IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CSAEPP: Design Of An Efficient Channel Security Framework Via Attribute-Based Hybrid Encryption With Privacy Preservation Optimizations

Madhavi Tota[1], Dr. Swapnili Karmore[2]
PhD. Scholar CSE[1], Associate Professor, Department of Data Science[2]
G H Raisoni University, Saikheda[1] , GHRIETN[2]

***Abstract*—** Users may connect with a large number of people at once by exchanging data packets across broadcast communication channels. As the number of interacting nodes increases, it seems that the possibility of spoofing, espionage, and other types of network attacks increases as well. Due to this, far less encryption is needed for node-to-node unicast connections than it is for this data. Several models are capable of playing this function, but they are all limited in their capacity to scale since they compromise the connection's quality of service (QoS) in order to enhance the performance of the encryption. In this book, a unique attribute-based hybrid encryption and privacy protection method is introduced to address this drawback (abbreviated as CSAEEP). The recommended method defends against intermediate assaults by using attribute-based encryption and packet lifetime awareness. This is made possible by combining the initialization vector (IV)-based encryption with the Fernet model. Using data gathered at the node level from all broadcasting nodes, the CSAEEP model creates a broadcast key. There is less chance that sensitive data along the communication chain may be compromised since the broadcast key is produced again after decryption using node-level attributes. In order to further improve the durability of the encryption, IV encryption employs random values for the same key vector. This approach also makes use of network-wide automatic key verification. To better protect encrypted data and maintain differential privacy, an exponential approach is used. This prevents broadcasting parties from unintentionally learning a node's individual identification information. A variety of attack patterns were tried against the proposed model, and its defence mechanisms and quality of service metrics were evaluated. The suggested model was shown to have 23% less latency, 19% stronger attack resistance, and 20% less complexity than methods considered to be state-of-the-art, making it simpler to apply in real-time deployment scenarios.

Keywords*— *Privacy, security, encryption, hybrid, fernet, IV, QoS, Attack.

I. Introduction

Attribute-based encryption (ABE) enables per-node customized encryption by using instantaneous node characteristics such as location, temporal communication performance, and current parametric state, among others. This (ABE) standard allows the underlying network architecture to achieve greater degrees of anonymity by reducing dependency on key-exchange protocols. [1, 2, 3] In this essay, the established ABE paradigm for broadcasting is reviewed and analysed. In this system, several nodes participate in a variety of broadcast-based interactions. Combining the properties of each of these nodes and applying Equation 1 yields a set of broadcast level keys.

$$B_{key} = f\left(\bigcup_{i=1}^{N_{users}} \bigcup_{j=1}^{N_{attribs_i}} A_{i,j} \right) \dots (1)$$

$B_{Key}, f, N_{Users}, N_{Attribs}, and\ A$ in this context stand for the broadcast key, the key's calculation function, the number of users taking part in the broadcast, the number of attributes that can be applied to a single user, and the actual attribute value used for key generation and transmission, respectively via Game Theory Models (GTM) [4, 5, 6]. The broadcast key is sent to the encryption process, which is secure against all known threats, after converting input data into cypher form (both local and remote). The network uses a wide range of privacy preservation strategies in addition to broadcast encryption to reduce the risk of communication attacks. In the next section, we will take a broad look at these models, emphasizing their distinguishing qualities, limitations, and suggestions for more study. Researchers will find the best models for a certain network application with the help of this discussion. The most safe and private approaches according to this analysis are differential privacy models and symmetric key encryption. Part 3 describes the internal operations of a special attribute-based hybrid encryption & privacy preservation architecture for safeguarding broadcast communication channels. In Section 4, we assess the parametric performance of the suggested model and contrast it with several cutting-edge methods. This study concludes with several illuminating conclusions about the proposed paradigm and ideas for development in future use cases.

II. Literature Survey

Several different models of system have been suggested in an effort to improve the efficiency of individual safety and security during the course of the conversation. The level of difficulty involved in calculating these figures, the level of safety they provide, the level of quality of service (QoS) they provide, and the scope of the area in which they can be implemented are all distinct characteristics of each of these approaches. Examples of models that help deploy models with low key exchange overheads include Ciphertext-Policy Attribute Based-Encryption (CPABE), Integrated Broadcast Attribute Based Encryption (IB ABE), Outsourced Attribute Based Ranked Searchable Encryption (ABRE), and Pairing Free Attribute Based Encryption (PF ABE). These models were proposed in [7, 8]. These models take into consideration the requirements of the end user as they exist right now in order to develop encryption and data privacy standards [9, 10] that offer sufficient protection while maintaining a degree of service quality that is acceptable. With the assistance of ABE in dynamic groups [11, 12] and the Lattice-Based Key-Policy ABE Model via Chaos Engineering (CE) [13, 14], designers of network communication and security model designs are able to reduce latencies and decrease the number of duplicates used in their models. This improves the Quality-of-Service (QoS) performance of the products. Using keyless data protection, the writers of an innovative combined Concealed Ciphertext Policy based ABE (HCP ABE) suggest using a rapid deciphering methodology in [7]. The model outperforms other methods of security and privacy protection in terms of assault resistance and quality of service performance. As a result, it is appropriate for use in the construction of high-security networks that are capable of functioning in real time. Attribute-Based Access Control Models, Profile Matching via Private Identity-based Data Exchange, and Revocable Cloud-Assisted ABE are some of the models that are suggested in [15, 16, 17, 18] that are analogous to one another. The context-aware quality of service (QoS) of a system can be improved by its programmers by taking advantage of these models, which are widely used in applications such as file-sharing and transportation.

Methods that provide application-specific security to different communication interfaces, such as Attribute and Time Conditions based Encryption (ATCE) via Integrated Knowledge Graph (IKG) [19, 20], fine grained identity-based broadcast model via proxy re-encryption [21, 22, 23, 24], Collusion-Resistant Conditional Access Model [25, 26, 27, 28], broadcast group key management [29, 30, 31, 32], and Location-Aware Authorization Model (LAAM) [33, 34, 35, 36], are able to further improve the security performance of existing cyber physical system models. Because these versions experience a low rate of packet mistakes, they are able to achieve a high conversational speed. This, in turn, helps to reduce the number of times that packets need to be resent when exchanging data. Similar application-specific privacy preservation schemes were proposed by the researchers in [37, 38]. These schemes made use of Friendly CryptoJam for full frame encryption and Modulation obfuscation, blockchain in peer-to-peer (P2P) mode for faster and more reliable broadcasts, and privacy preservation using social-assisted content dissemination models to address domain-specific security and privacy concerns. These models, when implemented for a particular use case, provide outstanding performance in terms of onslaught resilience and QoS factors; however, because of the context-specific optimization features they possess, they cannot be expanded to bigger networks. As an illustration, the research presented in [39, 40] that suggests unlimited key Policy ABE and black box surveillance, ABE with blockchain, and policy-based broadcast access and authentication models can all contribute to the sustainability of the system. Because of how well these models operate in context-free software, they are able to be utilised to safeguard the personal information of members of numerous networks. However, due to complications with key transmission, data synchronisation, and the complexity of the processing, these approaches can only provide a basic level of quality of service. These problems can be alleviated and the quality of service improved by employing models such as secure gateway servers [22], verifiable and accountable access control [23], security level aware information exchange via customized ABE [24], and reciprocal data communication [25]. These instruments make it possible to generate keys while travelling and require very little to no synchronisation between the communicating nodes. However, these models do not have the durability and resistance to assaults that are seen in their competitors' models. Their competitors' models enable for interactions based on applications and have restricted QoS. According to the findings of this study, numerous models have been suggested to enhance the privacy and security of cyber-physical systems; however, the vast majority of these models sacrifice either quality of service (QoS) or security (security) in order to achieve their goals. Because of this, scaling the options and putting them into practice won't be nearly as simple. The following section makes a suggestion that, in order to address this shortcoming, an ABE model with hybrid encryption and differential privacy should be developed, and then the model's performance should be evaluated using a variety of network and node configurations.

III. Design of the Proposed Attribute-Based Hybrid Encryption & Privacy Preservation Framework for Securing Broadcast Communication Channels

According to the findings of an analysis of the pertinent literature, the packet size that is currently utilised in contemporary methods for the preservation of anonymity and the encryption of broadcasts is directly proportionate to the transmission delay. The effectiveness of real-time delay-aware interactions is hindered as a result of this latency, which grows at a rapid rate in proportion to the number of messages. In this segment, an innovative attribute-based hybrid encryption methodology that circumvents this deficiency is introduced and discussed. The suggested technique enhances the efficiency of security by combining dual encryption with key generation that is based on the characteristics of individual nodes. Because it eliminates the need for confidential information to be passed back and forth between the parties involved, attribute-based encryption dramatically improves both the speed and storing capacity of communications. Figure 1 illustrates the procedure that would be followed by the suggested framework. It demonstrates that all incoming data is subjected to an asymmetrical privacy protection layer, which strengthens security at the node level. The strategy makes it exceedingly clear that requests for user contact information are made accessible in the cloud, and it does so in a very straightforward manner. In response to these requests, the storage layer retrieves the required data and transmits it to a private differential layer, where it is processed using a large number of segments whose sizes are increasing at an exponential rate. The spectator receives data for assessment based on these segments, which are displayed to them. The user has the option of choosing to use either unicast or disseminate encryption while they are in the process of making a communication request. Because of this, it is necessary to employ a composite encryption layer, which, prior to the data's storage on the computer, protects the information using both Fernet and IV-based techniques. At the moment of delivery, the mixed-cipher procedure is started, and instantaneous passcode generation based on characteristics is performed for different scenarios.

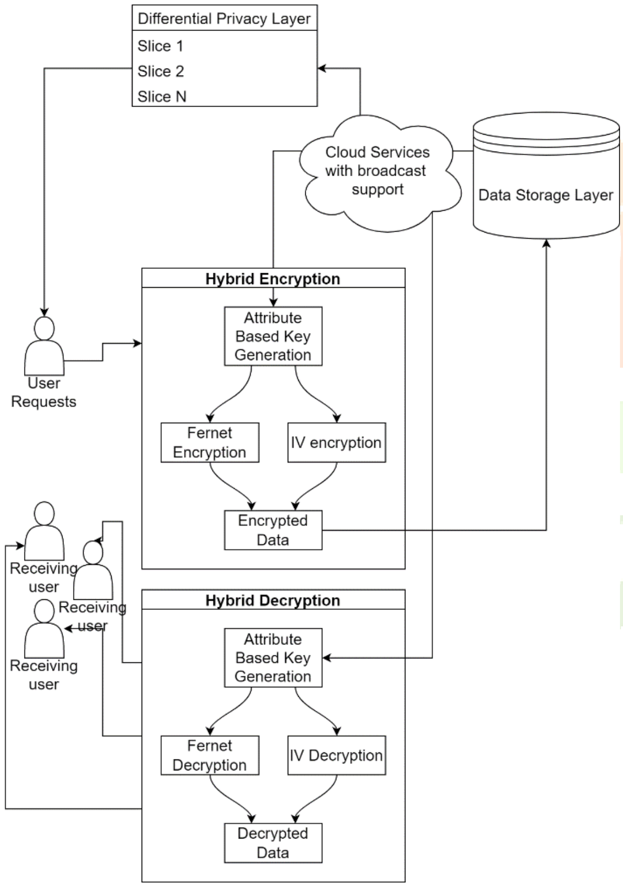

Figure 1. Flow of the proposed model for improving security in cloud deployments

Using these passphrases, it is possible to decrypt unicast transmissions and transmit data in a private and effective manner. The instantaneous generation of keys makes it possible for connections of this type to accomplish both high velocities and high throughputs simultaneously.

An attribute-based passcode is generated while the encrypting and deciphering procedures are being carried out. The characteristics of each of the organisations that were discussed in this conversation have been compiled into this key. Cryptanalysis of these keys is made challenging by the fact that they are used in real time and that there are a large number of participants. Algorithm 2 is what we use to encrypt and decipher a communication that is being passed around between N different individuals.

$$K_{out} = \bigcup_{i=1}^{N} \sum_{j=1}^{N_a} f(Att_{i,j}) \dots (2)$$

Where, K_{out}, N_a, f, Att gives information about the final key, including the number of attributes used, the technique used to generate the key, the attribute values, and the number of attributes used. The solution to Equation 3 yields the following information about the function for key Generation as follows,

$$f\left(Att_{U,A}\right) = B64\left(Fold\left(\bigcap_{i=1}^{N_k} SHA256\left(Att_{U,A}\right)_i\right)\right) \dots (3)$$

Hashing the input data with the provided hashing algorithm is what SHA256 does. However, B64 transforms the input data to base64 format, Fold uses consecutive ANDing of surplus characters to constrain the generated data to 256 bytes, and Nk signifies the number of keys made through hashing. In this section, we will demonstrate how to determine the Fold function by utilising Equation 4,

$$Fold_i(x) = \bigwedge_{j=i+256}^{N} x_i \,\&\, x_j \dots (4)$$

where xi is a character that was taken from the input data and N is the overall number of characters that were taken from the input data. The SHA256 hashing algorithm can be computed with the aid of the following equation,

$$SHA256(x) = 2 * T_1(x) + T_2(x) \dots (5)$$

Where, $T_1, and\ T_2$ are calculated via equations 6 & 7 as follows,

$$T_1(x)_{current} = \sum_{i=1}^{256} T_1(x_i)_{previous} + CH(x_i) + x_i + w_i(x) \dots (6)$$

$$T_2(x)_{current} = \sum_{i=1}^{256} T_2(x_i)_{previous} + Maj(x_i) \dots (7)$$

Where, w is a weight factor value, and is estimated via equation 8,

$$w_i(x) = ROT^6(x) \oplus ROT^{11}(x) \bigoplus ROT^{25}(x) \dots (8)$$

Where, ROT^i is number of i rotations. Similarly, CH & Maj are calculated via equations 9 & 10 as follows,

$$CH_i = T_{1_{i-1}} \bigoplus T_{2_{i-1}} \dots (9)$$

$$Maj_i = T_{1_{i-1}} \otimes T_{2_{i-1}} \dots (10)$$

Based on the results of this analysis, we produce keys that can be utilised within the initialization vector (IV) and Fernet encryption techniques. The following portion of this book devotes its attention to discussing these various approaches.

A combination technique that combines IV encryption and Fernet encryption is used to protect the data before it is finally transferred. Equation 11 is used to perform an analysis of this cryptography. This equation demonstrates how the IV model and the Fernet model can be used together for efficient encryption performance under real-time scenarios.

$$Enc_{out} = IV(Fernet(IN_{data}, K_{out}), K_{out}[0]) \dots (11)$$

Where, $Enc_{out}, IN_{data}, and\ K_{out}[0]$ locates the beginning of the encrypted output data, the original text input data, and the attribute-based key that was generated. recognises the beginning of the encrypted output data samples. The calculation for IV is done using equation 12, which is as follows,

$$IV_i(x,k) = E^k\left(x_i, IV_{i-1}(x,k)\right) \dots (12)$$

Where, $IV_0(x,k) = k$, and E^k is the encryption look-up table, which is estimated via equation 13,

$$E^k(x,y) = random(x,y), and$$

$$E^k(x,y) \in \bigcup_{i=1}^{N} E^i(x,y) \dots (13)$$

N is the total number of items that have been successfully encrypted by using IV up until this point. The data that has been obtained is then further compressed with the help of Equation 14, which is used by the Fernet model, as follows,

$$Fernet(x,k)_i = XOR(Fernet(x,k)_{i-1}, w_i) \dots (14)$$

Where, w is the weight which is calculated via equation 15,

$$w_i = k_i \bigoplus k_{i+1} \bigoplus k_{i+2} \bigoplus k_{i+3} \dots (15)$$

Eight repetitions of Fernet are applied to each keyset, resulting in 256 bits of output for each set of 32 bytes. This is accomplished by having the buffer group of the received data set to PKCS7. The g matrix is utilised in order to generate findings, which are subsequently input into the procedure for the ultimate data transmission. Radio conversations can be conducted without risk if the data are encrypted and other types of sensitive data are also used. Before the data are presented to the user, they are altered using exponential sampling across a number of different database categories. This is done to safeguard the confidentiality of the users. In order to complete this work, you will need to use an exponential classification to evaluate and contrast the various categories and entries contained in your database. The security of the data will be improved if the columns and rows are sorted into increasing rank order based on this number. The user is provided with immediate access to the confidential information, which assists them in making the decision regarding whether to communicate with unicast or disseminated companions. With the help of Equation 16, we are able to establish a preferred retrieval order as well as rate the user data items.

$$R(X|Y) = \frac{\sum_{i=1}^{N_c} R(X,i)}{\sum_{i=1}^{N_c} R(Y,i)} \dots (16)$$

The following is an assessment of R(X,i), which is the objective number for row X in relation to column I and is based on equation 17,

$$R(X,c) = \frac{\exp\left(\frac{\in}{2} * f(X,c)\right)}{\int_{p=1}^{R} \exp\left(\frac{\in}{2} * f(X,p).dp\right)} \dots (17)$$

Where, $\in, f \ and \ R$ is the privacy function, along with the overall number of elements in the collection and the exponential privacy constant. The private function is computed by Equation 18, which takes into account the differences between the different column categories.

$$f(X,m) = \sqrt{\frac{\sum_{j=1}^{m}(x_j - \frac{\sum_{k=1}^{m} x_k}{m})^2}{m-1}} \dots (18)$$

The result of this difference is converted into an exponential number, and then a classification is established between each row and column. With the assistance of equation 19, we will be able to shuffle these portions around at the beginning of each new round of iterations.

$$\in = random(timestamp \oplus iteration) \dots (19)$$

The utilisation of differential exponential encryption in conjunction with random value sampling has resulted in extremely unreliable incoming data. This makes it challenging for any potential adversary, whether they come from the inside or the outside. Data contact is established between a large number of computers, and the outcomes are analysed using a variety of measures, including those pertaining to transmission latency, Memory consumption, and assault resistance precision. In the following part of the article, we are going to compare these findings to the models that were evaluated for different use cases.

IV. Result evaluation and comparision

The technique that has been suggested combines hybrid encryption with differential exponential privacy in order to provide protection against both internal and exterior threats. Deception and eavesdropping are two instances of this type of assault because the primary objective of both of these methods is to view and modify data sources without the appropriate authorization. Ninety percent of the nodes communicate with one another and the network in either the unicast or disseminate mode. The remaining ten percent of the nodes are malicious and attempt to eavesdrop on the communications without authorizations.

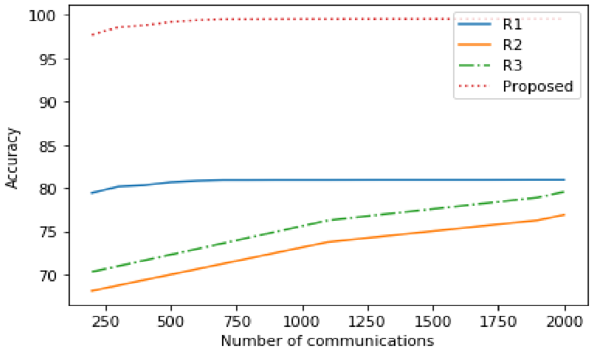

Figure 2: Accuracy of detecting different attacks

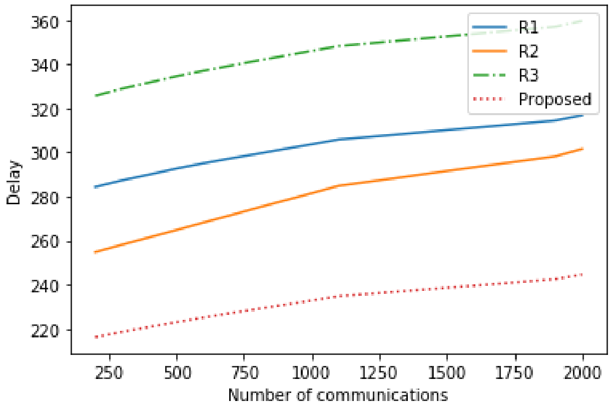

Figure 3: Delay needed to detect these attacks

Communication was carried out between a total of 200 sites, and the number of messages ranged linearly from 100 all the way up to 2000. Throughout the course of each communication, the typical end-to-end latency (D), memory consumption (M), and precision of assault detection (A) were measured, then compared to the GTM [5], CE [14], and IKG [20] models. For example, table 1 demonstrates the values of the precision of assault identification (A) for varying numbers of communications (NC) and various models.

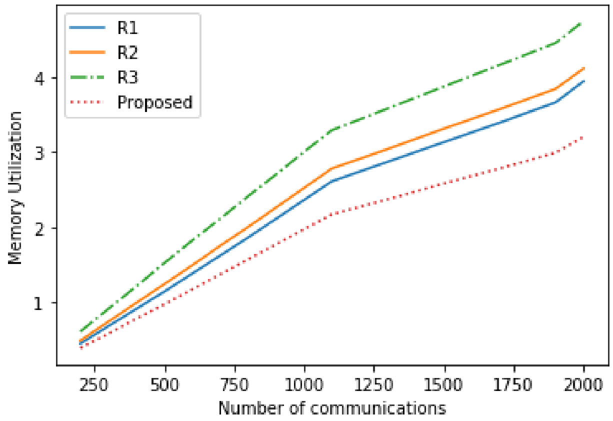

Figure 4: Memory needed to identify different attacks

Equations 20, 21, and 22 are utilised in order to determine the accuracy (represented by the letter A), the typical end-to-end duration (D), and the memory utilization (M) levels,

$$A = \sum_{i=1}^{N(Attacks)} \frac{A(Detected)}{A(Total) * N(Attacks)} \ldots (20)$$

$$D = \sum_{i=1}^{N_C} \frac{t_{finish_i} - t_{start_i}}{N_C} \ldots (21)$$

$$M = \sum_{i=1}^{N_C} \frac{M_{before_i} - M_{after_i}}{N_C} \ldots (22)$$

Where tfinish, tstart, Mafter, Mbefore, NC, and A(Detected), A(Total), and N(Attacks) stand for the total number of communications, assaults, and attacks discovered, done, and present in the system model, respectively, during the assessment process. Based on Figure 2's accuracy figures, it can be deduced that the proposed model is 20%, 23%, and 19% more accurate than GTM [5], CE [14], and IKG [20] when it comes to the detection of actual attacks in progress. As a result, it can be implemented in practically attack-proof network software. Figure 2 displays the corresponding data for assault identification accuracy (A) across various call numbers (NC) and approaches. Figure 3 displays the delay times for each model, demonstrating that the suggested model is 23% faster than GTM [5], 20% faster than CE [14], and 33% faster than IKG [20]. Because of this, it can be utilised for high-capacity and high-efficiency network applications. This time savings is possible thanks to the use of attribute-based encryption in tandem with dynamic key generation. In a manner analogous to how the memory utilization of each model is analysed to evaluate computational intricacy. Image 3 of this comparison shows that when compared to GTM [5], CE [14], and IKG [20], the proposed model has a 20% reduced computational complexity. It's useful for low-priced application setups because of the absence of high-speed processor methods in these environments. The results of the assessment show that the proposed model is more secure than competing cutting-edge models and requires less complex and faster processing. The technique enables instantaneous network deployments.

V. Conclusion

The CSAEEP paradigm was suggested to enhance assault resilience and communication efficiency. Multiple layers of cryptography and other private safeguards are built in. Using two straightforward encryption models and an attribute-based key generation method, the suggested model improves data transmission efficiency. It is possible to further reduce this latency by employing on-the-fly key generation, which facilitates communication between data senders and receivers. The suggested method is praised for its efficient use of Memory across all cryptographic and privacy-protecting operations. Furthermore, it is easier to implement than many methods that are currently considered cutting edge. Real-time assault identification is where the suggested model shines, where it outperforms the previous state-of-the-art by 20% compared to IKG [20], 23% compared to CE [14], and 19% compared to IKG [20]. In turn, this can be put to use in the development of extremely secure network applications. According to the delay assessment, the transmission speed of the suggested model is 23% faster than GTM [5], 20% faster than CE [14], and 33% faster than IKG [20]. This allows its use in high-volume, high-performance network applications. Advantageous for low-cost programme implementations is the suggested model's computational complexity, which is reduced by 20%, 24%, and 37%, compared to that of GTM [5], CE [14], and IKG [20], respectively. Memory utilisation assessment metrics provide evidence of this. Using bioinspired models, researchers can determine which future cryptography and hidden security methods will be most effective. Distributed encryption can be improved by incorporating deep learning algorithms to make it more robust against a broader set of network threats. It's not impossible to raise the bar to this level with other encryption techniques.

REFERENCES

[1] W. Qiao et al., "A Novel Method for Resource Efficient Security Service Chain Embedding Oriented to Cloud Datacenter Networks," in IEEE Access, vol. 9, pp. 77307-77324, 2021, doi: 10.1109/ACCESS.2021.3082644.

[2] M. Yang, T. Gao, W. Xie, L. Jia and T. Zhang, "The Assessment of Cloud Service Trustworthiness State Based on D-S Theory and Markov Chain," in IEEE Access, vol. 10, pp. 68618-68632, 2022, doi: 10.1109/ACCESS.2022.3185684.

[3] T. Wang, Y. Liang, Y. Tian, M. Z. A. Bhuiyan, A. Liu and A. T. Asyhari, "Solving Coupling Security Problem for Sustainable Sensor-Cloud Systems Based on Fog Computing," in IEEE Transactions on Sustainable Computing, vol. 6, no. 1, pp. 43-53, 1 Jan.-March 2021, doi: 10.1109/TSUSC.2019.2904651.

[4] S. An, A. Leung, J. B. Hong, T. Eom and J. S. Park, "Toward Automated Security Analysis and Enforcement for Cloud Computing Using Graphical Models for Security," in IEEE Access, vol. 10, pp. 75117-75134, 2022, doi: 10.1109/ACCESS.2022.3190545.

[5] T. Halabi and M. Bellaiche, "Towards Security-Based Formation of Cloud Federations: A Game Theoretical Approach," in IEEE Transactions on Cloud Computing, vol. 8, no. 3, pp. 928-942, 1 July-Sept. 2020, doi: 10.1109/TCC.2018.2820715.

[6] J. -S. Shin and J. Kim, "SmartX Multi-Sec: A Visibility-Centric Multi-Tiered Security Framework for Multi-Site Cloud-Native Edge Clusters," in IEEE Access, vol. 9, pp. 134208-134222, 2021, doi: 10.1109/ACCESS.2021.3115523.

[7] K. Zhang, Z. Jiang, J. Ning and X. Huang, "Subversion-Resistant and Consistent Attribute-Based Keyword Search for Secure Cloud Storage," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1771-1784, 2022, doi: 10.1109/TIFS.2022.3172627.

[8] R. Alturki et al., "Sensor-Cloud Architecture: A Taxonomy of Security Issues in Cloud-Assisted Sensor Networks," in IEEE Access, vol. 9, pp. 89344-89359, 2021, doi: 10.1109/ACCESS.2021.3088225.

[9] S. Majumdar et al., "ProSAS: Proactive Security Auditing System for Clouds," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 4, pp. 2517-2534, 1 July-Aug. 2022, doi: 10.1109/TDSC.2021.3062204.

[10] S. Feng, Z. Xiong, D. Niyato, P. Wang, S. S. Wang and S. X. Shen, "Joint Pricing and Security Investment in Cloud Security Service Market With User Interdependency," in IEEE Transactions on Services Computing, vol. 15, no. 3, pp. 1461-1472, 1 May-June 2022, doi: 10.1109/TSC.2020.2996382.

[11] A. Nhlabatsi et al., "Threat-Specific Security Risk Evaluation in the Cloud," in IEEE Transactions on Cloud Computing, vol. 9, no. 2, pp. 793-806, 1 April-June 2021, doi: 10.1109/TCC.2018.2883063.

[12] F. M. Awaysheh, M. N. Aladwan, M. Alazab, S. Alawadi, J. C. Cabaleiro and T. F. Pena, "Security by Design for Big Data Frameworks Over Cloud Computing," in IEEE Transactions on Engineering Management, vol. 69, no. 6, pp. 3676-3693, Dec. 2022, doi: 10.1109/TEM.2020.3045661.

[13] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami and M. Ayaz, "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies," in IEEE Access, vol. 9, pp. 57792-57807, 2021, doi: 10.1109/ACCESS.2021.3073203.

[14] K. A. Torkura, M. I. H. Sukmana, F. Cheng and C. Meinel, "CloudStrike: Chaos Engineering for Security and Resiliency in Cloud Infrastructure," in IEEE Access, vol. 8, pp. 123044-123060, 2020, doi: 10.1109/ACCESS.2020.3007338.

[15] W. Zeng and M. Koutny, "Quantitative Analysis of Opacity in Cloud Computing Systems," in IEEE Transactions on Cloud Computing, vol. 9, no. 3, pp. 1210-1219, 1 July-Sept. 2021, doi: 10.1109/TCC.2019.2894768.

[16] P. Mishra, V. Varadharajan, E. S. Pilli and U. Tupakula, "VMGuard: A VMI-Based Security Architecture for Intrusion Detection in Cloud Environment," in IEEE Transactions on Cloud Computing, vol. 8, no. 3, pp. 957-971, 1 July-Sept. 2020, doi: 10.1109/TCC.2018.2829202.

[17] J. Srinivas, A. K. Das, N. Kumar and J. J. P. C. Rodrigues, "Cloud Centric Authentication for Wearable Healthcare Monitoring System," in IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 5, pp. 942-956, 1 Sept.-Oct. 2020, doi: 10.1109/TDSC.2018.2828306.

[18] J. Srinivas, A. K. Das, N. Kumar and J. J. P. C. Rodrigues, "Cloud Centric Authentication for Wearable Healthcare Monitoring System," in IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 5, pp. 942-956, 1 Sept.-Oct. 2020, doi: 10.1109/TDSC.2018.2828306.

[19] J. -N. Liu et al., "Enabling Efficient, Secure and Privacy-Preserving Mobile Cloud Storage," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 3, pp. 1518-1531, 1 May-June 2022, doi: 10.1109/TDSC.2020.3027579.

[20] K. P. Joshi, L. Elluri and A. Nagar, "An Integrated Knowledge Graph to Automate Cloud Data Compliance," in IEEE Access, vol. 8, pp. 148541-148555, 2020, doi: 10.1109/ACCESS.2020.3008964.

[21] H. Alavizadeh, S. Aref, D. S. Kim and J. Jang-Jaccard, "Evaluating the Security and Economic Effects of Moving Target Defense Techniques on the Cloud," in IEEE Transactions on Emerging Topics in Computing, vol. 10, no. 4, pp. 1772-1788, 1 Oct.-Dec. 2022, doi: 10.1109/TETC.2022.3155272.

[22] X. Li, S. Liu, R. Lu, M. K. Khan, K. Gu and X. Zhang, "An Efficient Privacy-Preserving Public Auditing Protocol for Cloud-Based Medical Storage System," in IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 5, pp. 2020-2031, May 2022, doi: 10.1109/JBHI.2022.3140831.

[23] Z. Wen, R. Qasha, Z. Li, R. Ranjan, P. Watson and A. Romanovsky, "Dynamically Partitioning Workflow over Federated Clouds for Optimising the Monetary Cost and Handling Run-Time Failures," in IEEE Transactions on Cloud Computing, vol. 8, no. 4, pp. 1093-1107, 1 Oct.-Dec. 2020, doi: 10.1109/TCC.2016.2603477.

[24] M. Shabbir et al., "Enhancing Security of Health Information Using Modular Encryption Standard in Mobile Cloud Computing," in IEEE Access, vol. 9, pp. 8820-8834, 2021, doi: 10.1109/ACCESS.2021.3049564.

[25] W. Qiang, W. Chunming, Y. Xincheng and C. Qiumei, "Intrinsic Security and Self-Adaptive Cooperative Protection Enabling Cloud Native Network Slicing," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1287-1304, June 2021, doi: 10.1109/TNSM.2021.3071774.

[26] H. Jin, Z. Li, D. Zou and B. Yuan, "DSEOM: A Framework for Dynamic Security Evaluation and Optimization of MTD in Container-Based Cloud," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 3, pp. 1125-1136, 1 May-June 2021, doi: 10.1109/TDSC.2019.2916666.

[27] H. Zhong, C. Zhang, J. Cui, Y. Xu and L. Liu, "Authentication and Key Agreement Based on Anonymous Identity for Peer-to-Peer Cloud," in IEEE Transactions on Cloud Computing, vol. 10, no. 3, pp. 1592-1603, 1 July-Sept. 2022, doi: 10.1109/TCC.2020.3004334.

[28] D. K. Sharma, K. K. Bhardwaj, S. Banyal, R. Gupta, N. Gupta and L. Nkenyereye, "An Opportunistic Approach for Cloud Service-Based IoT Routing Framework Administering Data, Transaction, and Identity Security," in IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2505-2512, 15 Feb.15, 2022, doi: 10.1109/JIOT.2021.3078810.

[29] J. Li, H. Yan and Y. Zhang, "Efficient Identity-Based Provable Multi-Copy Data Possession in Multi-Cloud Storage," in IEEE Transactions on Cloud Computing, vol. 10, no. 1, pp. 356-365, 1 Jan.-March 2022, doi: 10.1109/TCC.2019.2929045.

[30] K. Huang, X. Zhang, Y. Mu, F. Rezaeibagha and X. Du, "Bidirectional and Malleable Proof-of-Ownership for Large File in Cloud Storage," in IEEE Transactions on Cloud Computing, vol. 10, no. 4, pp. 2351-2365, 1 Oct.-Dec. 2022, doi: 10.1109/TCC.2021.3054751.

[31] X. Zhang, C. Xu, H. Wang, Y. Zhang and S. Wang, "FS-PEKS: Lattice-Based Forward Secure Public-Key Encryption with Keyword Search for Cloud-Assisted Industrial Internet of Things," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 3, pp. 1019-1032, 1 May-June 2021, doi: 10.1109/TDSC.2019.2914117.

[32] U. Ahmed, I. Raza, O. F. Rana and S. A. Hussain, "Aggregated Capability Assessment (AgCA) For CAIQ Enabled Cross-cloud Federation," in IEEE Transactions on Services Computing, vol. 15, no. 5, pp. 2619-2632, 1 Sept.-Oct. 2022, doi: 10.1109/TSC.2021.3073783.

[33] Y. Li et al., "Traceable and Controllable Encrypted Cloud Image Search in Multi-User Settings," in IEEE Transactions on Cloud Computing, vol. 10, no. 4, pp. 2936-2948, 1 Oct.-Dec. 2022, doi: 10.1109/TCC.2020.3034232.

[34] R. Gupta, D. Saxena, I. Gupta and A. K. Singh, "Differential and TriPhase Adaptive Learning-Based Privacy-Preserving Model for Medical Data in Cloud Environment," in IEEE Networking Letters, vol. 4, no. 4, pp. 217-221, Dec. 2022, doi: 10.1109/LNET.2022.3215248.

[35] N. M. Allifah and I. A. Zualkernan, "Ranking Security of IoT-Based Smart Home Consumer Devices," in IEEE Access, vol. 10, pp. 18352-18369, 2022, doi: 10.1109/ACCESS.2022.3148140.

[36] N. Dhakad and J. Kar, "EPPDP: An Efficient Privacy-Preserving Data Possession With Provable Security in Cloud Storage," in IEEE Systems Journal, vol. 16, no. 4, pp. 6658-6668, Dec. 2022, doi: 10.1109/JSYST.2022.3159847.

[37] S. Meng et al., "Security-Aware Dynamic Scheduling for Real-Time Optimization in Cloud-Based Industrial Applications," in IEEE Transactions on Industrial Informatics, vol. 17, no. 6, pp. 4219-4228, June 2021, doi: 10.1109/TII.2020.2995348.

[38] C. Li, C. Xu, S. Li, K. Chen and Y. Miao, "On the Security of Verifiable Searchable Encryption Schemes," in IEEE Transactions on Cloud Computing, vol. 10, no. 4, pp. 2977-2978, 1 Oct.-Dec. 2022, doi: 10.1109/TCC.2021.3071779.

[39] M. Dickinson et al., "Multi-Cloud Performance and Security Driven Federated Workflow Management," in IEEE Transactions on Cloud Computing, vol. 9, no. 1, pp. 240-257, 1 Jan.-March 2021, doi: 10.1109/TCC.2018.2849699.

[40] J. Wang et al., "S-Blocks: Lightweight and Trusted Virtual Security Function With SGX," in IEEE Transactions on Cloud Computing, vol. 10, no. 2, pp. 1082-1099, 1 April-June 2022, doi: 10.1109/TCC.2020.2985045.

.