Crimson Publishers
Wings to the Research

Review Article

Security Concerns in Electronic Files Authenticated Systems

Femi Temitope Johnson[1]*, Elugbadebo Oladapo Joseph[2] and Akande Adenike Folasade[3]

[1]Department of Computer Science, Federal University of Agriculture, Abeokuta, Nigeria

[2]Department of Computer Science, Federal College of Education, Abeokuta, Nigeria

[3]Department of Computer Science, Babcock University, Ilishan-Remo, Nigeria. Abeokuta, Nigeria

ISSN: 2832-4463

***Corresponding author:** Femi T Johnson, Federal University of Agriculture, Abeokuta, Nigeria

Submission: January 22, 2024

Published: January 31, 2024

Volume 3- Issue 3

How to cite this article: Femi Temitope Johnson*, Elugbadebo Oladapo Joseph and Akande Adenike Folasade. Security Concerns in Electronic Files Authenticated Systems. COJ Rob Artificial Intel. 3(3). COJRA. 000565. 2024.
DOI: 10.31031/COJRA.2024.03.000565

Abstract

Traditional file management systems and manual processes have presented a number of difficulties and restrictions, such as difficult administration, inadequate security, and restricted data sharing options for users and organizations. After overcoming these obstacles, file management systems have typically moved to the more advanced models of today, which offer better features and benefits, particularly in critical areas where their applications cannot be compromised. The primary goal of this paper is to expound on the security concerns risks, issues associated with the traditional file systems and to highlight the benefits of implementing contemporary security measures for better data and information security in files authenticated systems.

Keywords: File encryption; Security; Management Concerns; Decryption; Algorithms

Introduction

The essential elements of our contemporary society are data and information. Their constant generation and regular interval utilization are indispensable to our day-to-day existence and decision-making processes. These days, a variety of data and databases are used by people [1], institutions and organizations in their daily lives and activities, such as phone directories, library catalogs, and dictionaries. Real-time use of blogs, WhatsApp, Facebook, Twitter, LinkedIn, and other websites on the Internet is one of the well-known means used globally for constant generation of data and information.

Figuring out how to stop illegal usage, safeguard, protect and prevent unauthorized access [2,3] to these sensitive, valuable and indisputable data while maintaining their integrity has occupied the heart of not only the organization users but also the security experts and researchers in the information security [4,5] space with topmost priority. They have continuously improved data security practices techniques to protect digital information from forgery, theft, corruption, and unauthorized access [6-8] throughout its entire lifecycle. The adopted methods cover major facets of data and information security, including administrative and access controls, logical security of software programs using cloud security frameworks and features, and physical security of hardware and storage devices [9,10].

Furthermore, a welcome development for the storage of information in cloudlets is made possible through cloud computing and its implementation methods. This makes it feasible to analyze the data using a variety of methods and produce quick results due to its associated characteristics (velocity, volume, value, variety, and veracity). The implementation of these contemporary methods for information storage and retrieval though seems to be effective [11,12] but have not totally eliminated associated risks or difficulties especially in bio-metric authentication systems [13].

Literature Review

One of the first attempts to computerize the manual filing system used in organizations for information storage was the adoption of the file processing system. The system helps in keeping computer files and the information they hold in a well-organized format to enable easy access and retrieval. They also use drives for storage and maintain the physical location of the files [14] unlike the traditional format where records and information are kept in different files and can be easily altered without detection [15].

In a quantitative study on the security of library information, Ariff et al. [16] involved two hundred and twenty-two university libraries in Pakistan. It was found that the majority of libraries did not have the common security procedures in place to safeguard their electronic records. During the digitization process of library content, certain users, particularly librarians who meet the requirements for responding to a 5-likert scale questionnaire, failed to address library vulnerability issues, putting them at risk.

The Authors in [17] presented an entropy and n-gram-based approach for the detection of malicious files. Their belief stemmed from the simple observation that any file that has been exploited should have less randomness than the original file. The proposed belief was examined using three distinct files. The findings indicated that a file's level of randomness decreases with a lower entropy value, and that overwritten data is almost always present in large quantities over a brief period of time, alerting formal investigators to the presence of corruption in a file. Restricting file access can help prevent unauthorized access to sensitive information. Researchers [18] created a window-based application that included user device privilege control mechanisms with distinct identifiers for both standalone and networked systems in order to support his claim. They tested a variety of file formats, including image, video, audio, and presentation files. The technique made it possible for files to be secured and protected in exactly 18.5 seconds.

In order to achieve and guarantee effective performance, many organizations that face difficulties implementing file security techniques frequently opt for one or more trade-offs [19]. It was observed that the trade-offs have resulted in an unbalanced real-world performance, functionality, and security requirements. In order to balance file performance, functionality, and security, they also created a file security system that makes use of trusted execution environments (TEEs) and shielded execution. Users and organizations are turning to cloud storage as a more secure method of sharing and storing data since its introduction. A file access control system with three phases of updating key signatures that can be used to grant or deny access to hosted files was proposed [20]. They modified the deferred re-encryption and revocation scheme to assess how well their suggested techniques worked. It was found that, despite offering a high rate of access revocation, it was only applicable to social network files.

Limitations of conventional file-based approach and benefits of database inclusion in management system

Considering the overall advantages of digitalization and the use of electronic file management systems [21,1] for file storage and retrieval, one may conclude that it contributes to calming alleviation of the tension and constraints of traditional file management with the following limitations.

Data Redundancy and inconsistency: The primary source of data redundancy and inconsistency in processing systems is the needless duplication of data files [2]. It may require more resources (storage space, time and money) and more work must be done to maintain the most recent versions of all files. Multiple files containing the same data do not get updated simultaneously in traditional file processing systems due to over-existence and duplication of data. This causes inconsistencies, conflict issues and compromises the accuracy of the data as a whole [22]. These disparities eventually erode the quality of the data file's content, which has an impact on the processing system's ability to generate accurate reports.

Poor Data Control and security: A traditional file system is decentralized by nature because the centralized control over data elements is often times not enforced. This leads to poor data control and security which also makes it difficult to enforce security checks and access rights because application programs are added on an as-needed basis.

Data and Program Dependence: Applications and programs in file processing systems are dependent on both data and programs. The requirements of the specific application determine the physical location, organization, and retrieval of files from the storage media. When there is a change in the format or structure of data and records in a file, the reports generated typically don't match. Either user must manually gather the necessary data or complex programs must be developed to retrieve data from every file.

Absence of sharing data Integration and the capacity for integration: Users encounter difficulties obtaining information that necessitates accessing data stored in multiple files [23] because independent data files exist. The traditional file system offers few options for sharing data, every application has its own private files, and users are not given many options when it comes to sharing the data with other apps.

One way to get around the limitations of the traditional file processing methods was to implement a basic database provision and inclusion. According to Cherry et al. [24] databases help with precise data management [24] and ensure that all data files are updated immediately after system updates. Other advantages of using databases in file management systems are as follows:

A. Data Independence and consistency: The effects of data redundancy are reduced in database managed systems. Programs that access the data are not impacted by modifications to the database structure because the data files are stored in a way that allows for this. Once every occurrence of a data item in the processing system has been recorded, there is no risk of one system updating the item while another does not.

B. Improved security, control and integrity of Data: The database administrators set up the database according to security requirements and manages who can access what information [25] With the help of a validation routine or by making the entry of one or more fields mandatory, users of the DBMS can impose restrictions on data [26]. It can guarantee that access to the data is restricted to authorized users only.

C. Data Accessibility and Enhanced Productivity: More data, formerly kept on disparate departments' and sometimes incompatible platforms' systems, is now available to users. Besides, it provides an easy-to-use query language so that users can query and get responses right away without having to pay a programmer to write the queries.

Encryption for Security Measures in File Management Systems

Preventing unauthorized users from stealing, altering, or erasing private information is enforced in encryption. During the encryption process, data is converted into cipher text and could be stored in a database [27] making it accessible to only users who possess the secret key to decrypt it. This is done by using a mathematical function to generate secret keys using one, two, or more algorithms. The user can request plain text when they want it by using decryption algorithms to extract cipher texts saved in the database. These algorithms can be used with the same key (symmetric method) or different keys (asymmetric method) used for encryption (Figure 1).

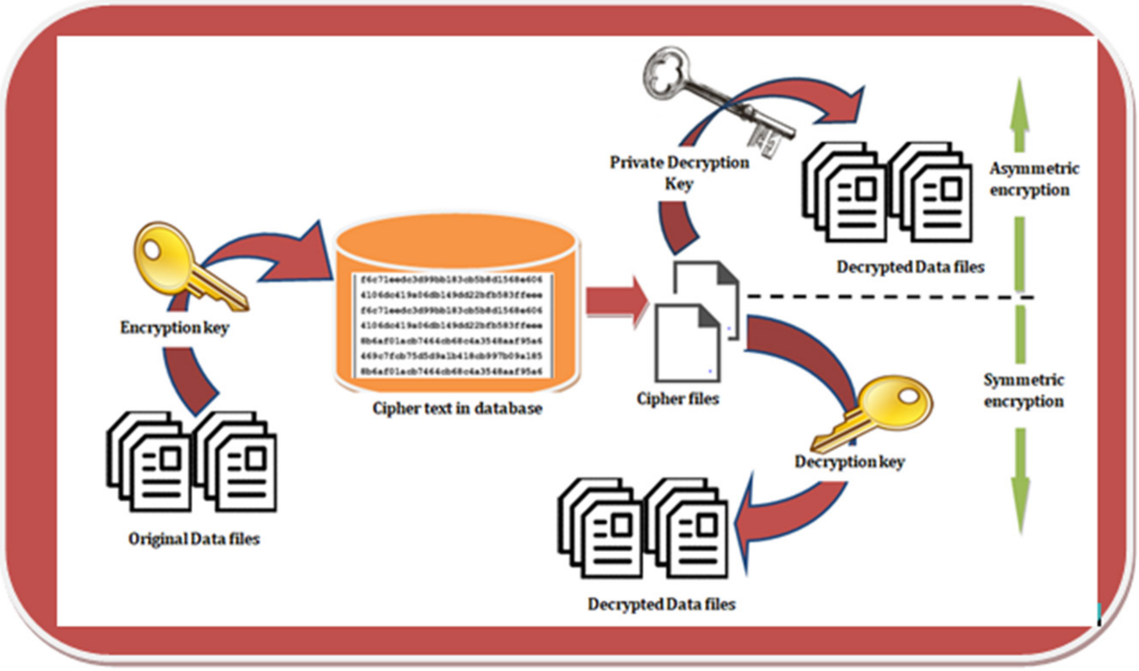

Figure 1: Encryption processes framework in database file management systems.

In addition, deploying hashing and encryption in a database limit access through authentication and authorization. Even with access to the database, an intruder cannot access the data if it has been properly encrypted before being saved in the database. A user can be assisted in creating a fixed-length value that condenses the contents of a file or message used in database-managed systems by deploying hashing techniques that make use of developed functions and algorithms. Database encryption also seeks to guarantee the proper use of data. The database structure needs to be carefully considered from the beginning, with security precautions supplied with keys at every development stage. It is simpler for unauthorized users to decrypt and access the database if all of the database's keys are the same.

Consequently, it is also necessary to match distinct corresponding keys to the various database sections and units. Several authors have used one or more of these methods to develop cryptography and digital signatures that impose integrity controls for better message and file security [4,15,28].

Another security measures for file management is Software encryption. Software development requires a lot of time in investment [29]. One common method of encrypting software is the provision of a combination of automatically generated codes in the form of serial numbers. Additional techniques is the adoption of internet facilities for software serial numbers of transfers through service providers with data encryption technology to create the serial number or registration code with the corresponding host ID.

Ensuring the authenticity of the transaction object and the total security of user data are very crucial for organization, especially in e-commerce. Although some unwanted activities by potential users may inevitably occur to circumvent the security measures put in place, the e-commerce application's security can be enhanced by the efficacy of digital signatures that encrypt user information and make them to be un-accessible to others. Furthermore, this public key can be used by the digital certification institution to decode the receiver's data and digital signature, identify any denial behavior, and take quick action to stop an attack.

Biometric systems for modern file security

Biometric data and systems are commonly used in security devices and are applied in systems that attempt to identify a specific user or other human through unique characteristics [30]. These systems depend on large amount of data [31] and rely on complex algorithms to sort and uniquely distinguish among multiple collected data to achieve an identifying result in a given application [32]. Biometric recognition is a challenging task but the human brain can carry out this incredibly complex process.

In spite of the fact that there have been several complaints about how trustworthy biometric authentication could be [33], other security measures have continuously been incorporated, setting them apart from more conventional password, PIN, or token-based authentication technologies [34]. The operational principles of biometric systems rely on two distinct processes: enrollment and recognition. At the enrollment phase, user's characteristics are captured, processed, and stored for later use in embedded systems. The enrollment procedures are highlighted below as.

A. The input signal is acquired by means of a biometric scanner. When the quality of the sensed signal is checked and found below a threshold it becomes rejected and a new acquisition is performed to fit the system.

B. The required data is extracted from the input signal by means of digital signal processing techniques.

C. Measured parameters and features from the data are stored and used for the modeling of each individual recognizable attribute. In addition, at the recognition mode, extracted features are compared with input signals from which access will be granted. Occasionally, access may be denied when the model fails to generate features for identification that would increase the Failure to Enroll (FTE) rate.

D. The second phase is the Recognition phase: Once the user is enrolled, the system can then proceed with the user identification or verification mode.

Security and privacy concerns for biometric systems

One of the astonishing features about biometric security systems is that users may be assigned equal level of access with or different level of privilege [35] depending on the user roles which makes it possess some level of security. When the hacker's goal of deciphering the password of at least one worker or user is accomplished, he is able to utilize all of the system's resources. This could also lead to overall security compromise of every system to which the user has access is compromised in this instance by a weak password.

Another concern with biometric systems is the fact that biometric data are not made secret [36] and could be difficult to replace after being compromised by a third party. Although, it may require simpler processes to rectify in some applications where the administrators can easily detect the authenticity of the data but in other internet enabled applications it could be very complex. Generally speaking, in terms of security issues, ongoing and continuous updates are required to maintain protection. Failure to update may turn the system to an obsolete type which can no longer be appropriate for the modern world. Because of this, no one can assert that they have a flawless security system or that it will endure forever.

The generation of too many false positive or negatives is also another concern in biometric based file authenticated systems. This occurs when a condition or file that exists in the system's database is devoted to being false or has not existed. Often times, this may result in the delay of the authentication process and access to urgently needed files as repeated trials will be demanded. The aftermath effect of this may result in severe damage especially in very pressing situations involving lifesaving conditions or seeking immediate protection from attacks. During these repeated trials, the system utilizes more resources and undergoes serious trials.

Conclusion

The problems with data and file security are ever evolving. Emerging best practices and improved identification techniques of newer threats to sensitive information protection keep people and organizations on the cutting edge. The architecture of the security system and related network, along with user privileges and mission requirements, must be understood in order to take a comprehensive approach to data, file security and combat emanating threats. The use of data encryption technology is expanding and is progressively being integrated into applications and systems pertaining to other fields including finance, education, healthcare, and energy.

These applications and systems do not only offer convenient security for businesses and government organizations, but also safeguard the lives of individuals. Biometric secured systems encryption offer more reasonable security features than password or pin secured systems. With this advantage, it is obvious that biometric systems with improved security features have begun to govern the security domain in our present days but the speed and accuracy of authentication is still worth looking into for improved solution.

References

1. Danielsen F (2021) Benefits and challenges of digitalization: An expert study on Norwegian public organizations. In: DG. O2021: The 22nd Annual International Conference on Digital Government Research, pp. 317-32.
2. Brunner M, Sauerwein C, Felderer M, Breu R (2020) Risk management practices in information security: Exploring the status quo in the DACH region. Computers & Security 92: 101776.
3. Prabhakar S, Pankanti, S, Jain AK (2003) Biometric recognition: Security and privacy concerns. IEEE Security & Privacy 1(2): 33-42.
4. Ali O, Shrestha A, Chatfield A, Murray P (2020) Assessing information security risks in the cloud: A case study of Australian local government authorities. Government Information Quarterly 37(1): 101419.
5. Johnson AL (2022) The analysis of binary file security using a hierarchical quality model Doctoral dissertation, Montana State University-Bozeman, Norm Asbjornson College of Engineering, USA, pp. 1-112.
6. Kubigenova A, Aktayeva A, Sharipbay A, Beissekov A, Muradilova G, et al. (2023) Views on big data technology information security. International Journal of Open Information Technologies 11(5): 63-67.

7. Thomas PA, Preetha Mathew K (2023) A broad review on non-intrusive active user authentication in biometrics. Journal of Ambient Intelligence and Humanized Computing 14(1): 339-360.

8. Rafique W, Khan M, Zhao X, Sarwar N, Dou W (2020) A blockchain-based framework for information security in intelligent transportation systems. Intelligent Technologies and Applications: Second International Conference, INTAP 2019, Bahawalpur, Pakistan, Springer, Singapore, pp. 53-66.

9. Manap A, Abitova G, Uskenbaeva G, Shaikhanova A (2023) Design of technology for secure file storage based on hybrid cryptography methods: Short overview. Vestnik Kazatk 129(6): 205-215.

10. Liu S, Shao W, Li T, Xu W, Song L (2022) Recent advances in biometrics-based user authentication for wearable devices: A contemporary survey. Digital Signal Processing 125: 103120.

11. Belanger F, Crossler RE (2011) Privacy in the digital age: A review of information privacy research in information systems. MIS Quarterly 35(4): 1017-1041.

12. Yang C, Wang L (2007) TLDFS: A distributed file system based on the layered structure. International Conference on Network and Parallel Computing Workshops pp. 727-732.

13. Almheri AMO, Patel SS, Sharma BK (2022) A conceptual study of forgery of 3D fingerprints and its threat to biometric security systems. Journal of Positive School Psychology 6(4): 4453-4462.

14. Feng G, Liu M, Wang G (2014) Genetic algorithm based optimal placement of PIR sensors for human motion localization. Optimization and Engineering 15: 643-656.

15. Hari N, Khairil K, Kurniawansyah AS (2021) The implementation of blowfish algorithm in client server network-based file security. GATOTKACA Journal 2(2): 97-108.

16. Khan A, Ibrahim M, Hussain A (2021) An exploratory prioritization of factors affecting current state of information security in Pakistani university libraries. International Journal of Information Management Data Insights 1(2): 1-8.

17. Muhammad Edzuan Z, Rohayanti H, Zalmiyah Z, Shahreen K (2021) Combination method for malicious file detection. Proceedings of Malaysian Technical Universities Conference on Engineering and Technology (MUCET) pp. 416-417.

18. Oyekan A, Oluwatobi (2021) File protection and security using basic access limits technique. Scientific & Engineering Research 1-5.

19. Burke Q, Beugin Y, Hoak B, King R, Pauley E, et al. (2023) Securing cloud file systems using shielded execution. Crptography and Security pp. 1-16.

20. Lakum T, Reddy T (2022) An efficient file access control technique for shared cloud data security through key signatures search scheme. Journal of Theoretical and Applied Information Technology 100(1): 1-10.

21. Tian Z, Li X (2021) Application of artificial intelligence technology in personnel files management. In: Cyber Security Intelligence and Analytics, International Conference on Cyber Security Intelligence and Analytics (CSIA2021) pp. 793-800.

22. Kang P, Yang W, Zheng J (2022) Blockchain private file storage-sharing method based on IPFS. Sensors 22(14): 5100.

23. Khan A, Ibrahim M, Hussain A (2021) An exploratory prioritization of factors affecting current state of information security in Pakistani university libraries. International Journal of Information Management Data Insights 1(2): 100015.

24. Cherry D, Larock T (2011) 2-Database encryption. Securing SQL server. In: Denny Cherry, Thomas Larock, (Eds.), Syngress, Boston, USA, pp. 27-71.

25. Bhojarau G (2003) Intranet for library services. Issues and Opportunities pp. 1-10.

26. Stegiadis C, Kostaridou VD, Veloudis S, Kazis D, Klados MA (2022) A personalized user authentication system based on EEG signals. Sensors 22(18): 6929.

27. Huang X, Dong Y, Ye G, Yap WS, Goi BM (2023) Visually meaningful image encryption algorithm based on digital signature. Digital Communications and Networks 9(1): 159-165.

28. Saqib RM, Khan AS, Javed Y, Ahmad S, Nisar K, et al. (2022) Analysis and intellectual structure of the multi-factor authentication in information security. Intelligent Automation & Soft Computing 32(3): 1-15.

29. Johnson F, Oluwatobi O, Folorunso O, Ojumu AV, Quadri A (2022) Optimized ensemble machine learning model for software bugs prediction. Innovations Syst Software Eng 19(1): 91-101.

30. Veeraiah V, Kumar KR, Kumari PL, Ahamad S, Bansal R, et al. (2022) Application of biometric system to enhance the security in virtual world. 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, pp. 719-723.

31. Abdulrahman SA, Alhayani B (2023) A comprehensive survey on the biometric systems based on physiological and behavioural characteristics. Materials Today: Proceedings 80: 2642-2646.

32. Singh G, Bhardwaj G, Singh SV, Garg V (2021) Biometric identification system: Security and privacy concern. Artificial Intelligence for a Sustainable Industry 4.0, Springer Cham, Switzerland, pp. 245-264.

33. Arora S, Bhatia MPS (2022) Challenges and opportunities in biometric security: A survey. Information Security Journal: A Global Perspective 31(1): 28-48.

34. Thomas PA, Preetha Mathew K (2023) A broad review on non-intrusive active user authentication in biometrics. Journal of Ambient Intelligence and Humanized Computing 14(1): 339-360.

35. Bhattacharyya D, Ranjan R, Alisherov F, Choi M (2009) Biometric authentication: A review. International Journal of u-and e-Service, Science and Technology 2(3): 13-28.

36. Ross A, Jain AK (2009) Biometrics, overview. In: Li SZ, Jain A, (Eds.), Encyclopedia of Biometrics. Springer, Boston, MA, USA, pp. 168-172.