CLOUD DATA LAYERED PRIVACY AND SECURITY ARCHITECTURE

Henna Abdul Jaleel[1], Rahul P[2]

[1] (Mtech Cyber Security,Department Of Computer Sceience And Engineering,Met's School Of Engineering,Mala

[2] (Assistant Professor,Department Of Computer Sceience And Engineering,Met's School Of Engineering,Mala

ABSTRACT

The cloud owner may be concerned about managing knowledge while keeping its utility and maintaining the security plan. We developed a layer-based architecture to reduce the overhead at the cloud service provider for adding security to each document and then transferring it to the client. This method protects the sensitive document's security and the privacy of its data. The proposed approach categorises data according to its sensitivity to achieve a balance between data security and utility. Different algorithmic schemes are required for various categories' perseverance. We discovered a cloud-based distributed environment in which data is classified into four levels of sensitivity: public, confidential, secret, and top secret, with each level requiring a different approach to ensure data security. We built a provision to detect the malfunctioning node that is responsible for data leakage at the most sensitive layers, such as secret and top secret data. Finally, experimental analysis is used to evaluate the layer-based approach's performance. The experimental results show that when processing 200 documents with a total size of 20 MB, the point taken (in ms) for public, confidential, secret, and top secret data is 437, 2239, 3142, 3900 for public, confidential, secret, and top secret data, respectively, when the documents are distributed among different users.

Keywords **:** *Cloud Computing, Data Leakage, Data Privacy, Data Sensitivity, Information Security, Guilty Client are some of the terms used in this article.*

1. INTRODUCTION.

In today's fast-paced world, it is necessary to exchange organisational information with diverse entities such as employees, business partners, customers, and so on [1], [2], [3]. With the advent of cloud computing technologies, web-based connectivity has been achieved, allowing users to access distributed and scalable computing environments. However, this information is frequently obtained through unauthorised access while being transmitted, or it can be intentionally or mistakenly released by the receiving party, and then it is frequently misused by malevolent actors [4], [5]. It poses a serious risk to the organization's goodwill and reputation [6], [7]. As a result, data security and data leakage detection have become crucial challenges for any company. There is a need for a technique that can protect the confidentiality of the information being transferred and detect the hostile entity that is causing data leakage. However, from 2013 to 2018, the number of cloud users is expected to expand from 2:4 billion to 3:6 billion [8]. As a result, data availability has gradually increased, necessitating security and privacy. To prevent information from being leaked, it is critical to maintain privacy [9]. According to a study, the number of leaked sensitive data records surpassed 1:1 billion between 2011 and 2014. It has continued to rise as the number of cloud users, as well as malevolent users, has grown [10]. As a result, to deal with the rising number of cyberattacks, cybersecurity demands a strategy that will manage, safeguard, and locate harmful agents and activities. Limiting data sharing to ensure security, on the other hand, reduces data utility, which may have an impact on the organization's performance [11], [12]. While transferring data to the cloud and later to the user, security mechanisms are applied to the full data, incurring considerable computational costs. When a greater security system is applied to the total amount of data, security and privacy are frequently violated, and there are frequent chances of knowledge leakage and data misuse. We developed a layer-based security and privacy architecture to reduce overhead while ensuring data security and utility. The focus of previous research has been on sending encrypted data from the owner to the cloud. We improve on typical architectural behaviour by providing a layer-based architecture for safeguarding data that moves between three parties: the cloud, the owner, and the client. The approach to data preservation that we offer in this research is stated to address data utility while assuring data security. Our method maintains privacy and data utility while increasing processing speed and overhead. If no security system is present, security contributes in the following ways: When cloud data is shared across various entities, the article presents a layer-based privacy and security architecture to maintain data confidentiality. To reduce the computational overhead of implementing security.

The layer-based approach divides information into four categories: public, confidential, secret, and top secret. to strike a balance between the usefulness of information and the cost of it At each layer, a unique integrated combination of multiple technologies is used to ensure the privacy and security of all data. The stored data is classified according to its level of confidentiality, and the appropriate level of security is applied when the information is retrieved. For different types of data, the usage and security needs may be quite varied. Furthermore, just in case of a leak, we use the message authentication mechanism to validate the identified leaker. We assess the cost of calculation, i.e. The amount of time it takes to process the document at each tier. Furthermore, it was demonstrated in the experimental evaluation that by effectively sharing information, the computation time can be reduced. The remainder of the paper is laid out as follows: discusses related work, describes the threat model and thus our system's design goals, highlights the proposed model, which is followed by performance evaluation in section V, which explains the experimental analysis and includes the results, and discusses the work's conclusion.

Requirements based on the sensitivity of the information Each successive layer adds to the previous layer's security by providing stronger security. In the case of secret and top secret data, the watermarking technique is used to identify the leaker who is responsible for leaking the sensitive information.

2. CONNECTED WORK

Various organisations are migrating their data to the cloud in today's emerging world due to a long list of benefits. [13], [14] are two examples. Table I and Table II contain the results of the data storage analysis [15], [16], [17], [18]. Table I shows the cloud data storage specifications in percentage terms (%) for normal data (both sensitive and non-sensitive data), with the highest percentage of ‘Relational' data type (with 34 percent). Table II also specifies the storage requirements for sensitive data, with a maximum range of 73 percent customer data being stored in the cloud. As more data is stored in the cloud and shared among users, resilient security services and leakage detection mechanisms are required. Access control mechanisms, cryptography, fingerprinting, probabilistic evaluation, and watermarking are the five categories of proposed solutions in this field. Through access control mechanisms, [19], [20], [21], [22], [23] provide data security and privacy. In [19], data owners form coalitions in order to distribute information in a Secure manner Usage control enforcement systems are described in [20], [21] to ensure the controlled transfer of knowledge in a distributed environment while adhering to well-defined policies. [22], [23] provide access control policies for securing data in a cloud setting. Despite the fact that this method can control the release of sensitive data and protect knowledge. However, this method will not prevent unauthorised access to and misuse of the information. Furthermore, using this method to provide security reduces the data's utility. Cryptography is another method proposed for ensuring the security and privacy of information stored in the cloud. This method is used to protect data during transmission from unauthorised disclosure. The goal of the strategy is to make it difficult for malicious entities to access the information. [4], [5], [6], [7], [8], [9], [3], [10], [12], [13], [14], [17], [18], [19]. Cloud is a user-centric key management scheme proposed by Kao et al. [25]. It protects the keys by storing private keys on the user's mobile devices and displaying them through 2D barcode images. Later, Qin et al. proposed a PKE-based approach to control .

Because of the lower maintenance costs of specialised data centres, outsourcing such services to a third party may be a more logical option. [12], [13] proposed Ciphertext-Policy Attribute-Based Signcryption for safe exchange of private Health Records (PHR) (CP-ABE). This CP. ABE combines the assets of encryption and digital signature to provide collision resistance, unforgeability, and CIA services. Due to high acquisition costs and performance limits, the combination of these two results in an efficient strategy that is unfeasible.

Ciphertext-Policy Attribute-Based Proxy Re-Encryption (CP-ABPRE) was proposed by Liang et al. and is generally applicable for privacy in all types of network sharing applications. By combining dual system encryption technology with a selective proof technique, this effectively addresses the privacy issue. To solve the key escrow problem, attribute authority and key server construct the attribute secret keys of the user using homomorphic encryption in addition to attribute based encryption in an attribute-based secure data sharing scheme with efficient revocation (EABDS). The method stops the entity from accessing the information on its own. By combining the concepts of PKE-ET and CP-ABE approaches, Wang et al. proposed the CP-ABE-ET scheme. The authors presented privacy-preserving reputation systems based on secure multi-party cryptographic approaches for assessing the trustworthiness of commercial entities and autonomous machines in a machine-to-machine network. Without relying on a centralised trusted system, these systems ensure privacy, security, and correctness, as well as public verifiability. For the protection of privacy, a homeomorphic cryptographic system is used. The development of a decentralised reputation aggregation system called "PrivBox" is reported, which secures users' privacy without relying on anonymous identities or trusted systems. With the important traits of decentralisation and privacypreservation, the proposed system has low communication and computation overheads. Azad et al. offer cryptographic protocol-based decentralised collaborative solutions for effectively blocking spammers who target numerous TSPs. The performance of the systems was assessed using synthetic and real-world call detail records. Al-Haj et al. presented two crypto-based techniques using whirlpool hash codes and internally produced symmetric keys to deliver CIA services. As a result, signal distortion is reduced, and the system is more resistant to signal processing attacks. Although the cryptographic approach provides a higher level of security for the information, it does not guarantee that data will not be leaked by the receiving party once the information has been sent to it. When information is leaked to unauthorised access, this strategy is ineffective. Furthermore, it is unable to detect the data breach and the malevolent entity responsible for the data leak. To protect knowledge from unlawful disclosure, a content-based fingerprinting approach is provided. Leakage is identified by extracting the document's patterns and comparing them to the departing documents. The scheme's advantage is that it does not divulge the entire sensitive document to the intermediary party; instead, only a set of keywords is revealed to the semi-honest supplier. However, the system can only detect leaks that are intentionally created by a malevolent party. Another important drawback of the method is that it fails to detect data leakage even when minor changes in data transmission are made. [3], [14], [4] recommended using a probabilistic technique that uses a variety of data distribution algorithms to find the guilty agent. This increases the odds of the distributor catching a leaker. Although the strategy does not rely on data manipulation, the probability method has the drawback of being unable to pinpoint the particular leaker accountable for the data leak. A specific approach known as watermarking has been given for proof of ownership and copyright protection by masking the knowledge [6], [7], [8]. To cover the message within the data, several techniques have been developed. Watermarking is required to hide data using four different formats: Text in Text, Image in Image, Image in Text, and Text in Image. For watermarking is named to process pictures and text bound as I, T, it works over 2n combinations; when n = 2, the pairings are I +I, I +T, T +I, and T + T. Various conventional classifications of this technique are mentioned in [4], [5]. Singh et al. [10] proposed a discrete wavelet transform, Singular Value Decomposition (SVD), and Discrete Cosine Transforms-based digital watermarking technique (DCT). Several well-known attacks have been thoroughly evaluated, yielding reliable and undetectable results when compared to other methods. We utilise a watermarking approach to track out the person or entity who leaked the information. It can pinpoint the hostile entity responsible for data leaking. When information is delivered to the user, this system is unable to secure it from unauthorised disclosure. Because the aforementioned solutions alone are incapable of imposing several security paradigms, different technologies are creatively coupled to meet multiple data security criteria. to get overriding.

To address the aforementioned flaws, we developed a layered-based hybrid strategy that categorises data according to its sensitivity and then applies the appropriate security mechanisms to achieve a considerably better balance between data security and utility while lowering overhead. At each layer, a distinct combination of encryption, watermarking, and hashing algorithms is employed in accordance with the requirements, taking advantage of the advantages of each technology.

The main benefit of our suggested method is that it may be used for any data type that a watermarking scheme can handle, and it can be used with any existing watermarking technique without requiring any changes.

Table-1: CLOUD SENSITIVE DATA STORAGE SPECIFICATIONS IN PERCENTAGE TERMS (percent) 15% of the total

Data type	Percentage	Example
Information that should not be shared (Text, Numbers, Images, Video, Audio)	15	University-conducted legal investigations, sealed bids, etc.
Information that should not be shared (Text, Numbers, Images, Video, Audio)	40	Copyrights, patents,trade-marks, and other intellectual property rights account for of the total.
Customer Information (Relational)	73	Percent of information such as name, company, address, e-mail, and contact info is retained at service centres.
Medical Records (Relational)	8	Patient, Disease, Prescription, and so on.

To protect knowledge from illegal disclosure, a content-based fingerprinting approach is given [20], [21], [22]. Leakage is identified by extracting the document's patterns and comparing them to the departing documents. The scheme's advantage is that it does not divulge the entire sensitive document to the intermediary party; instead, only a set of keywords is revealed to the semi-honest supplier. However, the system can only detect leaks that are intentionally created by a malevolent party. Another important drawback of the method is that it fails to detect data leakage even when minor changes in data transmission are made. [13], [4], [24] preferred to use a probabilistic strategy that employs a variety of data distribution algorithms to find the guilty agent. This increases the odds of the distributor catching a leaker. Although the strategy does not rely on data manipulation, the probability method has the drawback of being unable to pinpoint the particular leaker accountable for the data leak. As we progress from category P to T S, the sensitivity of knowledge grows, necessitating greater security to secure the information than the mechanism at the previous layer. As we progress from layer zero to layer three, each layer adds to the previous layer's security by increasing the safety mechanism.

3. THE MODEL THAT HAS BEEN PROPOSED

The suggested framework lowers the overhead and, as a result, the computational cost of executing operations on all data. Cloud provides a consistent log-in registration for the general public Data (P), with credentials provided by cloud. Cryptography is used to convert data from plain text to cypher text for Confidential Data (C). Cryptography and watermarking procedures are used to safeguard Secret Data (S), resulting in Watermarked Crypto-Document (WCD). Client (Clid): an entity that retrieves information shared by the owner Oid and uses it to accomplish a task. Cloud Server (CSid): an entity that provides a high-quality service by utilising a group of servers (CS1;CS2; : : : ;CSp) with significant computing and storage capacity. In our approach, data flow between the three parties is represented in. When information is exchanged among clients, our security model assesses the most serious danger to cloud data secrecy. In this example, the approach protects data confidentiality by securely sharing cloud data and identifying the malevolent entity responsible for data leaking, potentially lowering the likelihood of data leakage. Clid is a character in our storey.

The model is untrustworthy because it cannot ensure that the intended receiver will not disclose the information once it has been given to them. Also, once the user receives the information, no one can stop him from disclosing it.

The suggested method's purpose is to identify the guilty party in the event of sensitive data leaking. In our scenario, the following attacks will occur: a) Knowledge leakage, which results in the loss of secrecy. b) to prevent the system from detecting the malicious object. As a result, our system views Clid as an attacker who goes to great lengths to disclose personal information without taking responsibility for their actions. Our security model considers the adversary to be a malicious person who may misuse the information and disseminate it in an unauthorised location. Because the sender does not trust the client, the unique code is included in the document whenever it is sent to a client. However, we believe that the client is attempting to obtain this identifying information in order to safely expose the document without being discovered. After embedding the knowledge in the document, the sender may transfer the document to the receiving client, who may maintain a copy of the document with the embedded information, publicise it, and accuse the receiving entity. Another possibility is that it points to another client by embedding its identifying information within the document, and then publishes the content without even sending it to the receiving client. The refusal of the allegation will be a unique case that will develop. The criminal customer can claim that he is innocent and that the sending party is to blame. Our system requires that our protocol satisfy the following qualities, and we can only accept failures with minuscule probabilities.

1) Accuracy: The guilty entity is frequently recognised when both the sender and the receiver accurately obey the protocol specification and divulge just their version of the document.

2) No framing: For its own leaking, the sender cannot frame the receiving entities.

3) No refusal: If the receiving entity publishes any document, he is likely to be engaged in the leaking.

4) Collusion resistance: We want our model to be collusion resistant, which means it should be able to withstand a limited number of conspiring attackers. The information owner Oid is regarded as a trustworthy party by the model. It argues that because the data owner is the person who is concerned about knowledge confidentiality, Oid will not be able to disclose the information. Because significant research on cloud data security has been completed [2], [12], [13], [14], [25], [7], [18], [19], [2], we account the entity CSid as trusted in our model. Our model assumes that CSid follows all safety protocols, securing the critical data and preventing it from being leaked. We need to secure the knowledge from this entity because the user is an untrustworthy party. Our model's critical phase is the transfer of papers to clients via untrustworthy companies. We also assume that three-party cloud systems have trustworthy communication links. The data owner must establish the access hierarchy, indicating which files are frequently accessed by which user. Only if the user id and password are correct is data sent to the user. If the user harmful record is satisfied, the prior record of the user in the database is checked. If the user has authorization to access the file that has been requested. Users should have access to only the data that they are permitted to access without having access to unlawful data. Users should not be able to access cloud data when their rights are withdrawn, according to our system.

3.1 Architectural Model

Table IV summarises the notations used throughout the paper. The information gathered is divided into logically distinct categories. This distinction is based on the sensitivity of data. We use = 4 on a conventional sensitive measure scale, which stands for Public (P), Confidential (C), Secret (S), and Top Secret (TS) (T S). These documents are then shared with the cloud distributor, and a cloud server ID (CSid) is provided to them. The diagram to establish the architecture flow step by step is shown in Figure 3. Client Clid makes the query req request to retrieve data from a cloud distributed environment. Processing data from the owner to the customer involves a layered strategy based on the document's sensitivity category, such as Public, Confidential, Secret, and Top Secret. Using a certain category (P; C; S; T S) to access data uses a scientific technique that is tailored to the data's sensitivity. As we progress from category P to T S, the sensitivity of knowledge grows, necessitating greater security to secure the information than the mechanism at the previous layer. Each layer delivers as we progress from layer zero to layer three.By enhancing the safety system, the preceding layer of security has been enhanced. The suggested framework decreases the overhead and, as a result, the computational cost of

operating on the complete data set. Cloud provides a consistent log-in registration for the general public Data (P), with credentials provided by cloud. Cryptography is used to convert data from plain text to cypher text for Confidential Data (C). Cryptography and watermarking procedures are used to safeguard Secret Data (S), resulting in Watermarked Crypto-Document (WCD).

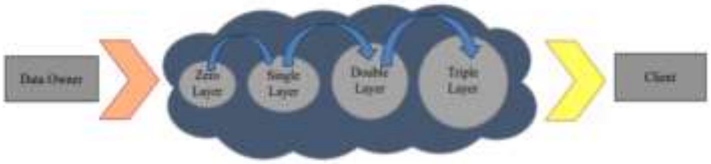

Fig -1: Layered Approach Process

3.2 Layered Methodology

During this division, we analyse a thorough scenario in order to determine how our model constraints interact in a distributed context. We explain how security and privacy are kept at each stage for delivering security in subdivisions.

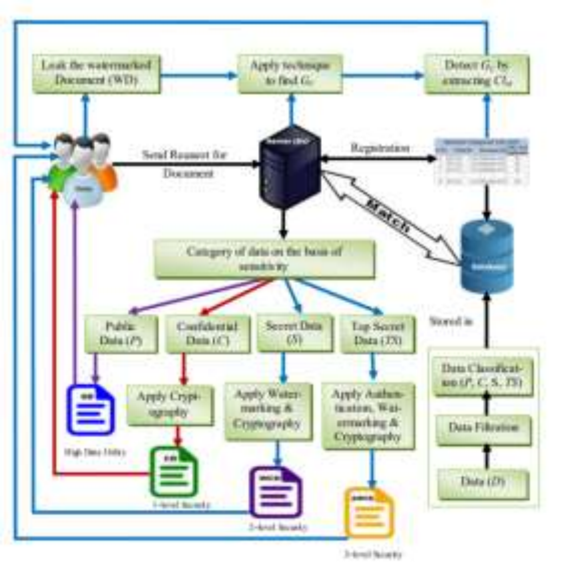
Leak the watermarked Document (WD)
Apply technique to find G_i
Detect G_i by extracting CI_d
Send Request for Document
Registration
Match
Category of data on the basis of sensitivity
Public Data (P)
Confidential Data (C)
Secret Data (S)
Top Secret Data (TS)
Stored in
Apply Cryptography
Apply Watermarking & Cryptography
Apply Authentication, Watermarking & Cryptography
Data Classification (P, C, S, TS)
Data Filtration
Data (D)
1-level Security
2-level Security
3-level Security

Fig -2: Shows The Architecture

Layered Based Security Mechanism Algorithm Any client can request data as input.

Output: An authenticated document has been generated and will be sent to the client.

1:begin

1:I = 1; 2; : : : ; n 3: cat (D) Di 2 8 I = 1; 2; : : : ; n 5: where I 2 f1; 2; : : ; ng & k 2 f1; 2; : : ;mg

2: **switch** (si) **do**

3: **Case 1**: P

4.SD is P.

5.**Case 2**: C

6: AES-256 CD ('KS,C')

KE RSA('KP ','KS') KE RSA('KP ','KS') KE RSA('KP ',

7: **Case 3**: S

8: AES-128('KS'; 'Clid') E(Clid)

9: W D DWT('S'; 'E(Clid)') W D DWT('S'; 'E(Clid)') W D DWT('S'

10: Digital Watermarking Technique (DWT)

11: AES-256 WCD ('KS'; 'WD')

KE RSA('KP ','KS') KE RSA('KP ','KS') KE RSA('KP ',

T S is the fourth case.

12: SHA-3 SHA (T S)

13: AES-128('KS'; 'Clid') E(Clid)

DWT('AD'; 'E(Clid)') 21: AWD

14: AES-256('KS'; 'AWD') AWCD

KE RSA('KP ','KS') KE RSA('KP ','KS') KE RSA('KP ',

k 2 f1; 2; : : : ;mg 24: Ck Transfer(Di) for k 2 f1; 2; : : ;mg 25:

15.**end**

To urge cypher text C = E(M) and plain text M = D(C), this must consider two processes: encrypting E(M) = C and decrypting D E(M) = M. To encrypt cryptographic keys and encrypt document Di, it must utilise standard algorithms. The document was encrypted with AES-256 to decrease the document's complexity. Additionally, the AES-256 key key KS is encrypted with RSA for added security. By selecting private and public keys KPV, KP, respectively. The approach generates a cryptographic document CD, which is subsequently sent to the client and decrypted. See Figures 4(a) and 4(b), where Fig. 4(a) shows how sensitive data records are encrypted and Fig. 4(b) shows how three keys are used to decrypt them (secret key KS, private key KPV and encrypted key KE). Double Layer: If Di's information sensitivity falls below 3 on the sensitivity scale, a higher security is required. By adopting the preceding layer as the base layer, we provide a mechanism for data leakage detection and leaker identification liable for leaking the information at this layer.

4. FINAL RESULTS

In this research, we present a layered architecture based on sensitivity that can be used to secure data and information.maintaining its privacy in a cloud-based environment By implementing a layered-based security mechanism, the proposed architecture reduces the overall overhead at the cloud service provider. Because the utility and security requirements for different data can be quite different, our adapt method maintains security and privacy at each layer in a different way while taking data utility into account. At each layer, hashing, encryption, and watermarking schemes are combined in novel and creative ways to achieve a far better balance of data security and utility. The approach provides a mechanism to spot malicious entities in the case of knowledge leakage for the most sensitive data, such as secret and top secret data. The document's embedded ID is extracted, and the ID is then tracked in the Information Management Table (IMT). If the IDs match, the leaker has been identified, and the owner's authorization has been revoked. In addition, just like with top-secret data, the leaker is verified using SHA authentication. The extracted ID's hash value is compared to the embedded hash value. If both are the same, the guilty client has been identified. The experimental results demonstrate that the proposed approach is correct, practical, reliable, and efficient. Our research is frequently extended by taking into account the case of world leakage scenarios and the case where security protocols aren't followed by any entity.

5. ACKNOWLEDGEMENT

First and foremost, I thank God, without whose blessings, I would not have been able to finish my paper work. Mr. SUNIL S.S., the Head of the Department of Computer Science, deserves special thanks for his constant guidance and assistance. My heartfelt gratitude to our Project Coordinator, Mr. RAHUL, M.TECH., faculty of computer science, for his assistance with this project. We gratefully acknowledge his contributions, constant support, and encouragement in the preparation of this paper. And the computer science faculty for their assistance in shaping my paper into what it is now. I appreciate my parents' mental support during the project, especially when my energy levels were at their lowest.

6. REFERENCES

[1] A. Shabtai, Y. Elovici, and L. Rokach, Springer-Verlag NY, 2012, DOI: 10.1007/978-1-4614-2053-8, “A Survey of Knowledge Leakage Detection and Prevention Solutions.”

[2] X. Dong, J. Yu, Y. Luo, Y. Chen, G. Xue, and M. Li, “Achieving an effective, scalable, and privacy-preserving data sharing service in cloud computing,” Future Generation Computer Systems, vol. 42, no. 1, pp. 151-164, 2014, DOI: 10.1016/j.cose.2013.12.002.

[3] S. Alneyadi, E. Sithirasenan, and V. Muthukkumarasamy, “A survey on data leakage prevention systems,” Journal Network Comput. Applicat., vol. 62, no. 1, pp. 137-152, January 2016, DOI: 10.1016/j.jnca.2016.01.008.

[4] B. Hauer, “Data and Knowledge Leakage Prevention Within the Scope of Information Security,” IEEE Access: The Journal for Rapid Open Access Publishing, vol. 3, no. 3, December 2015, pp. 2554-2565, DOI: 10.1109/ACCESS.20152506185.

[5] A. M. Nia, S. Sur-kolay, A. Raghunathan, and N. K. Jha, “Physiological Information Leakage: a New Frontier in Health Information Security,” IEEE Trans. Emerg. Topics Comput., vol. 4, no. 3, pp. 321-334, September 2016, DOI: 10.1109/TETC.2015.24

[6] M. Backes, N. Grimm, and A. Kate, IEEE Trans. Dependable Secure Comput., vol. 13, no. 2, pp. 178-191, Mar./Apr. 2016, DOI: 10.1109/TDSC.2015.2399296.

[7] B. C. Fung, K. Wang, and P. S. S., "Anonymizing Classification Data for Privacy Preservation," IEEE Trans. Knowl. Data ENG., vol. 19, no. 5, May 2007, pp. 711-725, DOI: 10.1109/TKDE.2007.1015.

[8] Statista, "Number of consumer cloud-based service users worldwide (in billions) between 2013 and 2018," [Online] Global consumer cloud computing users can be found at https://www.statista.com/statistics/321215/global-consumer-cloud-computing-users/.

[9] T. M. Payton and T. Claypoole, "Privacy in the Age of Massive Data," Rowman and Littlefield, United States of America, 2015.

[10] "2014 Data Breaches – A Billion Exposed Records – a Replacement All-Time High," Risk Based Security (RBS). [Online] https://www.riskbasedsecurity.com/2015/02/2014-data-breach-a-billion-exposed-records-a-new-all-time-high/

[11] A. Harel, A. Shabtai, L. Rokach, and Y. Elovici, "M-Score: A Misuseability Weight Measure," IEEE Trans. Dependable Secure Comput., vol. 9, no. 3 (May/June 2012), pp. 414-428, DOI: 10.1109/TDSC.2012.17.

[12] J.-J. Yang, J.-Q. Li, and Y. Niu, "A hybrid solution for privacy-preserving medical data sharing in the cloud," Future Generation Computer Systems, vol. 43-44, pp. 74-86, 2015, DOI: 10.1016/j.future.2014.06.004.

[13] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing Secure Cloud Storage," IEEE Trans. Comput., vol. 62, no. 2, Feb. 2013, DOI: 10.1109/TC.2011.245.

[14] X. Zhang, C. Liu, S. Nepal, S. Pandey, and J. Chen, "A Privacy Leakage Boundary Constraint-Based Approach for Cost-Effective Privacy Preserving of Intermediate Data Sets in Cloud," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1192-1202, June 2013, DOI: 10.1109/TPDS.2012.238.

[15] Ernst & Young, "Data loss prevention – Keeping your sensitive data out of the general public domain," [Online] Insights on governance, risk, and compliance, Oct. 2011. EY Data Loss Prevention/$FILE/EY Data Loss Prevention.pdf is available at https://www.ey.com/Publication/vwLUAssets/ EY Data Loss Prevention/$FILE/EY Data Loss Prevention.pdf.

[16] M. Hilbert, "What is the content of the world's technologically mediated information and communication capacity: how much text, image, audio, and video?" DOI: 10.1080/01972243.2013.873748, The Inform. Soc., vol. 30, no. 2, pp. 127-143, 2014.

[17] L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, "Information Security in Big Data: Privacy and Data Processing," IEEE Access: The Journal for Rapid Open Access Publishing, vol. 2, no. 2, pp. 11491176 ,October 2014, DOI: 10.1109/ACCESS.2014.2362522.

[18] J. Hua, A. Tang, Y. Fang, Z. Shen, and S. Zhong, "Privacy-Preserving Utility ".

[19] A. Pretschner, M. Hilty, F. Schutz, C. Schaefer, and T. Walter, "Usage control enforcement: Past, Present, and Future," IEEE Security Privacy, vol. 6, no. 4, pp. 44-53, July/August 2008, DOI: 10.1109/MSP.2008.101.

[20] F. Kelbert and A. Pretschner, "Data usage control enforcement in distributed systems," ACM Conf. Data Appl. Security Privacy, pp. 71-82, 2013, DOI: 10.1145/2435349.2435358.

[21] M. Nabeel and E. Bertino, "Privacy Preserving Delegated Access Control Public Clouds," IEEE Trans. Knowl. Data ENG., vol. 26, no. 9, pp. 2268-2280, September 2014, DOI: 10.1109/TKDE.2013.68

[22] M. Sookhak, F. R. Yu, M. K. Khan, Y. Xiang, and R. Buyya, “Attributebased data access control in mobile cloud computing: Taxonomy and open issues,” Future Generation Computer Systems, vol. 72, no. 2, pp. 273-287, 2017, DOI: 10.1016/j.future.2016.08.018.

[23] V. Velichkov, V. Rijmen, and B. Preneel, “Algebraic cryptanalysis of a small-scale version of stream cypher Lex,” IET Inform. security, vol. 4, no. 2, pp. 49-61, DOI: 10.1049/iet-ifs.2009.0118.

[24] Y.-W. Kao, K.-Y. Huang, H.-Z. Gu, and S.-M. Yuan, “uCloud: a user-centric key management scheme for cloud data protection,” IET Inform. Security, vol. 7, no. 2, pp. 144-154, 2013, DOI: 10.1049/ietifs.2012.0198.