IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURE CLOUD DATA SHARINGWITH OPTIMIZED STORAGE& PRIVACY PRESERVATION

[1] Pradeep M, [2] Mala K , [3] Hemanth Kumar S, [4] Haridhar K B
Assistant Professor, Department of ISE, CIT, Gubbi, Tumakuru
Assistant Professor, Department of ISE, CIT, Gubbi, Tumakuru
Student, Department of ISE, CIT, Gubbi, Tumakuru
Student, Department of ISE, CIT, Gubbi, Tumakuru

Abstract: This paper introduces a privacy control model to optimize cloud storage. The main goal is to provide data security, confidentiality, integrity and availability to cloud service providers at a low cost, while ensuring that users trust them. To achieve this goal, a clear security strategy to protect data during storage and transmission in the cloud is aimed. This framework aims to keep costs low while maintaining data security and accuracy. The solution compresses high-resolution images and reduces storage size by 60%. The device is divided into blocks, and the blocks are encrypted using the owner's private key, providing two layers of security. Only users authorized to access the file can decode it and restore it to its original format. Create a signature to verify the authenticity of the information. If an unauthorized user tries to update the data, the audit process can identify the relevant data. Using asymmetric keys, when users send data to the cloud, a digital signature will be created using the user's private key. Using the design, you can not only reduce the costs associated with data storage, thanks to the effective data compression process, but also effectively demonstrate the importance of protecting personal information during the data access process. The result of the experiment is that the proposed method has better performance than the existing method in all aspects. Optimized storage and privacy management standards can be used to ensure secure storage and sharing of data in a shared cloud environment.

Keywords: Privacy control model, Cloud storage optimization, Security strategy, Digital signature

I. INTRODUCTION

The emergence of cloud computing has changed the way businesses store and exchange information. With the development of this technology, the information sharing process has undergone a major change and has become easier, faster and more efficient than the previous process. But the convenience of cloud computing comes at a price, as it also brings with it significant concerns about data privacy and security. As data moves to the cloud, organizations will have to face the challenge of managing data while granting access to data. One of the biggest challenges facing organizations today is how to provide secure information to other organizations, third-party vendors or customers while managing data. The traditional access control model of role-based control (RBAC) or behavior-based control (ABAC) has limitations when it comes to sharing data in the cloud. RBAC and ABAC models can be immutable and difficult to manage, which can lead to inaccuracies and vulnerabilities that can compromise the confidentiality of your information. To solve these challenges best prospects and governance model for data sharing were proposed. The proposed model provides a simple and scalable access control method that ensures that information is accessed only by authorized individuals while maintaining confidentiality. We intend to reduce many problems and disadvantages in cloud computing as follows: Allowing access to the cloud environment is a serious event, it poses a threat to both people. and organizations. This occurs when someone accesses cloud-based data without authorization or permission and can be caused by many things, including weak passwords, exposure to network attacks, cloud unpatched vulnerabilities in the infrastructure, and certificate impacts. The impact of unauthorized access to cloud data can be serious. For individuals, this can lead to identity theft, financial loss, and loss of privacy. For organizations, the impact will be greater, with the potential for data breaches, loss of assets, and damage to reputation and those responsible.

It is important to implement good security procedures to reduce the possibility of being affected by unauthorized data exposed in the cloud environment. These measures include the use of two-factor authentication, stringent security controls, encryption technology and routine security measures. Employees also need to learn how to detect and prevent social attacks, and building climates need to be monitored for signs of illegal or unusual business infiltration. Issues with cloud technology for data storage and access include reliance on third-party providers, raising concerns about limited data visibility and control for security risks. Responsibility for cloud security is shared between cloud service providers and customers, with the provider responsible for cloud security and the responsibility to ensure the security of the customer's information. However, using third-party data sharing services can expose data to the external IT environment and therefore sharing data in an unsecured manner can be risky. To reduce these risks, it is recommended that data be encrypted during storage and transmission. In addition, since the data of many customers are stored on the same server, the possibility of data transfer through access by third parties should also be taken into account. Therefore, it is important to invest in good cloud security, which includes encryption of sensitive data and protection of unique credentials. environment. To ensure security, two conditions must be met: To ensure the security of data security, a key distribution module responsible for the generation and distribution of security keys. Both the file owner and the user file must keep these keys secure to prevent unauthorized access. By following this principle, organizations can enjoy the advantages of cloud storage and sharing services such as flexibility, scalability and cost savings while protecting the confidentiality and integrity of their data.

II. LITERATURESURVEY

In a recent study, Kharya et al. According to CNN, it is claimed that there are many challenges in cloud computing, such as data security, data backup, data storage technology and usability. One of the limitations of cloud storage is that users can get the minimum amount of storage space determined by the cloud service provider.

Cloud service providers need to monitor data storage when backing up data. And there is also the secret of working harder on data entry and deletion. Figure 3.1 shows the system architecture consisting of a data manager, two storage providers, and many end users (the data manager's customers). However, since the system is not trusted, there is a risk of man-in-the-middle attack.

In this case, the reliability of the storage provider is called into question due to concerns about the storage provider's integrity, curiosity, or vulnerability to external opposition. But there is trust in communication between users. The data owner uses a symmetric encryption method to convert the original data into a set of k fragments to ensure the identity of sensitive data. These partitions are distributed across at least two different cloud providers, thus increasing data redundancy. The key encryption keys for decrypting the data are shared among N authorized users, ensuring access control and protecting the confidentiality of the data. Even if only part of the record is available, the part can be decrypted using the real key. Many end users can save externally stored data by downloading the data from two cloud storage providers and decrypting the pieces using the appropriate keys. The key encryption keys for decrypting the data are shared among N authorized users, ensuring access control and protecting the confidentiality of the data. Even if only part of the collection is accessible, the part can be decrypted using the real key. Many end users can save externally stored data by downloading the data from two cloud storage providers and decrypting the pieces using the appropriate keys.

The responsibility for ensuring data integrity lies with the Cloud Service Provider (CSP). CSP has two main components: Trusted Key Generation Center (TKGC) and data manager. TKGC creates the global constraints and keys of the system, data manager works on outsourcing and updates the data. Data users interact with CSPs by submitting audit questions and verifying the evidence provided. Keys are sent securely by a trusted source. In summary, SecACS provides an overview of this process. To create a secure solution, a secret key must be generated and shared securely between the data owner and users through secure communication. The data owner then sends the data block and its identifier to the cloud. Users can use the tag and private information to create certificates to check the authenticity of the information. This certificate is then verified by users to ensure the accuracy of the information.

Secure data sharing and cloud-based collaborative storage According to the author's theory, the Cloud Collaborative Storage (CECS) framework provides solutions that can manage data generated by the Internet of Things (IoT). This new system can use edge servers to process IoT data in real time and then store the processed data on cloud servers. Internet of Things data processing is related to data leakage. Current security CECS plans rely heavily on the reliability of all end servers. To solve this problem, the authors propose an alternative method that improves existing CECS security in two important ways. The plan will allow users to create and manage their own public and private keys. Second, the proposed method incorporates a public key cryptocurrency search, thus improving the security, efficiency, and flexibility of the data search process. With this new approach the authors focus on ensuring the security of data in the cloud, making data sharing and searching easier, and eliminating any point of failure in the system.

III. PROPOSED SYSTEM

We create data integration to ensure low data storage costs; There are three processes of the proposed model as shown in Figures 3.1, 3.2 and 3.3, which will ensure data management, data confidentiality and evidence of data to be stored. If you allow price optimization technology. We recognize that storing large amounts of data in the cloud can be expensive, so we offer a solution that will improve data storage while controlling data security and privacy.

3.1 Storage Cost Optimization

The solution involves compressing the object to reduce its size, splitting the object into multiple pieces, and encrypting the object using the owner's private key. It is recommended to compress the image and then store it in the cloud. Our tests show that compressing high-resolution images can reduce file size by up to 60%. This module reduces the image size by half, takes the image as input and compresses it using the DCT (Discrete Cosine Transform) algorithm. DCT is preferred because it is easy to calculate and has piecewise properties that can generate various DCTs for lines and lines. Improve your results.

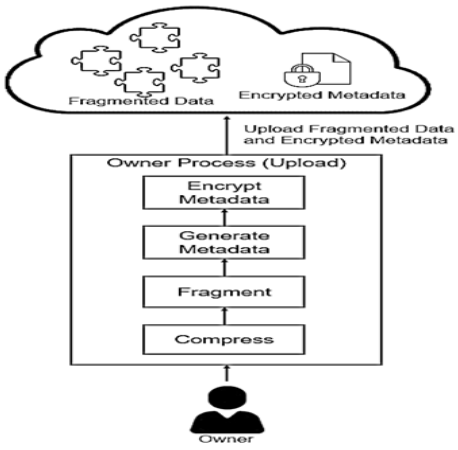

Fig. 3.1 OwnerProcess

3.2 Privacy-Preserving Access Control

Another important aspect of our design is privacy-controlled access. Control systems ensure that only authorized users can access and modify data, preventing unauthorized access and modifications. In our proposed model, we use access control methods for users to determine who can access information. We also recommend splitting compressed files into multiple parts to utilize space. The pieces are then encrypted using the owner's private key, providing two layers of security. This ensures that only users authorized to access the file can identify and restore the file to its original format. Once the owner approves the user's download request, the user can continue downloading the image. However, explosives must have a special system in order to improve image data. To access these messages, the encrypted log file is first decrypted using the decryption process and passed to the file defragmentation module. It needs to be decrypted to convert it into a readable format. The decrypted blocks and decrypted log files are then fed to the file defragmentation module to restore the file to its original form. Here, the public key of the file owner who originally uploaded the file is used to decrypt the fragment.

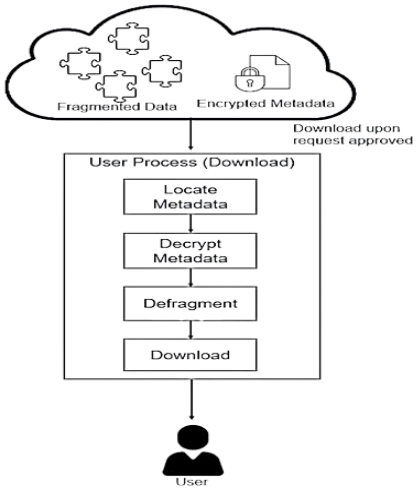

Fig. 3.2UserProcess

3.3 Data Correctness and Verification

Our approach enables auditors to perform data audits more effectively because it supports automation and accuracy of data in cloud-based systems. At runtime, reviewer has read-only permissions and supports bulk review. Create a unique signature. This reduces storage costs when storing new data. According to the diagram. 3.3 TPA uses characteristics of each user to create its own signature.

The system does not keep copies of files, does not leak private keys during the decryption process, and ensures that files remain accurate. TPA always creates its own signature that is updated when users save or

modify files to ensure that data remains current. This system operates in batch mode and supports user cloud responsiveness without interrupting the data store.

Access control mechanism is when a user decides to upload a file to the cloud, the user's private key will be used to create a digital signature. If third-party verifiers need to verify the integrity of user data, they can use the public key to create a digital signature. This method ensures the protection of the user's personal information while completing the review process and verification to ensure the integrity of the information.

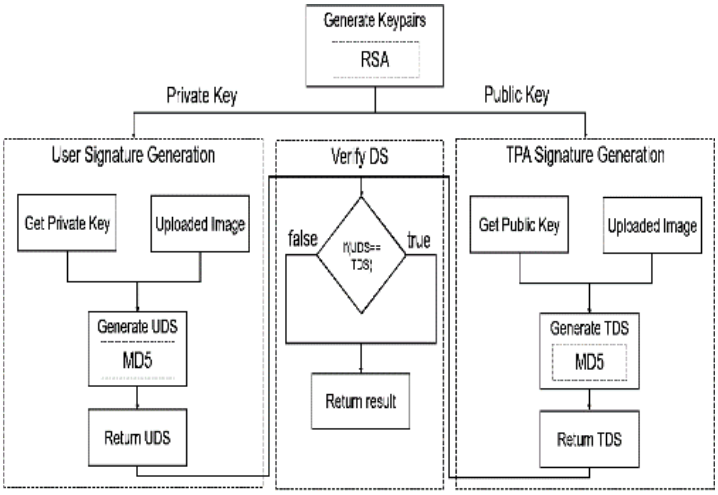

Fig. 3.3 Data Correctness and Verification Model

IV. CNN Train and Test Model:

You can use a database like ImageNet (a subset of the Kaggle dataset) to perform image compression. The existence of labeled datasets is not necessary as there is no detection of relevant objects. The main goal is to reduce the physical size of the image by more than 50% while maintaining visual quality. It is a Fourier-related transform that provides good image compression. In our implementation, we use a modified version of the DCT algorithm that gives the best results. This change is necessary to preserve the quality of compressed images because compressing images uses one of the best methods to ensure that image quality is not lost. Convert image to cosine function of multiple frequencies for multiple frequency and direction sub bands Compression efficiency High compression ratio, More suitable for image content with sharp edges and high compression ratio, Better to get smooth and consistent images Image better preservation of detail, better compression Images with high levels of compression may more often show artifacts being suppressed in calculating competition higher level of decomposition, especially at a given time usually faster and cost less money and resources.

Criteria	DWT	DCT
Transformtype	Decomposes animage into sub-bands ofdifferentfrequencies andorientations	Converts an imageinto a sum ofcosinefunctionsof differentfrequencies
Compressionefficiency	High compressionratios, better forimageswithsharp edges anddetails	High compressionratios, better forsmooth anduniformimages
Imagequality	Preserves imagedetails better,higher qualitycompressedimage	May introduceblock artifacts athigh compressionlevels
Computationalcomplexity	Morecomputationallycomplex,especially athigher levels ofdecomposition	Generally faster,requires lesscomputationalresources

Table 1.1 Comparative Analysis of DCT and DWT

In general, DWT and DCT technologies have different advantages and disadvantages. The choice of the two methods depends on the specific requirements of the application and the characteristics of the compressed image. Compressed size in megabytes (MB) and kilobytes (KB), respectively. The size of "Image 1" is 1 MB and has been compressed and reduced to 250 KB. Observe the image, it is clear that the larger image exhibits a lower contrast ratio, causing the size to shrink compared to the original size.

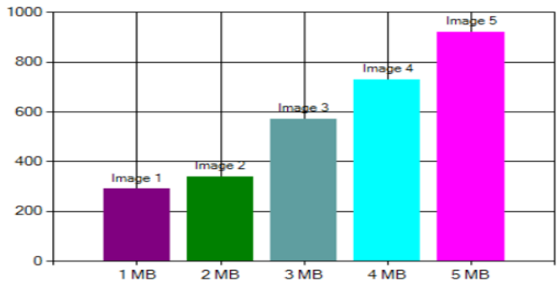

Fig. 4.1 Storage size difference between original image and compressed image

Figure 4.2 shows the different images and their corresponding PSNR values used to measure the quality of the image in terms of its fidelity to the original. In the first row, the image labeled "Camera Man" has a DCT of 37.04 PSNR, while in the second row, the same image has a slightly higher DWT of 37.37 PSNR. When we move to the second line, the PSNR value for DCT of the image labeled "Rice" is 39.04, while in the next line the PSNR value of the same DWT image drops to 37.7.

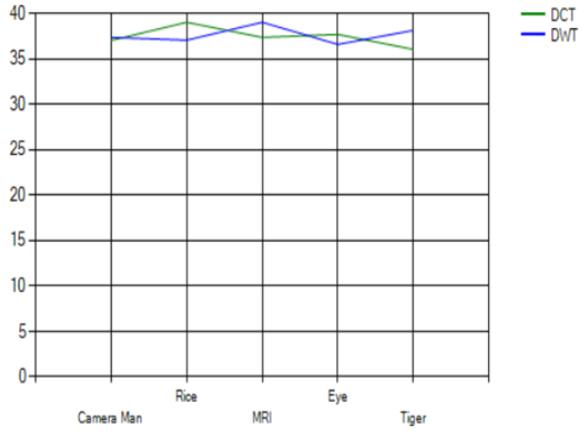

Fig 4.2 Images compressed by DCT and DWT and their respective PSNR Values

Figure 4.3 shows the comparison between the analytical model and the SecACS model. The above description clearly shows that the proposed scheme reduces the computation time compared to SecACS. It is also worth noting that as the number of audit questions increases, the calculation time of the direct audit process also increases.

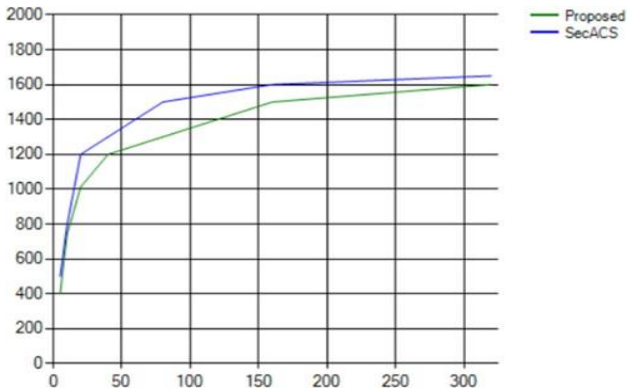

Fig. 4.3 Analysis of proposed auditing scheme and SecACS

V. CONCLUSION

The data protection policy outlined facilitates data sharing between involved parties while empowering the data subject with the prerogative to retract access at their discretion. Our approach champions security through a multifaceted strategy, leveraging both data fragmentation and encryption techniques. This entails dividing a file into smaller segments, encrypting each segment individually, and subsequently storing them in the cloud. Importantly, without authorized access, each segment must undergo decryption for the restoration of the original file. Such a multi-policy management system underscores our commitment to providing a robust solution for safeguarding sensitive data shared within cloud environments. In essence, our proposed framework stands as a beacon of promise in the realm of data security and privacy. Its effectiveness is evident in its ability to address the complex challenges associated with data protection in storage environments. By integrating multiple layers of security, including fragmentation and encryption, our framework ensures a formidable defence against potential breaches or unauthorized access. Moreover, its adaptability renders it suitable for implementation across diverse storage infrastructures, irrespective of scale or complexity.

The significance of our approach extends beyond mere data protection; it embodies a proactive stance towards preserving individual privacy rights in an increasingly digitized world. By granting data subjects the agency to control access to their information, we foster a culture of transparency and accountability in data management practices. This not only bolsters trust between stakeholders but also aligns with regulatory frameworks aimed at upholding data sovereignty and confidentiality. In conclusion, our proposed framework represents a pivotal advancement in the ongoing quest for data security and privacy. By combining innovative technologies with robust policy frameworks, we empower organizations to navigate the evolving landscape of data governance with confidence. As data continues to play an ever-expanding role in modern society, our commitment to fortifying its protection remains unwavering, ensuring a safer and more resilient digital future for all.

REFERENCES

[1] Katarzyna KAPUSTA, Han QIU, and Gerard MEMMI LTCI, Telecom ParisTech, Paris, France “Secure Data Sharing with Fast Access Revocation through Untrusted Clouds” 978-1-7281-1542-9/19/$31.00 ©2019 IEEE.

[2] Li Li, JiayongLiub “SecACS: Enabling lightweight secure auditable cloud storage with data dynamics” 2214-2126/© 2020 Elsevier Ltd. All rights reserved.

[3] Reyhaneh Rabaninejad, Seyyed Mahdi Sedaghat, Mohamoud Ahmadian Attari, Mohammad Reza Aref “An ID-Based Privacy-Preserving Integrity Verification of Shared Data Over Untrusted Cloud” K. N. Toosi University of Technology Department of Electrical Engineering Tehran, Iran, 978-1-7281-5937-9/20/$31.00 ©2020 IEEE.

[4] Premlata Singh, Sushil Kr. Saroj “A Secure Data Dynamics and Public Auditing Scheme for Cloud Storage” Department of Computer Science & Engineering, Madan Mohan Malaviya University of Technology Gorakhpur, India 978-1-7281-5197- 7/20/$31.00 ©2020 IEEE

[5] Jian Wang, Kehua Wu, Chunxiao Ye, Xiaofeng Xia, Fei Ouyang ∗ Colleage of Computer Science, Chongqing University, Chongqing, China “Improving Security Data Access Control for Multi-Authority Cloud Storage” 978-1-7281-4328-6/19/$31.00 ©2019 IEEE

[6] Aritra Dutta, Rajesh Bose, Swamendu Kuma Chakraborty, Sandip Roy, Haraprasad Mondal, Computational science Brainware University, Kolkata India "Data Security Mechanism for Green Cloud", IEEE 2021

[7] Ding ManJiang 1, Cao Kai 1, Wang ZengXi 2, Zhu LiPeng 3, 1. State Grid Jiangsu Tendering Co., Ltd, Nanjing, China 2. Jiangsu Electric Power Information Technology Co., Ltd, Nanjing, China 3. Global Energy Interconnection Research Institute Co., Ltd, Beijing, China, "Design of a Cloud Storage Security ncryption Algorithm for Power Bidding System", IEEE 2020

[8] YANG Zhen, WANG Wenyu, HUANG Yongfeng, and LI Xing, Department of Electronic Engineering, Tsinghua University, Beijing 100084, China “PrivacyPreserving Public Auditing Scheme for Data Confidentiality and Accountability in Cloud Storage” 2019 Chinese Institute of Electronics. DOI:10.1049/cje.2018.02.017 ©2019 IEEE

[9] Fei Chen, Fengming Meng, Tao Xiang, Hua Dai, Jianqiang Li, Jing Qin "Towards Usable Cloud Storage Auditing" 1045-9219 (c) 2020 IEEE

[10] C.Jenifer Kamalin1, Dr.T.Arul Raj2, Dr.G.MuthuLakshmi3 1Research Scholar, 2, 3Assistant Professor 1,3Department of Computer Science & Engineering, ManonmaniamSundaranar University, Abishekapatti, Tirunelveli – 627 012 2Department of Computer Science, Sri Paramakalyani College, Alwarkurichi, Tenkasi – 627 412, "Comparative Analysis for Dct, Dwt Image Compression Performed with Huffman, Run Length and Lzw Encoding", NTERNATIONAL JOURNAL OF SPECIAL EDUCATION Vol.37, No.3, 2022

[11] SI HAN, KE HAN, AND SHOUYI ZHANG Department of Science and Technology, China University of Political Science and Law, 102249 China "A Data Sharing Protocol to Minimize Security and Privacy Risks of Cloud Storage in Big Data Era" 2169- 3536 2019 IEEE.

[12] Leyou Zhang, YileiCui , and Yi Mu , Senior Member, IEEE "Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing" 1937-9234 © 2019 IEEE

[13] T. A. Mohanaprakash, Dr.J.Andrews Department of CSE, Sathyabama Institute of Science and Technology, Chennai 600119, Tamilnadu, India "Novel privacy preserving system for Cloud Data security using Signature Hashing Algorithm" 978-1-7281-1576- 4/19/$31.00 ©2019 IEEE

[14] YE TAO, PENG XU, and HAI JIN, National Engineering Research Center for Big Data Technology and System, Services Computing Technology and System Lab "Secure Data Sharing and Search for Cloud-Edge-Collaborative Storage" 10.1109/ACCESS.2019.2962600, IEEE Access

[15] Zhuoran Ma, Jianfeng Ma, Yinbin Miao, Ximeng Liu, Tengfei Yang, School of Cyber Engineering, Xidian University, Xi'an 710071, China "Privacy-Preserving Data Sharing Framework for High-Accurate Outsourced Computation" 978-1-5386-8088- 9/19/$31.00 ©2019 IEEE

[16] Wenxiu Ding, Member, IEEE, Rui Hu, Zheng Yan, Senior Member, IEEE, Xinren Qian, Robert H. Deng, Fellow, IEEE, Laurence T. Yang, Senior Member, IEEE, and Mianxiong Dong, Member, IEEE "An Extended Framework of Privacy-Preserving Computation with Flexible Access Control" 1932-4537 (c) 2019 IEEE

[17] HAN YU, XIUQING LU, AND ZHENKUAN PAN, College of Computer Science and Technology, Qingdao University, Qingdao 266071, China, "An Authorized Public Auditing Scheme for Dynamic Big Data Storage in Cloud Computing" r 10.1109/ACCESS. 2020 IEEE

[18] Nikolaos Doukas, Oleksandr P. Markovskyi, Nikolaos G. Bardis Department of Mathematics and Engineering Science, Hellenic Military Academy, Vari – 16673, Greece "Hash function design for cloud storage data auditing" 0304-3975/© 2019 Elsevier

[19] NureniAyofe Azeez, Charles Van der Vyver School of Computer Science and Information Systems, Faculty of Natural and Agricultural Sciences, Vaal Triangle Campus, North-West University, South Africa. "Security and privacy issues in e-health cloud-based system: A comprehensive content analysis" 1110- 8665/2018 Production and hosting by Elsevier