Hybrid Cryptographic Framework for Cloud Data Security: Integration of AES-OTP, RSA, and Temporal Access Control Mechanisms

[1*]Mansi Ahirwar, [2]Dr. Manoj Tyagi

[1] M.Tech scholar, Department of Computer Science and Engineering, Technocrats Institute of Technology, Anandnagar, Bhopal

[2]Professor, Department of Computer Science and Engineering, Technocrats Institute of Technology, Anandnagar, Bhopal

Corresponding Author-

mansiahirwar253@gmail.com

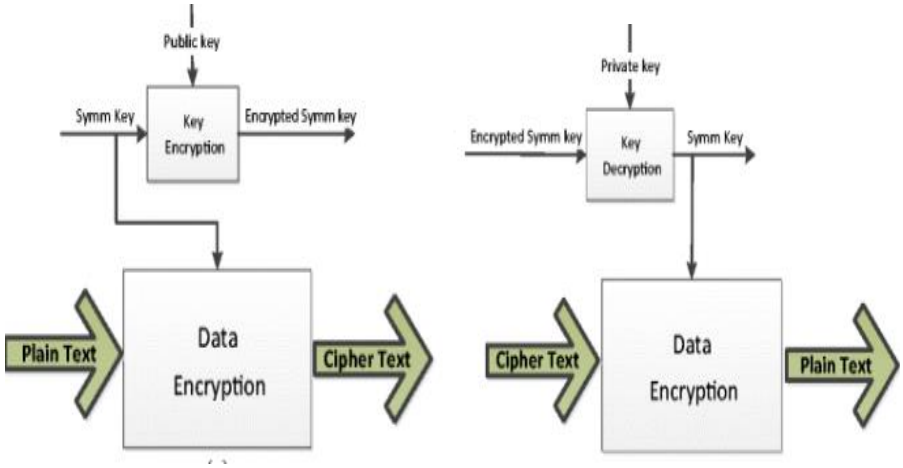
Abstract: This generation of cloud computing has characterized the Internet of Things with exponentially increasing data generation, processing, and storage. Regrettably, however, accompanying this trend of growth is the increased concern for cloud-based systems about security, privacy, and control of access to data. The proposed work introduces a hybrid cryptographic framework that combines AES, OTP, and RSA encryption methods with temporal mechanisms to enhance the security of data in the cloud. This framework benefits from both symmetric and asymmetric approaches to encryption; hence, the reliability for secure transfer, confidentiality, and efficient key management is enhanced. OTP integration will include security from brute force attacks and unauthenticated access into the application. Temporal security is added through time-bound implementation of access control mechanisms: access to data will be matched to the time intervals as well-the overall robustness of dynamic clouds over time. Side-channel attacks and defense: "The paper presents an overview of the application of hybrid deep learning models for countering side-channel attacks, showing potential towards better accuracy in key prediction." Although the proposed hybrid cryptographic model has drawbacks such as no scalability, APIs that are insecure, or data breaches, it is scalable, adaptive, and efficient in dealing with issues concerning cloud data security. Refinement of these hybrid models to deal with emerging threats and optimization of their performance in large-scale clouds may be some future research directions.

Keywords: Cloud computing, hybrid cryptography, AES, OTP, RSA, temporal access control, data security, IoT, asymmetric encryption, symmetric encryption, side-channel attacks.

I. Introduction

The goal of the Internet of Things (IoT) is to link the disconnected. It describes the quickly expanding internet-connected sensing equipment and technology that enable intelligent processing, dependable transmission, and overall information perception. IoT is the fusion of various information sensing devices, including Radio Frequency Identification (RFID), Wireless Sensing Networks (WSN), cloud computing, global positioning systems, and the Internet, to create a massive network and enable data management and identification. In the end, this allows people all over the world to access the entire range of services through the integration of applications. From logistics to smart neighborhoods, intelligent transportation, smart banking systems, and other sectors, this technology is developing at a rapid pace [1]. One important component of information security is cryptography. One crucial component of information security is cryptography. The Economic Times edition of the Indian Newspaper states that the process of transforming regular plain language through unreadable text or vice versa is known as cryptography. It is a technique for transmitting and storing data in a specific format so that only the intended recipients are able to read and analyze it [2]. The growth of healthcare organizations, including medical facilities, therapies, and the health systems for the administration of patient care, has led to an increase in human lifespan in recent times [3]. However, significant issues with the development of advanced healthcare include

needless mistakes, transmission delays, security risks, inadequate medical data, and fault diagnostics [4]. Therefore, new tactics must be used to protect patient data from unauthorized users. Moreover, IoT-based wearable sensor applications for disease prediction have seen a huge surge in use [5] in the healthcare industry. Additionally, IoT devices offer the same consumers and are coupled with cloud computing components [6]. The structure of hybrid encryption cryptosystem is shown in figure 1.



(a) (b)

Fig. 1: The structure of hybrid encryption cryptosystem. (a) Encryption. (b) Decryption [7]

A cloud service supplier platform generates and hosts an enormous volume of data [8]. Many of the services and apps for smart cities will be housed in the cloud because of its scalable, dependable, and high-performance datacenters. Storage is a key element of cloud computing. Storage could be used for a corporate database or just plain data storage, much as local hard disk storage. Instead of being hosted on dedicated servers as in classic networked data storage, data in cloud storage is stored across several third-party services [9]. The consumer "sees" a virtual server while storing data, giving the impression that the data is kept in a specific location with a certain name, even though that location does not actually exist.

One vision for the next generation of computer paradigms is cloud computing. Application and resources are provided as services over the Internet on demand in the framework of cloud computing. The cloud is a data center environment made up of software and hardware assets that offer a variety of services via networks or internet to meet customer needs [8].

The variety of data types grows daily. Anything from phones to wearables to cameras to sensors to cars might be considered a thing. The idea of the Internet of Things is to collect, exchange, and process data with the least amount of human intervention possible. IoT is bringing smart homes, smart good health, and smart city components to our life. Smart devices have resource limits, such as tiny RAM and a restricted battery life. To connect to the internet, Internet of Things (IoT) devices needed a special Internet Protocol (IP). Internet of Things (IoT) depends on physical things that share data among other objects online by using sensors to collect and share that data [10].

II. Background and Cryptographic Techniques

There has been a tremendous increase in the number of vehicles compared to the number of roads. This situation leads to many challenges like heavy traffic jams, economy, pollution, and many other issues related to efficiency and safety of transportation systems. Many initiatives have already been taken in response to these challenges in order to overcome the situation. For this scenario, utilization of wireless technology in vehicular networks makes a huge difference to overcome the traffic issues and reduce the chances of accidents or injuries. Intelligent

transportation systems (ITS) [11] are developed, aiming to improve the efficiency and safety of transportation systems. There is a lot of information and data in our world that is transmitted through communication channels or e-mail, and in various forms. Examples of this data are pictures, videos, or personal data. Once the data is sent from a phone or laptop to the recipient on the website, this data may be stolen or changed by another party. And that, through the use of modern applications that are developing day by day, and therefore with the increase in the amount of data sent via e-mail or taken from the web, there is no guarantee that it is the correct data [12].

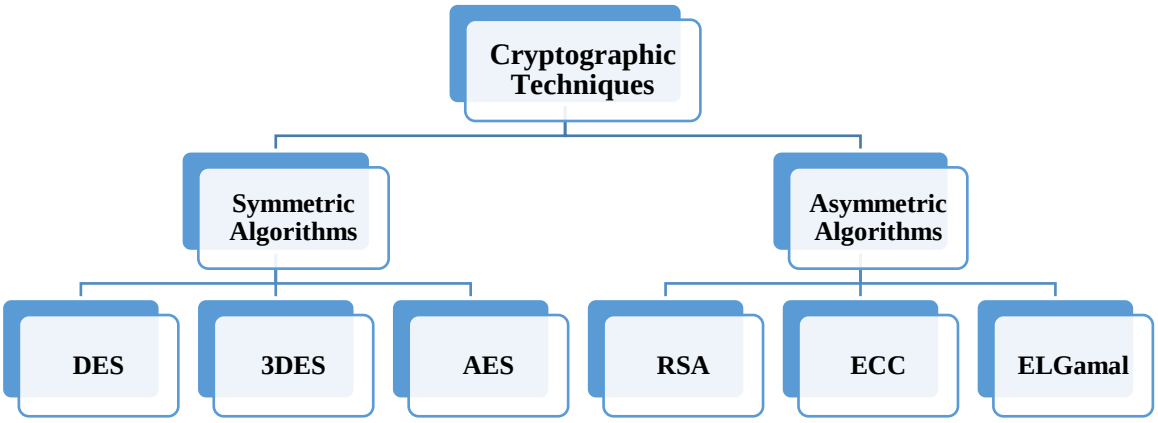


Fig. 2: Taxonomy of cryptography techniques [13].

A. Symmetric Algorithm Cryptography: As we shown in above figure 2 symmetric encryption techniques encrypt and decode data using the same single key. These kinds of algorithms are numerous and include Blowfish, DES, AES, and others. Every algorithm encrypts and decrypts data in a unique way, and they all decrypt and encrypt an identifiable quantity of data—a block and a fixed size of key—in the same way. Only the English alphabet, special symbols, and numeric values may be entered as plaintext using these kinds of algorithms [14]. As a result, the result (ciphertext) will be generated as a document consisting of unique characters, alphabets, numbers, or a combination of all three. The elements of symmetric encryption can be enumerated as follows:

1. **Plaintext:** Sender is willing to transfer the original data to a designated recipient. The encryption algorithm will be used to process these data.
2. **Encryption algorithm:** It is a series of operations that, with the use of a secret key, will run into plaintext and generate ciphertext.
3. **Secret key:** It is a value that is combined with plaintext to create ciphertext; the value is separate from the plaintext.
4. **Ciphertext:** This is the result of applying an encryption algorithm on the original plaintext. It will differ greatly from plaintext.
5. **Decryption algorithm:** It is a series of operations that, with the use of a secret key, will be carried out to convert plaintext into ciphertext.

B. Asymmetric Algorithm Cryptography: Separate keys are used for encryption and decryption in asymmetric key cryptography. The idea of both private and public keys is used in its operation. Each participant's public key has been made available in a public domain, meaning that anybody can access it, but each participant's private key is kept confidential. The message will be encrypted by the sender using the recipient's public key, and it will be decrypted by the recipient using his own private key. Data that has been encrypted by both keys can be decrypted [14]. In data security, asymmetric cryptographic algorithms come in a variety of forms. Although they are all based on various mathematical ideas, like factorization and discrete logarithm problems, each one offers a unique benefit. These various methods include the following in-depth discussions: RSA, Diffie-Hellman key exchange, Elliptic Curve Cryptography (ECC), and ELGAMAL Cryptosystem:

1. **RSA Cryptosystem:** One public key cryptosystem used to secure data transfer is the RSA cryptosystem. It was created in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman at Government Communications Headquarters, a British signals intelligence organization. The sir name of the algorithm's creators are where the name RSA originates. The primary goal in creating the RSA encryption system was to produce a one-way function that would be very difficult or nearly impossible to reverse. Its foundation is the mathematical truth that two very big prime values can be found and multiplied with ease, but that factoring them is extremely challenging. Two very big prime numbers serve as the foundation of both private and public keys used in the RSA cryptosystem [16].
2. **ECC (Elliptic Curve Cryptosystem):** The term "ECC" refers to a group of protocols where the security is derived from specific discrete logarithms rather than number modulo p. Similar to number modulo p, ECC uses a collection of numbers related to mathematical objects called elliptic curves. These values can be added to and computed using specific procedures. Because discrete logarithms are assumed to be more difficult to locate when applied to elliptic curves, ECC is utilized [17].
3. **ELGAMAL Cryptosystem:** Asymmetric encryption is utilized in public key cryptography with the ELGAMAL cryptosystem. The key exchange algorithm of Diffie-Hellman serves as its foundation. 1985 saw Taher Elgamal design this algorithm. Because it is very hard to compute gak even when we know gk and ga, the algorithm's security is based on its difficulty in solving the discrete logarithm issue in a cyclic group. Similarly, the algorithm's security is based on the difficulty of calculating the discrete logarithm in a shorter amount of time. One plain text can be converted into several cipher texts using Elgamal encryption [17].

III. Hybrid Cryptographic Models in Cloud Security

The document covers a schematic to generate keys relying on utilizing a hybrid deep learning model to perform side-channel attacks. The method consists of inputting various combinations of ciphertext, plaintext, encryption/decryption bits, side-band data, etc. to a hybrid deep learning model (CNN-RNN). Based on these inputs a 56-bit key is predicted. At this stage, the procedure is attempted without the side-band data with only ciphertext, plaintext, and encryption/decryption bits used as the inputs. These converting of the inputs from hex to binary is performed only for plain text and cipher text, and when the model predicts with the softmax layer, it generates probable keys for the real key. To address such issues, side-band data that records the alteration of hardware is incorporated so as to improve key prediction accuracy [18].

Complete results demonstrate that the addition of side band data enhances the accuracy of the model as well as the key prediction model parameters such as time execution, accuracy, and memory consumption efficiency over several training epochs. Nonetheless, some considerations remain chiefly because of the noise and variability inherent in side-channel analysis, which can affect the ability of the model to perform across various devices. There is also a consideration regarding the ethics of these models that they should not be able to withstand adversaries' attacks [18].

To sum up, it is apparent that hybrid deep learning models have room for improvement in deriving encryptions and countering side-channel attacks, but there are still some unaddressed issues. These are steps towards developing capabilities to withstand adversarial attacks, improving the models' efficiency in practical applications, and making them robust to hardware and environmental changes. There is potential, however, that hybrid encryption approaches may be exploited to provide enhanced security, but this needs to be developed [18].

It stresses the importance of a critical feature for the security of cloud computing and effectively points out comprehensive progress made towards cloud security covering a promising approach which uses a hybrid encryption with improved AuthPrivacyChain. This promising approach improves cloud data security with the usage of both symmetric and asymmetric encryption, access control, and prevention against unauthorized access [19].

The proposed approach shall be AuthPrivacyChain, which makes use of a blockchain-based access control system. To achieve a good balance between security and performance, it introduces a hybrid encryption

architecture. The need for advanced encryption techniques such as attribute-based encryption, homomorphic encryption, and multi-party computing, that shall be proved to be of paramount importance to reinforce cloud data security, is demonstrated. Blockchain adds value to authenticated transactions within the AuthPrivacyChain framework in terms of improving privacy and accountability [19].

One key challenge is scalability. This research article discusses over 50 research publications that review how cloud security can meet the complexity and volume or data in cloud environments. It presents the hybrid encryption model as a solution to the traditional mode of encryption. The approach has been shown to be scalable wherein, though security standards remain strict, increasing demands are kept under control [20].

The study forms a valuable input not only to the cloud security researchers and industry professionals but also to policymakers regarding protecting cloud data and setting a foundation for future innovation. Above all, it will be of good evidence for scalable, resilient, and adaptive cloud security solutions as cyber security threats evolve [20].

IV. Applications

1. **Data Encryption:** The encryption process transforms the primary data into encoded data in the presence of a symmetric key cryptographic algorithm called Blowfish. It needs a private key to encode as well as to decode the data. The transmission of the private key over the web can be fully avoided if an asymmetric key cryptographic system named RSA encrypts the private key. Blowfish deals with the data encryption and decryption with the help of a private key, which is transmitted well with the assistance of RSA. SHA-2 is also used for digital signatures to ensure data integrity and authenticity: Secure Hash Algorithm-2 imposes the enforcement of message authentication, so that a third party cannot alter data in transit [21]. Block diagram of encryption of data is shown in figure 3.

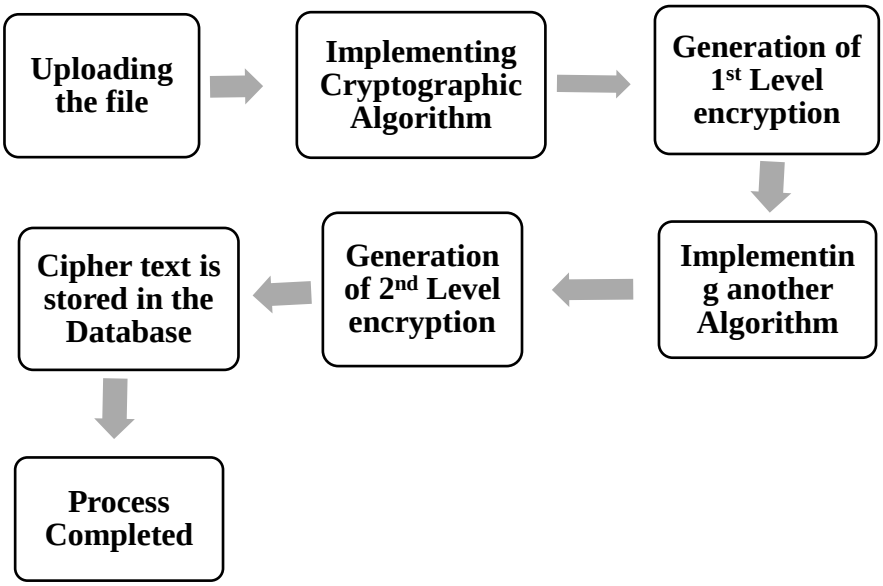


Fig. 3 Block diagram of encryption of data [22]

2. **Secure Key Management:** It involves using asymmetric encryption to safely exchange and manage the keys used in symmetric encryption. In symmetric encryption, the same key is used to both encrypt and decrypt data, but securely transmitting this key over a network can be risky. To solve this, asymmetric encryption is used. Asymmetric encryption uses two keys: a public key and a private key. This symmetric key is encrypted by the public key of the recipient; therefore, it is sent safely. The private key for decrypting the symmetric key is owned only by the recipient, and without the respective private key, the

recipient is unable to decrypt the symmetric key to perform data encryption and decryption on it. This prevents intercepted communications because the symmetric key cannot be intercepted. In this case, the leakage of any symmetric key can only occur in the initial transmission after establishing contact between communication parties [23].

3. \\TAccess Control: Role-based access controls (RBAC), which forms the basis for the implementation of access control through its use of encrypted tokens or credentials, is made to ensure that no unauthorized users of resources in the cloud are able to access it because under RBAC, users are assigned given roles which are based on specific responsibilities, and each role has given permissions. The user's authentication can be done using encrypted tokens or credentials to strengthen security. The tokens contain encrypted information about identity and roles of the user, and the cloud system verifies them before granting permission to access. With the use of encrypted tokens, unauthorized access is prevented because only legitimate, encrypted credentials are what give users their respective resources, ensuring safe and controlled access to sensitive cloud services. [24].
4. **Data Integrity:** In cloud security, data integrity is ensured so that the same data was neither modified nor manipulated during either its storage or transmission. Cryptographic hash functions play an important role by computing a unique output known as a hash from the original data, which is fixed in size. Any small change in data results in a completely different hash and thus becomes tamper-evident. This process, especially when combined with encryption, becomes all the more secure. This is where confidentiality matters-thanks to data encryption-and authenticity is ensured through the hash. For instance, before sending the data into a cloud, the sender first creates a hash of the original data and then sends both the data encrypted and the hash itself. When the recipient receives the data, he will be able to ensure the integrity and authenticity of its data by recomputing the hash value and comparing it with the original. [25].

V. Key Findings from Past Studies

The following table 1. summarizes some advanced cryptographic techniques proposed for cloud and data security: Main Features Application Domains Advantages Limitations First, hybrid encryption models such as AES-OTP and RSA leads to a multi-level encryption process, following by privacy-by-design principles in AI systems. The table underscores the increasing need for strong, flexible encryption systems to protect data in diverse environments such as cloud computing, multi-cloud storage, and digital governance. Even though they offer much better security compared to their predecessors, the solutions tend to become much more complex due to key management, processing overhead, and regulatory compliance.

Table 1: Comparative Analysis of Advanced Cryptographic Techniques in Cloud and Data Security

Reference	Encryption Technique	Key Features	Application Domain	Advantages	Limitations
D. Shivarama Krishna et al. (2023) [26]	Hybrid AES-OTP with RSA, Adaptive Key Management, Time-Limited Access	Adaptive key management, temporal access control, RSA and AES-OTP hybrid encryption	Cloud data storage	High accuracy (99.12%), robust key management, enhanced security	Increased complexity due to adaptive key management
NN Abdulrazaq (2024) [27]	Modified AES-CBC, OTP, and RSA	Encryption tailored for Kurdish alphabet, OTP for added randomness	Digital governance in Kurdistan region	Effective encryption for Kurdish alphabet, secure key transmission	Limited applicability to specific alphabets, complex RSA computation
Harish Naik Bheemanaik	Improved RSA (IRSA)	IRSA for multi-cloud	Multi-cloud storage (AWS,	Better encryption and	Complexity in key

et al. (2024) [28]		security, AWS-IAM for secure access	Google Cloud)	decryption times, secure multi-cloud handling	management and tracking across cloud platforms
Gayatri Kapil et al. (2020) [29]	Attribute-Based Honey Encryption (ABHE)	Combines attribute-based encryption with honey encryption	Big data storage in Hadoop (HDFS)	Improved performance with large files, effective for Hadoop systems	Performance decreases for smaller files
Shuang Wang et al. (2024) [30]	Data Encryption with robust access control	Cybersecurity, continuous threat monitoring, access control	Banking sector, data privacy protection	Improved data encryption strategies, regulatory compliance	Difficulty in integrating legacy systems
Okon et al. (2024) [31]	Privacy by Design (PbD), Logistic Regression	PbD principles integrated with AI systems for enhanced privacy protection	AI systems, cloud environments	Strong correlation between PbD and breach detection, comprehensive	High cost of implementation, complex regulatory compliance
Renuka Shone Durge et al. (2024) [32]	Multi-Level Encryption (RSA + AES, Tokenization)	Combines RSA and AES with byte-pair encoding (BPE) tokenization	Digital storage and communication	Stronger data protection via multi-layer encryption, highly secure	Increased processing overhead due to multi-layer encryption

VI. Conclusion

The effort and work on fusion of hybrid cryptographic frameworks have been explored in this paper towards improving cloud data security. The proposed solution has been based on AES, OTP, RSA, and access control mechanisms based on time with the aim of enhancing secure transmission of data in clouds. This trend has gained tremendous momentum due to the widespread use of the Internet of Things (IT); however, growth in this direction leads to increased security needs as a result of intensive complexity and volume with the ever-increasing volume of sensitive data being processed and stored within cloud environments. The proposed hybrid cryptographic model can address all the key security challenges such as data confidentiality, integrity, and access control with the help of the synergies of advantages of symmetric and asymmetric cryptographic techniques. AES is an encryption algorithm that allows bulk data to be efficiently encrypted, and RSA provides for secure key exchange. The addition of an OTP strengthens the encryption even more by making it much more resistant to brute force attacks. By incorporating some forms of temporal access control, the framework guarantees permissions to access data are time-bound, thus adding another layer of security, especially in very dynamic cloud environments. Further, hybrid deep learning models in countering side-channel attacks and improving the accuracy of key predictions, with even noise and variability in the real-world implementations, are discussed. The paper thus considers the tremendous importance of adapting cryptographic techniques according to the evolution of threats in cloud computing, where blockchain-based access control systems, similar to Auth Privacy Chain, offer promising solutions for secure authentication and authorization. The issues identified include scalabilities, data breaches, and insecure APIs, primarily in a multi-tenant cloud environment. These risks - accompanied by a "Foggy Cloud" type of phenomenon, standardized doubts - emphasize that cryptographic

solutions must constantly innovate to replace traditional solutions. In conclusion, the hybrid cryptographic framework developed by this study is a scalable and adaptive solution for the challenges related to Ongoing Cloud Security. It emphasizes that the only feasible approach may be to integrate various encryption techniques along with access control mechanisms to present a balanced, secure, and efficient cloud data security approach. Further research should refine these hybrid models in the future. DSto overcome current limitations, particularly in handling large-scale data and mitigating emerging cybersecurity threats.

VII. References

[1] Mohamed, N. N., Yussoff, Y. M., Saleh, M. A., & Hashim, H. (2020). Hybrid cryptographic approach for internet ofhybrid cryptographic approach for internet ofthings applications: A review. Journal of Information and Communication Technology, 19(3), 279-319. https://doi.org/10.32890/jict2020.19.3.1

[2] Ahmad, S. A., & Garko, A. B. (2019, December). Hybrid cryptography algorithms in cloud computing: A review. In 2019 15th International conference on electronics, computer and computation (ICECCO) (pp. 1-6). IEEE. https://doi.org/10.1109/ICECCO48375.2019.9043254

[3] Ferlie, E.B.; Shortell, S.M. Improving the quality of health care in the United Kingdom and the United States: A framework for change. Milbank Q. 2001, 79, 281–315. https://doi.org/10.3390/electronics10233013

[4] Javadi, S.S.; Razzaque, M.A. Security and privacy in wireless body area networks for health care applications. In Wireless Networks and Security; Springer: Berlin/Heidelberg, Germany, 2013; pp. 165–187. https://doi.org/10.3390/electronics10233013

[5] Farahani, B.; Firouzi, F.; Chang, V.; Badaroglu, M.; Constant, N.; Mankodiya, K. Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. Future Gener. Comput. Syst. 2018, 78, 659–676. https://doi.org/10.3390/electronics10233013

[6] Díaz, M.; Martín, C.; Rubio, B. State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. J. Netw. Comput. Appl. 2016, 67, 99–117. https://doi.org/10.3390/electronics10233013

[7] Khasawneh, Samer & Kadoch, Michel. (2018). Hybrid Cryptography Algorithm with Precomputation for Advanced Metering Infrastructure Networks. Mobile Networks and Applications. 23. 10.1007/s11036-017-0956-0.

[8] Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. Ieee Access, 8, 131723-131740. https://doi.org/10.1109/ACCESS.2020.3009876

[9] Odun-Ayo, I., Ajayi, O., Akanle, B., & Ahuja, R. (2017, December). An overview of data storage in cloud computing. In 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS) (pp. 29-34). IEEE. https://doi.org/10.1109/ICNGCIS.2017.9

[10] Mehmood, M. S., Shahid, M. R., Jamil, A., Ashraf, R., Mahmood, T., & Mehmood, A. (2019, November). A comprehensive literature review of data encryption techniques in cloud computing and IoT environment. In 2019 8th International Conference on Information and Communication Technologies (ICICT) (pp. 54-59). IEEE. https://doi.org/10.1109/ICICT47744.2019.9001945

[11] Jadoon, A. K., Wang, L., Li, T., & Zia, M. A. (2018). Lightweight cryptographic techniques for automotive cybersecurity. Wireless Communications and Mobile Computing, 2018(1), 1640167. https://doi.org/10.1155/2018/1640167

[12] Al Busafi, S., & Kumar, B. (2020, December). Review and analysis of cryptography techniques. In 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART) (pp. 323-327). IEEE. https://doi.org/10.1109/SMART50582.2020.9336792

[13] Maqsood, Faiqa & Ahmed, Muhammad & Mumtaz, Muhammad & Shah, Munam. (2017). Cryptography: A Comparative Analysis for Modern Techniques. International Journal of Advanced Computer Science and Applications. 8. 10.14569/IJACSA.2017.080659.

[14] Bokhari, M. U., & Shallal, Q. M. (2016). A review on symmetric key encryption techniques in cryptography. International journal of computer applications, 147(10).
[15] Aroraa, H., Singhb, S. P., & Prasadc, S. (2023). Analysis of Asymmetric Cryptographic Algorithms: A Review. ASM Group of Institutes, Pune, India, 87.
[16] Salami, Y., Khajevand, V., & Zeinali, E. (2023). Cryptographic algorithms: a review of the literature, weaknesses and open challenges. J. Comput. Robot, 16(2), 46-56.
[17] Thabit, F., Can, O., Aljahdali, A. O., Al-Gaphari, G. H., & Alkhzaimi, H. A. (2023). Cryptography algorithms for enhancing IoT security. Internet of Things, 22, 100759. https://doi.org/10.1016/j.iot.2023.100759
[18] Ahmed, A. A., Hasan, M. K., Aman, A. H., Safie, N., Islam, S., Ahmed, F. R. A., ... & Rzayeva, L. (2024). Review on hybrid deep learning models for enhancing encryption techniques against side channel attacks. IEEE Access.
[19] Ananthakrishna, V., & Yadav, C. S. (2024). Innovations in Cloud Security: Enhanced Hybrid Encryption Approach with AuthPrivacyChain for Enhanced Scalability. Nanotechnology Perceptions, 560-577.
[20] Ghadirli, H. M., Nodehi, A., & Enayatifar, R. (2019). An overview of encryption algorithms in color images. Signal Processing, 164, 163-185. https://doi.org/10.1016/j.sigpro.2019.06.010
[21] L. Kumar and N. Badal, "A Review on Hybrid Encryption in Cloud Computing," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-6, https://doi.org/10.1109/IoT-SIU.2019.8777503
[22] Mahalakshmi, B. & G., Suseendran. (2019). An Analysis of Cloud Computing Issues on Data Integrity, Privacy and Its Current Solutions: Proceedings of ICDMAI 2018, Volume 2. 10.1007/978-981-13-1274-8_35.
[23] Chandramouli, R., Iorga, M., & Chokhani, S. (2013). Cryptographic key management issues and challenges in cloud services. Secure Cloud Computing, 1-30.
[24] Zhang, Y., Deng, R. H., Xu, S., Sun, J., Li, Q., & Zheng, D. (2020). Attribute-based encryption for cloud computing access control: A survey. *ACM Computing Surveys (CSUR)*, *53*(4), 1-41.
[25] Ananthakrishna, V., & Yadav, C. S. (2024). Innovations in Cloud Security: Enhanced Hybrid Encryption Approach with AuthPrivacyChain for Enhanced Scalability. *Nanotechnology Perceptions*, 560-577.
[26] Shivaramakrishna, D., & Nagaratna, M. (2023). A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and Time-Limited access control. Alexandria Engineering Journal, 84, 275-284.
[27] Abdulrazaq, N. N. (2024). A Novel Approach for Safeguarding Kurdish Text Files via Modified AES-OTP and Enhanced RSA Cryptosystem on Unreliable Networks. EURASIAN JOURNAL OF SCIENCE AND ENGINEERING, 10(2), 102-119.
[28] Manjyanaik, H. N. B., Mohanty, R., & Kannan, J. M. (2024). Preserving Confidential Data Using Improved Rivest-Shamir Adleman to Secure Multi-Cloud. International Journal of Intelligent Engineering & Systems, 17(4).
[29] Kapil, G., Agrawal, A., Attaallah, A., Algarni, A., Kumar, R., & Khan, R. A. (2020). Attribute based honey encryption algorithm for securing big data: Hadoop distributed file system perspective. PeerJ Computer Science, 6, e259.
[30] Asif, M., Wang, S., Shahzad, M. F., & Ashfaq, M. (2024). Data Privacy and Cybersecurity Challenges in the Digital Transformation of the Banking Sector. Computers & Security, 104051.
[31] Okon, S. U., Olateju, O. O., Ogungbemi, O. S., Joseph, S. A., Olisa, A. O., & Olaniyi, O. O. (2024). Incorporating Privacy by Design Principles in the Modification of AI Systems in Preventing Breaches across Multiple Environments, Including Public Cloud, Private Cloud, and On-prem. Journal of Engineering Research and Reports, 26(9), 136-158.
[32] Durge, R. S., & Deshmukh, V. M. (2024). Advancing cryptographic security: a novel hybrid AES-RSA model with byte-level tokenization. International Journal of Electrical & Computer Engineering (2088-8708), 14(4).