Securing System Logs in Financial Institutions using Hybrid AES-ECC Cryptography

Arome Junior Gabriel
Department of Cyber Security
Federal University of Technology, Akure, Nigeria

Abstract

In today's modern Interconnected electronic world, securing log files is a significant problem which is rapidly becoming an issue of great concern to both individuals and corporate/business organizations. More often than not, editing (altering) or outright erasing of organization's log files seems to be the first point of call for hackers upon gaining access (unauthorized) into their system or network. This which they do in a bid to erase traces of their presence, often leaves system administrators clueless to the fact that they have been hacked, therefore preventing them from taking actions to secure their systems. This has often resulted in monumental loss to these organizations, especially those in the financial services domain like banks. Thus, development of secure methods for storing log files is of tremendous importance for continuous/sustained information security in such organizations. This paper proposes a hybrid Advanced Encryption Standard (AES) and Elliptic Curve Cryptography based framework for improving the security of log files in financial systems. This chemistry offers robust security of financial information. This will greatly enable organizations to mutually protect their sensitive log data even if their system or network gets maliciously compromised. The design was then implemented using Javascript, php and MySQL. The audit management system is robust against common cyber-attacks and has additional property of being lightweight and simple, that is, the proposed system has low computational resource demand

1. Introduction

The recent rapid advancement in technology, especially as it pertains to information and communication technologies, has made available enormous and vast amounts of information [1], [2]. This availability also generates significant risks to computer systems, information and to the critical operations and infrastructures they support [3], [4]. In spite of significant advances in the audit system management domain, many information systems are still vulnerable to insider or outsider attacks [5]. The existence of an internal audit for security audit management system increases the probability of adopting adequate security measures and preventing these attacks or lowering their negative consequences.

Security audit is a systematic evaluation of the security of a company's information system achieved by measuring how well it conforms to a set of established criteria [6]. A security audit is an audit on the level of information security in an organization. Within the broad scope of auditing information security there are multiple types of audits, multiple objectives for different audits, etc. Auditing information security includes physical security of data that centers on auditing the logical security of databases and highlights key components to look for and the different methods of auditing this area [7]. When centered on the Information Technology (IT) aspects of security auditing, it can be seen as a part of an information technology audit. It is often then referred to as an information technology security audit or a computer security audit.

Security audits, vulnerability assessments, penetration, testing have been described as the three main types of security diagnostics. Each of the three takes a different approach and may be best suited for a particular purpose. Security audits measure an information systems performance against the list of criteria. A vulnerability assessment, on the other hand, involves a comprehensive study of an entire information system, seeking potential security weakness. Penetration testing is a convert operation, in which a security expert tries a number of attacks to ascertain whether or not a system could withstand some type of attack from malicious hackers can include anything a real hacker might try, such as social engineering.

Attackers from diverse background and using diverse mechanism have been intruding into systems, in most publicly reported cases, the attackers had already been inside the compromised systems for weeks, months, or even years before the intrusion were finally detected. Similar cases have been found in Finland and in other countries and organizations all over the world. Sometimes intrusions have been made by professionals, where the professionals are

 | DOI: 10.20533/jitst.2046.3723.2022.0096

trying to intrude into the privacy of the company audit system, but in some cases, there have been simply trojan infections that have not been noticed by anyone. During this time systems have probably been monitored by administrators and even audited by internal or external organization. There has not been proper monitoring by administrators, auditing included only paper review or technical audit focused only on compliance. Due to these deficiencies, security measures are essential in audit management systems.

Cyber-attack incidences are growing exponentially, in most publicly reported cases, the attackers had already been inside the compromised systems for weeks, months, or even years before they will be detected, and volatile information will be stolen from the system which means to non-confidentiality of the system.

A large pool of cybercrimes can be carried out owing to exploitable vulnerabilities and loopholes in audit log files and their storage places or repositories. There is a serious need for a security structure or framework for ensuring the security of audit logs, especially in today's modern electronic society. Cryptography schemes would offer the solution required to guarantee security of system log files while in store or while being transmitted between client systems in banks and cloud storage servers remotely resident in the cloud.

All the afore-mentioned forms the major motivation for this current research work which is majorly targeted at developing a security structure or framework for cloud-based audit management systems in financial institutions.

Towards this end, a hybrid encryption algorithm which involves using two crypto-schemes: a symmetric Advanced Encryption Standard (AES) and an asymmetric algorithm Elliptic Curve Cryptography (ECC) is proposed. Using a symmetric algorithm otherwise known as private key cryptography with a single key for encryption and decryption coupled with an asymmetric algorithm (that is, public-key cryptography (PKC)) to enhance system log files in financial institutions offers so much benefits, and is described as good data security practice. While symmetric key encryption is of great advantage in terms of speed, and/or computation time, the public key encryption schemes have better key management than their private key encryption counterpart.

2. Related works

One of the best ways financial institutions have of protecting critical infrastructure is to monitor system logs, which contain a gold mine of information about the health of the network. Network devices such as servers, routers, firewalls, wireless access points, and antivirus systems all generate log data, which should be archived and monitored regularly for oversight of employee activity, as well as preventing and detecting system outages and breaches. When properly configured, logs record the day-to-day activity of system users, administrative changes made to critical production systems, and evidence produced by malicious activity. Logs provide a way to spot unusual activity from authorized users, as well as the ability to monitor unauthorized users and what they are doing when they get in. With the right logging configuration financial institutions can capture the history of a hacker's activity, from the establishment of unauthorized accounts to the installation of back-doors, enabling them to quickly isolate and repair affected systems after an intrusion.

Intruders will often attempt to conceal any unauthorized access by editing or deleting log files. Therefore, institutions should strictly control and monitor access to log files whether on the host or in a centralized logging facility. Some considerations for securing the integrity of log files include encrypting log files that contain sensitive data or are transmitted over the network; ensuring adequate storage capacity to avoid gaps in data gathering; securing back-up and disposal of log files; logging the data to a separate, isolated computer; logging the data to write-only media like a write-once/read-many (WORM) disk or drive; and setting logging parameters to disallow any modification to previously written data. When planning and implementing log collection and analysis, organizations often discover that they are not realizing the full promise of such a system. While collecting and storing logs is important, it is only a means to an end as knowing what is going on and responding to it. Thus, once the technology is in place and logs are collected, there needs to be a process of ongoing monitoring and review.

Looking at logs proactively helps financial institutions better realize the value of their existing security infrastructure. Network intrusion detection systems often produce false alarms of various kinds often leading to decreased reliability of their output and inability to act on it. Comprehensive correlation of network intrusion logs with other records such as firewalls logs, server audit trails allow companies to gain new detection capabilities from such correlation (such as real-time blocking and attack mitigation).

It is also very important that logs be converted into a universal format which allows financial institutions to compare and correlate different log data sources. Lack of standard logging formats leads to financial institutions needing different expertise to analyze the logs. Not all skilled Unix administrators will be able to make sense out of an obscure Windows event log record (and vice versa).

Individuals commonly have experience with a limited number of commercial intrusion detection and firewall solutions and thus will be lost in the log

 | DOI: 10.20533/jitst.2046.3723.2022.0096

pile spewed out by a different device type. As a result, a common format that can encompass all the possible messages from security-related devices is essential for analysis, correlation and ultimately for decision-making.

More than ever, financial institutions need to leverage modern technology to deliver improved customer experiences, at a lower cost, in real time. This requires the collection and processing of multiple data sources and the modernization of legacy systems and outdated operating models. Without an improved infrastructure, traditional financial institutions will be ill equipped to compete with more responsive and innovative competitors.

The majority of banking and financial services organizations have yet to deploy core systems to the cloud due to significant complexity and concerns over security, risk, governance and control. In fact, according to existing literature, "while about 90% of financial institutions are actively using (or plan to use) cloud services as of today, only 10% of mission-critical regulated banking workloads have shifted to a public cloud environment." It is safe to say that, Traditional banking systems are outdated and inflexible, making it costly to deploy new solutions or protect against advanced security risks

To address the need for capacity and speed, banks and credit unions are increasingly looking to cloud computing solutions to store data and support applied analytics. The result can be increased customer insights, improved efficiency, enhanced innovation, greater agility, and a reduced risk of security or business continuity breaches. As an overarching organizational advantage, cloud solutions can augment human productivity, providing insights that can positively impact both front-office and back-office transformation.

It is imperative for financial institutions to replace outdated on-premise infrastructure that has become harder and harder to update and increasingly costly to maintain. More than ever, successful organizations must look for flexible, scalable solutions that are both responsive and efficient. The technology is now available to help smaller banks compete. Waiting to leverage these new solutions is not a winning strategy.

Tian and Jing [6] reported a study on the development of a lightweight secure auditing scheme for shared data in cloud storage (LSSA) towards achieving security management of the groups and a lightweight calculation for the group members. lightweight secure auditing scheme for shared data in cloud storage (LSSA) is proposed, which achieves security management of the groups and a lightweight calculation for the group members. This work adopted the Hash graph technology and designed a Third-Party Medium (TPM) management strategy to improve agent security.

In Abu Othman et al. [7], the authors discussed the possibility of Information System (IS) audit in assessing mobile device security by exploring the risks and vulnerabilities of mobile devices for organizational IS security as well as the perception of Information system management in mobile device security.

The study by Ahmed and Khan [8] highlighted the high significance of audit logs. The authors posited that audit logs are important resources that demonstrate the current state of the systems and user activities. Such systems they stated, are often used for cyber forensics and maintenance. Sadly, these logs are susceptible to threats of several types (either insider or external). This article carried out a thorough survey of existing literature in a bid to identifying requirements of securing these very important audit logs. This study further emphasized the current challenges to these logs' security.

Livshitz et al. [9], the problem concerning the concept of the instantaneous information security (IT-Security) audits directed, including providing protection against "zero-day" threats was discussed. It was stated that effective "zero-day" counteraction based on implementation a set of preventive IT-Security controls, but not limited new technical facilities installation only.

Ismail et al. [10], presented a cloud security audit approach to enable users to evaluate cloud service provider offerings before migration, as well as monitoring of events after migration. The proposed approach entails a set of concepts such as actor, goals, monitoring, conditions, evidence, and assurance to support security audit activities. These concepts were considered as language for describing the properties necessary for cloud security audit both before and after migration.

Majumdar et al. [11] focused on the security auditing of Internet of Things devices. A technique for the extraction of actionable security rules from existing security policies and best practices and conducting security audits of Internet of Things devices. This approach was applied to devices in a smart home environment, and its efficiency and scalability were evaluated.

Gan et al., [12] introduced an online/offline remote data auditing (OORDA) framework that specifies the data auditing process as online and offline phases. A concrete OORDA scheme was proposed towards ensuring secure integrity checking for cloud data. The proposed OORDA scheme is probably secure in the random oracle model. Performance analysis confirms that the proposed scheme has optimized efficiency compared with the existing scheme.

In Wesland [13], publicly reported security breaches of internal controls in corporate information systems were investigated, with a view to determining whether U.S. Securities and Exchange Commission (SEC) data are information bearing

 | DOI: 10.20533/jitst.2046.3723.2022.0096

with respect to breaches of security and privacy. The analysis carried out supports a high predictability for credit card breaches, portable device related breaches and breaches conducted by firm insiders. This study also discovered evidence that employees are subverting particularly strict internal controls by using portable devices that can be carried outside the physical boundaries of the firm.

Several other authors have prescribed cryptographic means for achieving data security. For instance, Waters et al. [14] suggested an encrypted and search-able audit log scheme that offers verifiability and confidentiality preservation. Similarly, Attila Yavuz also proposed a cryptographic scheme as append only secure audit logging (LogFAS) in [15]. The system proposed by Schneier, and Kelsey [16] for secure logging, is one that detects any attempt at compromising the integrity of data on untrusted machines. What is also somewhat worrisome is the fact that most of the existing audit management system suffers susceptibility to common security breaches and even high complexity as well as high computational overhead. There is adequate motivation for the quest for a new.

3. The proposed system

The proposed system will consist of four (4) modules:

- User access control
- System activity monitoring
- The audit logs
- Vulnerability report

3.1. User Access Control

User access control is used to regulate who or what can view or use resources in a computing environment (see Figure 1). There are two types of access control: physical access control and logical access control. Physical access control limits access to campuses, buildings, rooms, and physical IT assets. Logical access limits connections to computer networks, system files and data. Logical access control will be considered whereby a unique username and password is generated to the user by the system. The set of all users in the organization is mathematically captured as:

$$U_n = u_1, u_2, u_3, \cdots, u_n \quad (1)$$

where, u_1→auditor
u_2→client 1
u_3→ client 2
u_4→ client 3
u_5→ client 4

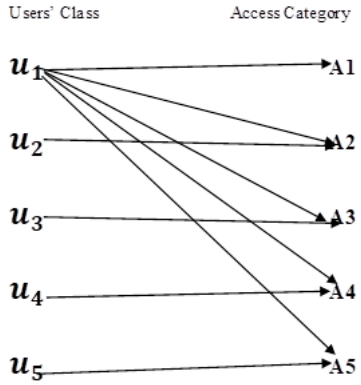

Figure 1. User's access control engine

U_1 representing the auditor can have full access to all system's views, reports and other information:

- U_2 can only have access to his/her own file
- U_3 can only have access to his/her own file
- U_4 can have access to his/her own file
- U_5 can have access to his/her own file

3.2. System Activity Monitoring

It is one of the many important tasks in the day of an administrator, monitoring the flow of work in the organization.

Some abnormal activities can be revealed during activity monitoring:

i. Monitor without the user knowing: view the computer in real time from the sever system. Activity monitor works invisible without slowing down the user computer.

ii. View multiple computers at the same time from your network. Activity monitoring could be illustrated as for instance, the problem of determining what is a normal activity and what is an abnormal activity:

If $t_o \leq T$ then
    Activity_type = Normal
Else
    Activity_type = Abnormal

where, T = Time threshold.
t_o = Time of user activity.

3.3. The Proposed System Architecture

The architecture for the proposed system is a four layered system architecture comprising of the application, access control, vulnerability scanning and the database layers:

 | DOI: 10.20533/jitst.2046.3723.2022.0096

3.3.1. Application layer: It serves as the interfacing layer of the system, it enables user interaction with the system via a user-friendly interface, this application layer conveys the user queries to the system. It conveys each of unique user authentication information to the access control layer of the system to determine the appropriate access level to be granted to the user.

3.3.2. Access control layer: This is the main security platform of the system; it is a logical layer which has instruction sets and rules to guide it in determining the function or appropriate task to execute at every use case scenario of the system. It receives unique instruction from the application layer, analyse the instruction and determine the access authentication for each specific users to determine their access to the auditory modules of the system.

3.3.3. Vulnerability scanning: Typically refers to the scanning of the systems that are collected to the internet but can also refer to system audits on internal networks that are not connected to the internet in order to assess the threat of rogue software or malicious employees in an organization. They seek out security flaws based on database of known flaws, testing system for the occurrence of these flaws and generating a report of the findings that an individual or an organization can use to tighten the network's security.

3.3.4. Database layer: A database is a storage location where organized information is stored, it is reliable because information can easily be managed, accessed and updated and also retrieved, it can also be referenced to for future purposes (see Figure 2).

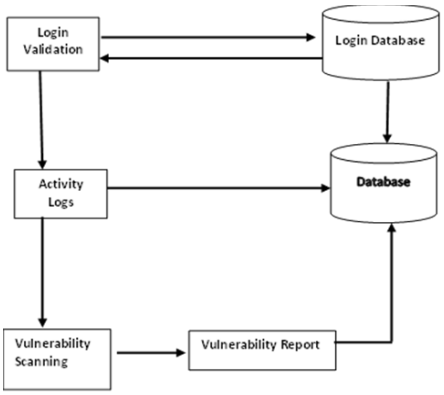

Figure 2. The Architecture of the proposed system

4. Results and Discussions

All program codes were written using java programming language. Other tools employed during the implementation phase include MYSQL. When the client and the admin launch the audit management system, the first page is the login page (shown in Figure 3), where the client and the admin will enter their unique username and password and will click on the login button. If the unique username and password corresponds to the one that is provided at the point of user registration or enrolment, then, the login will be successful, otherwise, the user is prevented from accessing the audit management system.

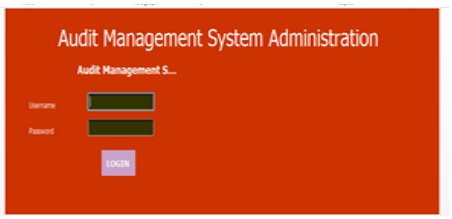

Figure 3. Admin/Auditor login page

Attempts to log in at odds (before/after working hours) would be rebuffed, and greeted with the message/warning display.

Once the login attempt is successful, then, the user is presented with the main menu page of the system (shown in Figure 4). Here the user is presented with a menu of activities or actions he can carry out on the system. All users' set of activities are limited or unique to them, except for the auditor, who by virtue of his role can carry out all sets of activities.

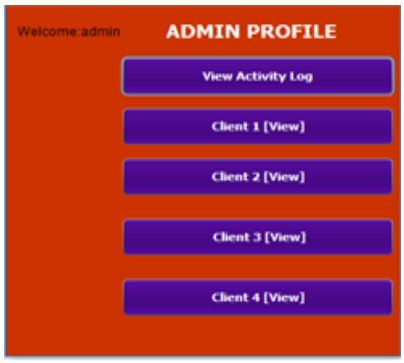

Figure 4. Admin menu page

The auditor vested with the duty of monitoring audits and keeping tabs on all activities within the system or organization, can view the general/entire audit log of the system. This enables the management to determine if a given user is working as should be. Non-repudiation is also prevented since, the log of every user's activity is collected and stored against their names or profiles, together with the time of day when such activity is carried out.

Furthermore, periodic vulnerability analysis of the system or organization can also be carried out using the proposed system. The vulnerability

 | DOI: 10.20533/jitst.2046.3723.2022.0096

analysis report page is the report generated after performing vulnerability scanning which actually provides information on vulnerabilities and risks identified, as well as suggestions. The proposed system automatically generates the vulnerability assessment report in a printable format.

The developed system also has a database used in the development of the audit management system; this database also keeps the information about the clients that is allowed to access the audit management system (via an authentication procedure).

5. Performance Evaluation

Performance evaluation of the proposed system was carried out, using standard metrics, especially the system's computation time, and throughput, in order to determine its suitability or its efficiency. The mix of AES and ECC (symmetric plus asymmetric crypto) offers efficiencies in speed and robustness respectively. Research has proven that the AES algorithm offers excellent strength, its cost-effective, and has little demand for memory, hence, is faster when compared to other symmetric encryption algorithms. The ECC on the other hand also has the characteristic of being fast and suitable for resource-constrained devices like sensors and mobile devices.
Table 1 shows the encryption and decryption runtime for varying sizes of data as transferred between Alice (the client) and Bob (the server) with file size stated. A graph of the result contained in the Table 1 is presented in Figure 5.

Table 1. Encryption vs Decryption times in the proposed system

Size (kb)	Time Consumed (secs)		
	AES	ECC	Proposed AES-ECC System
20	0.26	0.7	0.43
30	0.40	0.78	0.68
40	0.41	0.82	0.71
50	0.67	0.90	0.77
60	0.86	1.86	1.45

The results in Table 1 shows how the proposed hybrid model performed versus the individual AES and ECC crypto algorithms, in terms of time taken for encryption/decryption. It was observed that the ECC model took more time than the proposed hybrid AES-ECC system. Even though it was observed that the AES algorithm when implemented alone takes lesser time, the ECC algorithm might still be preferable, considering its better resistance to cyber-attacks, as well as the fact that ECC is better suited for resource-constrained devices such as sensors and mobile devices.

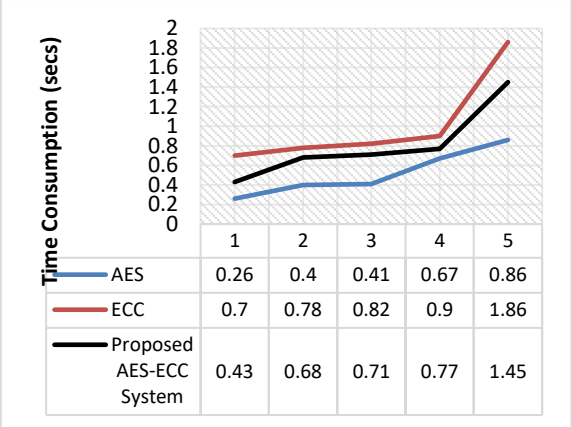

Figure 5. Graph of Time consumption of the proposed AES-ECC versus AES, and ECC

6. Conclusion and Future Works

In this paper, a detailed description of a cloud-based audit file log management system was given which is divided into four modules: access control, monitoring system, activity logs, vulnerability report. Security audit management systems have enormous potential for providing data security in a local area network environment. The system proposed is expected to enhance to a reasonable level that will help to enforcement access control policies in the development of the system. The access control policy used ensures that decisions are made based on a set of characteristics, or attributes associated with the users, the environment, and the time of login.

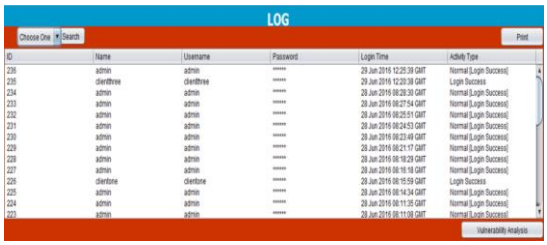

Figure 6. Activity log of the system

The major factor considered in this work for determining the type of user activity (normal or abnormal) is time (see Figure 6). Security audit systems with more factors could perform better.

7. References

[1] S. A. Oluwadare, A. J. Gabriel, O. G. Ogunride. (2019). Tabu-Genetic Algorithm-Based Model for Poultry Feed Formulation. International Journal of Sustainable Agricultural Research, Vol. 6, No. 2, pp. 94-109. DOI: 10. 18488/journal.70.2019.62.94.109.

 | DOI: 10.20533/jitst.2046.3723.2022.0096

[2] H. C. Ukwuoma, A. J. Gabriel, A. F. Thompson and B. K. Alese, (2021). Optimised Privacy Model for Cloud Data. 2021 16th International Conference on Computer Science and Education (ICCSE). pp. 267-269, DOI: 10.1109/ICCSE51940.2021.9569395.

[3] A. J. Gabriel, B. K. Alese, A. O. Adetunmbi, O. S, Adewale. (2015). Post-quantum crystography based security framework for cloud computing. J. Internet Technol. Secur. Trans. (JITST) 4 (1), 351-357.

[4] A. J. Gabriel (2020). Appliance Scheduling towards Energy Management in IoT Networks using Bacteria Foraging Optimization (BFO) Algorithm. In: A.E. Hassanien et al. (eds.). Artificial Intelligence for Sustainable Development: Theory, Practice and Future Applications, Studies in Computational Intelligence 912, pp. 290-310. Springer, Nature Switzerland. DOI: 10.1007/978-3-030-51920-9_15.

[5] A. J. Gabriel, A. Darwish, A. E. Hassanien, (2021). Cyber Security in the Age of COVID-19. In: Hassanien A.E., Darwish A. (eds) Digital Transformation and Emerging Technologies for Fighting COVID-19 Pandemic: Innovative Approaches. Studies in Systems, Decision and Control, vol 322. Springer, Cham.

[6] Tian, J., and Jing, X. (2019). A Lightweight Secure Auditing Scheme for Shared Data in Cloud Storage. In IEEE Access, vol. 7, pp. 68071-68082. DOI: 10.1109/AC CESS.2019.2916889.

[7] N. A. Abu Othman, A. A. Norman and M. L. Mat-Kiah, (2021). Information System Audit for Mobile Device Security Assessment. 3rd International Cyber Resilience Conference (CRC). pp. 1-6, DOI: 10.1109/CRC50527.202 1.9392468.

[8] Ali A., Ahmed M., Khan A., (2021). Audit Logs Management and Security - A Survey. Kuwait Journal of Science 48(3). DOI: 10.48129/kjs.v48i3.10624.

[9] Livshitz, I. I., Nikiforova, K. A., Lontsikh P. A., and Karasev, S. N., (2016). The new aspects for the instantaneous information security audit. 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies (ITMQI S). pp. 125-127, DOI: 10.1109/ITMQIS.2016.775 1920.

[10] Ismail, U.M., Islam, S., and Mouratidis. H., (2015). Cloud Security Audit for Migration and Continuous Monitoring. In 2015 IEEE Trustcom/BigDataSE/ISPA IEEE.

[11] Majumdar, S., Bastos, D., Singhal, A., (2021). Security Auditing of Internet of Things Devices in a Smart Home. In Peterson G., Shenoi S. (eds) Advances in Digital Forensics XVII. Digital Forensics 2021. IFIP Advances in Information and Communication Technology, vol 612. Springer, Cham. DOI: 10.1007/978-3-030-88381-2_11.

[12] Gan, Q., Wang, X., Li, J., Yan, J., and Li. S. (2021). Enabling online/offline remote data auditing for secure cloud storage. Cluster Comput 24, 3027–3041 (2021). DOI: 10.1007/s10586-021-03303-6.

[13] Wesland, J. C. (2021). Assessing Privacy and Security of Information Systems from Audit Data. Journal of Information Systems Frontiers. Springer Professional.

[14] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters. (2004). Building an Encrypted and Searchable Audit Log. In 'NDSS', Vol. 4, pp. 5–6.

[15] Yavuz, A. A., Ning, P., and Reiter, M. K. (2012a). 'BAF and FI-BAF: Efficient and publicly verifiable cryptographic schemes for secure loggingin resource constrained systems', ACM Transactions on Information and System Security (TISSEC 15(2), 9.

[16] B. Schneier, and J. Kelsey, (1998). Cryptographic Support for Secure Logs on Untrusted Machines., in 'USENIX Security Symposium', Vol. 98, pp. 53–62.

8. Acknowledgements

Many thanks to the Federal University of Technology, Akure, Nigeria, for providing the environment for the study.