the first widely adopted methods, while ECC provides similar security with smaller key sizes, making it more efficient.

In modern cybersecurity, encryption works hand-in-hand with hashing and digital signatures. Hashing is used to verify data integrity, generating a fixed-size string or hash from data. Digital signatures authenticate the sender of a message, ensuring that it originated from a trusted source and wasn't tampered with. Together, encryption, hashing, and digital signatures create a robust framework for securing data in various applications, such as VPNs, cloud storage, messaging apps, and e-commerce platforms. As cyber threats evolve, the need for more advanced encryption technologies continues to grow, with quantum cryptography on the horizon offering even stronger data protection.

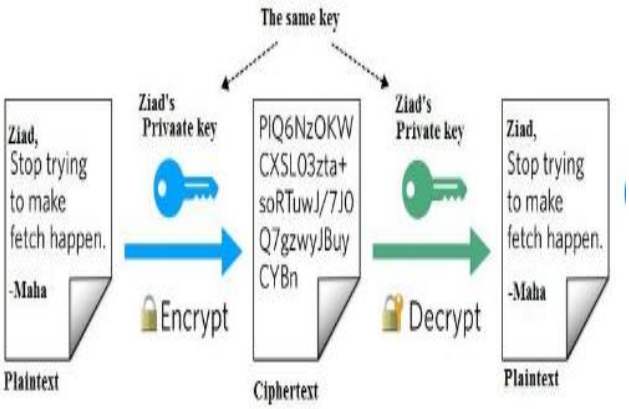

Fig 2. Type of Data Encryption and Decryption

Encryption and decryption play vital roles across various sectors, such as finance, healthcare, government, and personal communications, where the confidentiality of sensitive information is paramount. End-to-end encryption (E2EE) is widely used in messaging applications, ensuring that only the sender and the intended recipient can read the messages, even if intercepted during transmission. This is especially important for protecting personal data from cyberattacks and surveillance.

In addition to traditional encryption methods, homomorphic encryption allows computations to be performed on encrypted data without first needing to decrypt it. This means organizations can analyze or process data securely in its encrypted form, providing an added layer of security for tasks like cloud computing and big data analysis.

Another critical encryption concept is hashing, though not technically encryption. It converts data into a fixed-length hash value, which cannot be easily reversed back to its original form. Hashing is commonly used for password storage, ensuring that even if a database is breached, the actual passwords remain protected. Salting is often combined with hashing, adding random data to input before it is hashed to further enhance security.

Quantum cryptography represents the future of encryption, leveraging the principles of quantum mechanics to create virtually unbreakable encryption methods. Quantum key distribution (QKD) is one such technology that promises to revolutionize secure communications by allowing two parties to exchange cryptographic keys with complete security, even in the presence of eavesdroppers.

However, encryption has its challenges, such as the key management problem. The more keys there are, the harder it becomes to manage them securely, leading to potential vulnerabilities. Moreover, as encryption becomes stronger, it poses difficulties for law enforcement and government agencies that need access to data for legitimate purposes, sparking debates on encryption backdoors and privacy concerns.

Overall, encryption and decryption are indispensable in protecting data in an increasingly digital world, from securing online transactions to safeguarding personal information against cyber threats. As technology evolves, new encryption methods will continue to emerge, balancing the need for security with performance and accessibility.

IV. CHALLENGES TO ENCRYPTION AND DECRYPTION OF DATA

Encryption and decryption of data, while essential for securing sensitive information, face several challenges. One of the primary issues is the complexity of key management. As data is encrypted, keys must be securely distributed and stored, making them vulnerable to interception or loss. Additionally, advancements in computational power and quantum computing pose a threat to current encryption algorithms, potentially rendering them obsolete. Another challenge is the balance between encryption strength and performance; stronger encryption can slow down systems and increase processing times. Furthermore, compliance with varying legal regulations across regions can complicate encryption implementation, as some countries may require backdoor access to encrypted data. Lastly, human error, such as poor password management or failure to update encryption protocols, can weaken even the most robust encryption systems.

Moreover, the growing sophistication of cyberattacks poses an ongoing challenge to encryption. Attackers may exploit vulnerabilities in the encryption process, such as side-channel attacks, which target the implementation rather than the encryption algorithms themselves. Encryption systems must also be continuously updated to defend against these evolving threats, which requires resources and expertise that many organizations may lack. Additionally, encrypted data can sometimes be difficult to manage, particularly in scenarios requiring fast data retrieval or search functionality, as encrypted content must first be decrypted before use, adding complexity to data handling. The rise of encrypted traffic can also challenge security monitoring, as traditional threat detection tools may struggle to analyze data that is shielded by encryption. These challenges highlight the need for constant innovation in encryption technologies, as well as rigorous training and protocols to ensure secure and efficient use.

V. CONCLUSION

In this survey paper discuss on different Data encryption and decryption are fundamental techniques in protecting digital information from unauthorized access and ensuring data integrity. Encryption transforms readable data into an encoded format that can only be deciphered by authorized parties, using algorithms and keys to secure the data. Decryption, on the other hand, reverses this process, converting encrypted data back into its original form.

In this survey paper encryption and decryption techniques are vital for protecting data, they are just one part of a broader cybersecurity strategy. Continual vigilance, technological advancements, and adherence to security protocols are essential to maintaining robust data protection in an ever-changing digital landscapes.

REFERENCES

[1] Narendra Shyam Joshi, Kuldeep P. Sambrekar , Abhijit J. Patankar , Archana Jadhav and Prajakta Khadkikar. "Optimizing Encrypted Cloud Data Security and Searchability through Multi-Keyword Ranking Search Methods." ISSN (2210-142X) (2024) Int. J. Com. Dig. Sys. , No. (Mon-20..).

[2] Narendra Shyam Joshi, Kuldeep P. Sambrekar , Abhijit J. Patankar , Archana Jadhav and Prajakta Khadkikar. "Optimizing Encrypted Cloud Data Security and Searchability through Multi-Keyword Ranking Search Methods." International Journal of Computing and Digital Systems, ISSN (2210-142X) (2024).

[3] Le Li 1 , Dong Zheng 1,2, Haoyu Zhang 1 , And Baodong Qin. "Data Secure De-Duplication and Recovery Based on Public Key Encryption With Keyword Search." VOLUME 11, 24 March 2023.

[4] M. Suganya1 and T. Sasipraba. "Comparison and Analysis of Transformer-less Topologies for Grid-Connected PV Systems." Stochastic Gradient Descent long short-term memory based secure encryption algorithm for cloud data storage and retrieval in cloud computing environment, 09 May 2023.

[5] Bijeta Seth, Surjeet Dalal, Vivek Jaglan, Dac-Nhuong Le, Senthilkumar Mohan, Gautam Srivastava. "Integrating encryption techniques for secure data storage in the cloud." Citations: 27, Volume33, Issue4 04 September 2022.

[6] Udochukwu Iheanacho Erondu, Nehemiah Adebayo, Micheal Olaolu Arowolo, Moses Kazeem Abiodun. " Different Encryption and Decryption Approaches for Securing Data."2022.

[7] Muhammad Bilal Qureshi, Muhammad Shuaib Qureshi , Saqib Tahir , Aamir Anwar, Saddam Hussain, Mueen Uddin and Chin-Ling Chen, Volume 14, Issue 4 , 28 March 2022.

[8] Sultan Almakdi, Brajendra Panda, Mohammed S. Alshehr " An Efficient Secure System for Fetching Data From the Outsourced Encrypted Databases. Volume 9" June 4, 2021.

[9] Chin-Chen Chang and Chao-Wen Chan, A database record encryption scheme using the RSA public key cryptosystem and its master keys,ICCNMC '03: Proceedings of the 2003 International Conference on Computer Networks and Mobile Computing (Washington, DC, USA), IEEE Computer Society,2003.

[10] Luc Bouganim and Philippe Pucheral, Chip-secured data access:confidential data on untrusted servers, VLDB '02: Proceedings of the 28th international conference on Very Large Data Bases, VLDB Endowment, 2002, pp. 131–142.

[11] BalaIyer, Sharad Mehrotra2,Einar Mykletun,GeneTsudik, and Yonghua Wu, A Framework for Efficient Storage Security in RDBMS,Advances in Database Technology - EDBT 2004 Volume 2992 of the series Lecture Notes in Computer Science pp 147-164

[12] Tingjian Ge and S. Zdonik, Fast, secure encryption for exing in a column-oriented DBMS, Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference on, 2007, pp. 676–685.

[13] Berent, A. (2013). Advanced Encryption Standard by Example. Document available at URL http://www. networkdls. com/Articles/AESbyExample. pdf (April 1 2007) Accessed: June.

[14] Nadeem, H (2006). A performance comparison of data encryption algorithms," IEEE Information and Communication Technologies, (pp. 84- 89).

[15] Curtmola, R., Garay, J. A., Kamara, S., & Ostrovsky, R. (2006). Searchable symmetric encryption: Improved definitions and efficient constructions. In Proceedings of the 13th ACM conference on Computer and communications security (pp. 79-88). ACM. doi: 10.1145/1180405.1180418.

[16] Naveed, M., Kamara, S., & Wright, C. V. (2010). Inverted index for encrypted databases: beyond the cloud. In Proceedings of the 2010 ACM SIGMOD International Conference on Management of data (pp. 801-812). ACM.

[17] D. R. Miller, "AttributeConverter: An Innovative Approach for Searching Encrypted Data," in Proceedings of the 5th International Conference on Data Science and Information Technology, pp. 211-219, 2020.

[18] Y. Wang, A. H. Song, and J. Zhang, "Exploring Fully Homomorphic Encryption for Secure Data Searching," in IEEE Access, vol. 8, pp. 187255- 187263, 2020.

[19] T. A. Brown and S. Kumar, "A Comparative Analysis of AES, Triple DES, RSA, SHA, and Blowfish Encryption Algorithms," Journal of Computer and Communications, vol. 7, no. 3, pp. 33-40, 2019.

[20] F. Anderson and K. Thompson, "Comparing Encrypted Search Techniques: A Focus on Performance and Security," in IEEE Transactions on Knowledge and Data Engineering, vol. 32, no. 4, pp. 735-748, 2020.

[21] R. Singh and S. Gupta, "The Future of Database Encryption and Secure Search: Trends and Predictions," in Proceedings of the 5th International Conference on Information Systems Security, pp. 124-131, 2021.

[22] P. Kumar and L. Chen, "Blind Indexing: A Novel Approach to Secure Search in Encrypted Databases," in Proceedings of the 4th International Conference on Cyber Security and Cloud Computing, pp. 113-120, 2019.

[23] R. Smith and B. Jones, "Blowfish Algorithm: Its Relevance in Modern Cryptography," in IEEE Access, vol. 8, pp. 95050-95058, 2020.

[24] Online. (1999). Cloud Database Market. [Online]. Available: https://www.marketresearchfuture.com/reports/cloud-database-market6847

[25] R. A. Popa, C. M. S. Redfield, N. Zeldovich, and H. Balakrishnan, ''CryptDB: Processing queries on an encrypted database,'' Commun. ACM, vol. 55, no. 9, pp. 103–111, Sep. 2012.

[26] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, ‘‘Order preserving encryption for numeric data,’’ in Proc. ACM SIGMOD Int. Conf. Manage. Data (SIGMOD), 2004, pp. 563–574.
[27] Y.-D. Jang and J.-H. Kim, ‘‘A comparison of the query execution algorithms in secure database system,’’ Int. J. Electr. Comput. Eng., vol. 6, no. 1, p. 337, Feb. 2016.
[28] M. Naveed, S. Kamara, and C. V. Wright, ‘‘Inference attacks on propertypreserving encrypted databases,’’ in Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur., Oct. 2015, pp. 644–655.
[29] D. Pouliot and C. V. Wright, ‘‘The shadow nemesis: Inference attacks on efficiently deployable, efficiently searchable encryption,’’ in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., Oct. 2016, pp. 1341–1352.
[30] W. Wang, Y. Hu, L. Chen, X. Huang, and B. Sunar, ‘‘Exploring the feasibility of fully homomorphic encryption,’’ IEEE Trans. Comput., vol. 64, no. 3, pp. 698–706, Mar. 2015.
[31] F. Oggier and M. J. Mihaljević, ‘‘An information-theoretic security evaluation of a class of randomized encryption schemes,’’ IEEE Trans. Inf. Forensics Security, vol. 9, no. 2, pp. 158–168, Feb. 2014.
[32] A. Alsirhani, P. Bodorik, and S. Sampalli, ‘‘Improving database security in cloud computing by fragmentation of data,’’ in Proc. Int. Conf. Comput. Appl. (ICCA), Sep. 2017, pp. 43–49.
[33] H. Hacigümüş, B. Iyer, C. Li, and S. Mehrotra, ‘‘Executing SQL over encrypted data in the database-service-provider model,’’ in Proc. ACM SIGMOD Int. Conf. Manage. Data (SIGMOD), 2002, pp. 216–227.
[34] M. Nabeel, E. Bertino, M. Kantarcioglu, and B. Thuraisingham, ‘‘Towards privacy preserving access control in the cloud,’’ in Proc. 7th Int. Conf. Collaborative Comput., Netw., Appl. Worksharing (CollaborateCom), 2011, pp. 172–180.
[35] Y. Zhu, H. Hu, G.-J. Ahn, D. Huang, and S. Wang, ‘‘Towards temporal access control in cloud computing,’’ in Proc. IEEE INFOCOM, Mar. 2012, pp. 2576–2580

).