International Journal of Research in Advanced Engineering and Technology
ISSN: 2455-0876; Impact Factor: RJIF 5.44
Received: 02-04-2019; Accepted: 04-05-2019
www.newengineeringjournal.in
Volume 5; Issue 3; 2019; Page No. 05-09

Data: Centric integrity control system for cloud based structured databases

Okozor Nkeiruka Petrolina[1], **Okezie Christian Chikodili**[2], **Inyiama Hycinth Chibueze**[3]
[1] High Mega-System Limited Enugu, Nnamdi Azikiwe University Akwa, Nigeria
[2, 3] Department of Electronic & Computer, Nnamdi Azikiwe University Akwa, Nigeria

Abstract
Data –centric integrity control system for cloud based structured databases has been developed in this paper. The issue of data integrity in the cloud based database is important, in the sense that compromised data is of no use to any organization. Literature review has shown that there are gaps in the data integrity measures being used at the moment hence there is need to augment them with further innovation. The integrity measure being recommended is based on the use of supervisory software to ensure that only valid data is stored. The valid data is digitally signed at the record level and encrypted using symmetric-key encryption before it is sent to the cloud for storage. Similarly data retrieved from the cloud is first decrypted after which the digital signature it contains on record by record basis is used to authenticate the integrity of each record. Only the data that passes this integrity check is passed to the user. Data that fails integrity check is first reconstructed before being released to the user. Thus the user never gets anything but the correct originally stored data. This method ensures that data remains accurate through-out its life span. This enhanced model ensures that data owners are in total control of their data without even the cloud provider having a clear text to understand the data in the cloud.

Keywords: data integrity, cloud based, supervisory software, digital signature, encryption and decryption

Introduction

Miao Zhou (2013) [9] worked on data security and integrity in cloud computing, the work addresses the critical security challenges of data security in cloud computing which include key management, access control, searchable encryption techniques, remote integrity check and proof of ownership. The research on the other hand did not address the issue of how to prevent malicious cloud user from abusing cloud resources.

Ricardo J, (2014) [11] worked on Enhancing Data Security in data warehouse. He proposes a security framework for integrating data confidentiality solution and intrusion detection in data warehouse system. The framework was deployed as middle tier between end users interfaces and database server. The model provides an objective and comprehensive means of evaluating the intrusion detection efficiency and ability to improve as well as to impact on database response time of proposed data intrusion detection system (DIDS) and data warehouse (DW). While this benchmark offers a representative scenario of possible attacks on data warehouse, it does not reflect the entire range of possibilities. There is very scanty work in the literature in the area of data integrity in databases. Although some database management systems feature robust data integrity capabilities the work was limited to ensuring that one database table does not over write another inadvertently. It was not targeted at preventing fraudulent manipulation of individual database tables.

Georgia, K (2014) [3] did a work on cyber physical security for power grid protection. He used a novel network intrusion detection system (NIDS) that he called hybrid control network intrusion detection systems (HC-NIDS). The HC-NIDS focused on the implementation of security policies for specific applications, by creating models based on the hybrid automata that designate the expected behavior of cyber physical systems (CPSs). Limitation of this work is that it did not put into consideration general model of cyber and physical aspect of CPSs as well the coordination orchestration of the various components that compose such systems.

Singh H and Rajan (2014) proposed fraud detection by monitoring user behavior and activities. In this paper, the authors proposed a unique and hybrid approach containing data mining techniques, artificial intelligence and statistics in a single platform for fraud detection of on-line financial transaction, which combines evidence from current as well as past behavior. They determined the suspicion level of each incoming transaction based on the extent of its deviation from good pattern by using Bayesian approach and Density Based Spatial Clustering of Applications with Noise (DBSCAN) algorithm. The purpose of this method is to identify the customer behavior at the time of transaction to prevent fraudulent transaction. Limitation of this work is that it is hard to track user's behavior. All types of users (good users, business and fraudsters) change their behavior frequently.

The data security method employed in many universities and organizations did not include strong user authentication but is limited to use of user name and password to identify intended user. The use of asymmetric based authentication method is part of the enhancement that is still needed to be done. In addition there are loopholes in the present system used by many institutions such that it was possible in the past to release fraudulently manipulated degree results. There was no automated arrangement to recover the original version of fraudulently modified records. The gap needs to address.

Foteini Baldimtsi (2014) [2] proposed an efficient cryptography for information privacy using efficient cryptographic tools such as digital signatures, zero-

knowledge proof systems and encryption schemes but this work was focused on protocols that protect user privacy and not on data integrity. This gap still remains to be tackled.
Nabil Giweli (2013) [10] worked on enhanced cloud computing security and privacy. Based on his findings from the review work some research focused on improving the security at the application, operating system, virtual machine (VM) or hardware level. Another aspect of research was on trust computing (TC) concept, this methods allows trusted third party technologies to secure VM from the cloud provider. This type of security does not provide security at the data level, rather security of data are in the hands of cloud provider or trusted third party. This security issue leads to the development of enhanced cloud computing security and privacy. His framework is based on data-centric security (DCS) technique that provides security at data levels. His work uses Chinese Remainder Theorem and utilizes Symmetric and Asymmetric techniques. This method allows the data owners to be in full control of their data security without depending on the cloud providers or trusted third party. The enhanced system in this paper uses data- centric security measures that provides data security at data level without using Chinese remainders theorem. This provides the data owner the opportunity of securing hisr data without being at the mercy of cloud providers or trusted third party.
The works reviewed so far, did not have anything on automated validation of critical data such as are being handled in the organization environment. This paper will fully address this area to ensure that only proper data is kept in the databases.

A Novel approach to data Integrity

Cloud based database is a completely internet-based technology where data are stored and maintained in the data center of a cloud provider. U.S National Institute of Standards and Technology (NIST) defined cloud base as a model for enabling convenient, on-demand network access to shared pool of configurable computing resources (e.g network, servers, storage, applications and services) that can be rapidly provided and released with minimal management effort or service provider interaction (2013). There are a lot of risks that face data stored in the cloud database ranging from how to secure data from modification and alteration to unauthorized access. The issue of data integrity in the cloud based database is important, because compromised data is of no use to any enterprise. This paper deals with data integrity in cloud based systems by providing security at the data level. This enhanced model ensures that data owners do not depend only on the security from the cloud providers but have another level of security that focuses on data integrity. The work is based on the use of Encryption, Digital Signatures and Supervisory Software. To enhance the data integrity any data for cloud storage will be digitally signed at the record level and encrypted using symmetric method of encryption before sending it to the cloud. Symmetric encryption protects data at rest whether on a storage device or in the cloud. Symmetric encryption uses same key for encryption and decryption of data. Once a file is encrypted, it can be stored in the cloud without fear of unauthorized disclosure of the information in the database. This method would not allow the cloud providers to have access to the true meaning of the data since they have no access to the encryption key, thus making the data owners to be in control of their data. It is important to note that once accurate data is received, it is kept accurate for as long as it is in the database through a clever use of digital signatures and supervisory software. Inaccurate record cannot be supplied by the database no matter the modification or alteration attack. The focus of this work is on structured data such as are found in relational databases.

2. Data Capture and Validation

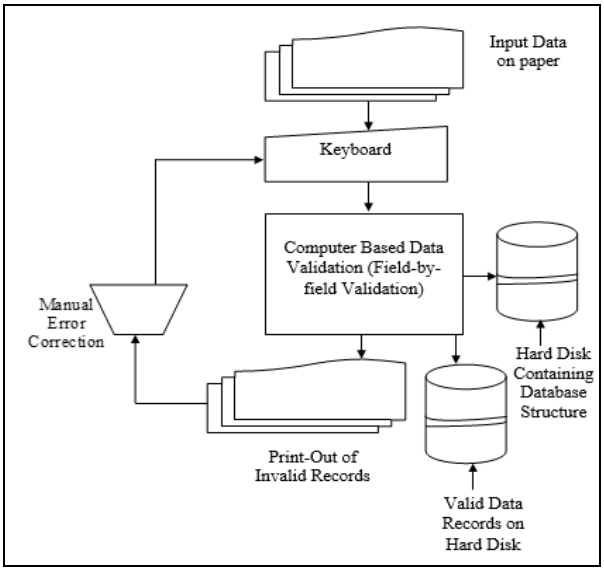

Fig 1a: Key-To Disk -System for Data Entry and Validation

Figure 1a shows a data entry and validation system. Originally data would typically be received as documents on paper, for example, grade report sheets on paper, in the case of university results. Sometimes however, a soft copy of the result is presented for storage. For example a university department may return students results in soft copy to the Dean who may also forward same to the university administration. Figure 1a is for the situation where the grade report sheets (or other structured documents) are presented on paper. If data is presented in soft it must still be validated, digitally signed and encrypted before storage on the cloud. Figure 1b would be a more appropriate system flow chart for structured data presented in soft copy.

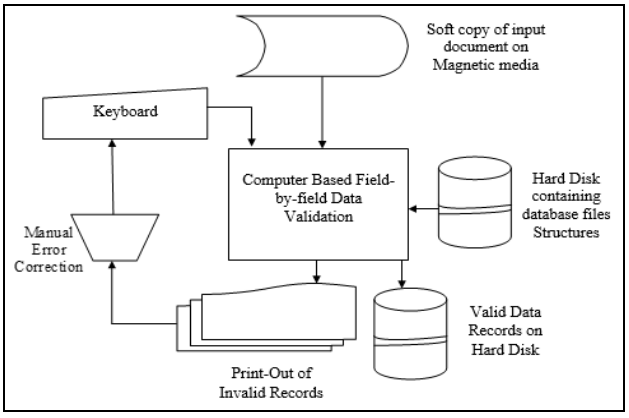

Fig 1b: Data capture and validation for data presented as soft copy

Also where information on payments is recorded by the banks it is usually in soft copy which is later transferred to the organization. Because we are handling structured data each record is comprised of a number of fields and the

database structure of a file is predefined prior to data storage on the file. When softcopy of structured data is captured it is important to validate each record field by field to ensure that they match the definition given by the database structure. Inconsistent data is flagged and corrected before the record is accepted as valid. This is necessary to ensure that wrong data is never received into the valid data pool which therefore has integrity right from the onset. This integrity is what the supervisory software seeks to conserve throughout the life span of the data.

3. Digital Signatures:

After validation the supervisory software appends digital signature to each record on a field by field basis with one digital signature character representing each field. The concatenation of these characters then forms the digital signature of the record. This process will detect any modification in the record or in a field thereof such that if any alteration is made to any field of the record the character representing that field would fail authentication test carried out automatically by the supervisory software. The use of digital signature plays an important role in ensuring that the integrity of data is maintained. A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. It is digital equivalent of a handwritten signature or seal stamp. A digital signature offers far more inherent security, and it is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide the added assurances of evidence of origin, identity and status of an electronic document, transaction or message and can acknowledge informed consent by the signer. For any data to be uploaded to the user's database or cloud database it must be digitally signed. The generated signature is masked off during normal data display as it is meant to be kept secret. It is only made available to the supervisory software at the time of integrity check. Data validation software is used to ensure that data is appropriate at the point of acquisition, while the digital signature is used to ensure that only appropriate data is released. The supervisory software adds digital signature to the data records before encrypting the data for storage in the cloud. Figure 2 shows how digital signature is appended.

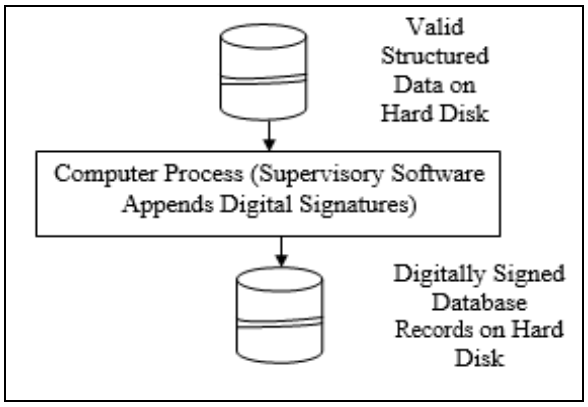

Fig 2: System Flowchart Digital Signature

4. Data encryption and cloud storage

The digitally signed data are encrypted using symmetric encryption method before sending the data to cloud database as depicted in figure 3. This symmetric method is essential for protecting data at rest. It uses the same key for both encryption and decryption. The data owners are always the custodian of the keys thereby making it impossible for the cloud provider to have access to clear text of the data that is stored in the cloud.

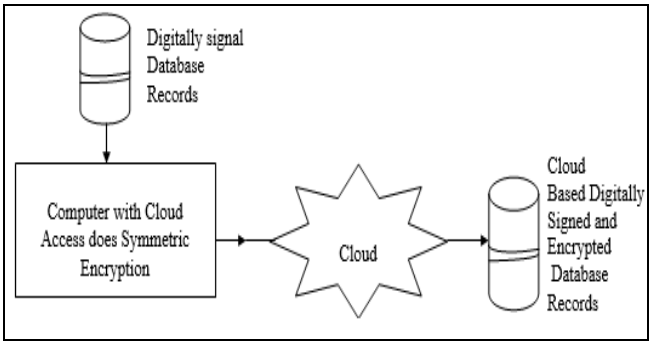

Fig 3: Data encryption and cloud storage

The entire steps taken by the Supervisory Software at Data Capture level is summarized in the flow chart of figure 4a.

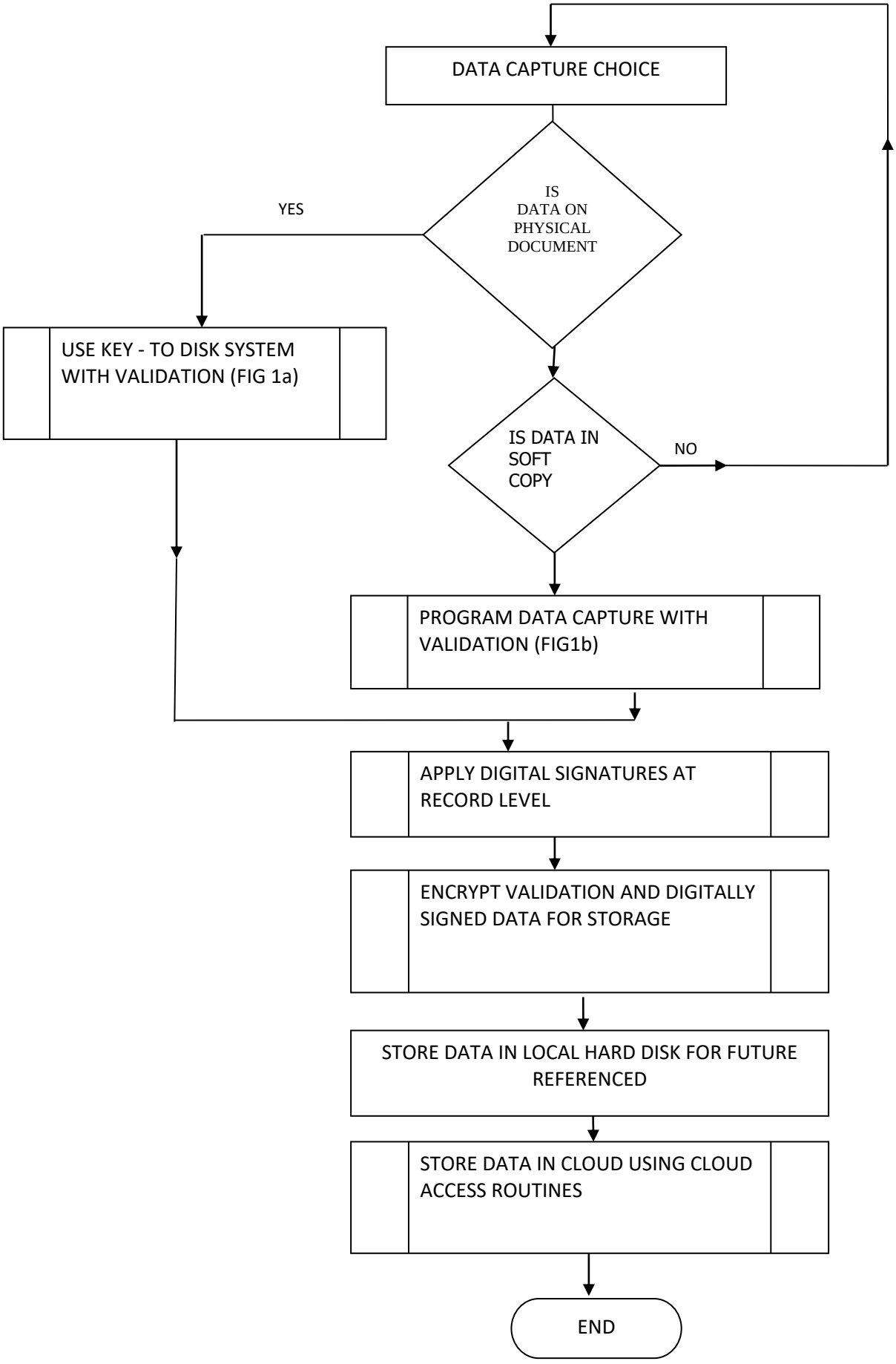

Fig 4b: Supervisory Software at Data Capture Level

5. The supervisory software and data release

The digitally signed and encrypted data in the cloud database are downloaded and decrypted. The supervisory software carries out integrity checks to automatically detect unauthorized access and check for data alteration and if altered recovers the original data and alerts the authority as regards the data records that failed data integrity check. Figure 5 shows the process carried out in this stage of supervisory software and data release.

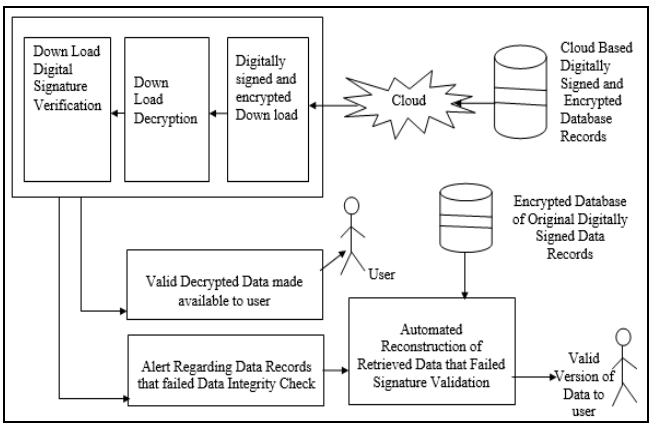

Fig 5: Supervisory Software Steps during Data Release

6. Conclusion

Most of the data driven enterprises depend on data for decision-making. Therefore, data integrity is a top priority for modern enterprises as well as educational institutions. Data integrity can be compromised in a variety of ways; for this reason data integrity practices should be an essential component of effective organization security protocols. The proposed system is generic in nature, in that it can be used by any organization that makes use of structured databases. It ensures that appropriate data are stored in the databases. The system will also help to detect any alteration in the record whenever integrity check is carried out. The system is also able to reconstruct the original value of altered data. To make this possible, an encrypted copy of the digitally signed records is saved. This is later decrypted and used by the supervisory software during altered data reconstruction. This paper has thus provided a novel combination of supervisory software, record level digital signatures and symmetric encryption to conserve data integrity throughout its life span.

Reference

1. Eliza Paul. What is Digital Signature- How it works, Benefits, Objectives and concept, 2017.
2. Foteini Baldimtsi. Efficient Cryptography for Information Privacy, 2014.
3. Georgia K. Cyber Physical Security for Power Grid Protection, 2014.
4. Grandison T, Maximilien EM, Thorpe S, Alba A. Towards a Formal Definition of Computing Cloud, in Services (SERVICES-1) World Congress on, 2010.
5. Hagemann John H. Securing Data by Encryption Accessed fromwww.bsa.org/encryptionmatters, 2015.
6. Kadhem H, Amagasa T, Kitagawa H. A Novel Framework for Database Security based on Mixed Cryptography; Internet and Web Applications and Services, 2014. ICIW '014. Fourth International, 2014.
7. Katanosh Morovat Data Integrity and verification in Cloud Computing, 2015.
8. McKendrick J. IOUG Enterprise Data Security Survey 2012: Closing the Security Gap, 2013.
9. Miao Zhou. Data security and Integrity in Cloud Computing, 2013.
10. Nabil Giweli. Enhanced Cloud Computing Security and Privacy, 2013.
11. Ricordo J. An Enhancing Data Security in Data Warehousing, 2014.
12. Introduction to cloud computing “office of the privacy of commission” Canada. Retrieve from www.bsa.org/encryptionmatters.