Scientific Research Publishing

Journal of Computer and Communications, 2023, 11, 166-189
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

# Design of an E-Administration Platform and Its Cryptography-Based Security Model

**Ohwobeno Omohwo[1], Iwasokun Gabriel Babatunde[2], Boyinbode Olutayo Kehinde[3], Gabriel Junior Arome[4]**

[1]Department of Computer Science, Delta State University, Asaba, Nigeria
[2]Department of Software Engineering, Federal University of Technology, Akure, Nigeria
[3]Department of Information Technology, Federal University of Technology, Akure, Nigeria
[4]Department of Cybersecurity, Federal University of Technology, Akure, Nigeria
Email: gbiwasokun@futa.edu.ng

**How to cite this paper:** Omohwo, O., Babatunde, I.G., Kehinde, B.O. and Arome, G.J. (2023) Design of an E-Administration Platform and Its Cryptography-Based Security Model. *Journal of Computer and Communications*, **11**, 166-189.
https://doi.org/10.4236/jcc.2023.114008

**Received:** March 22, 2023
**Accepted:** April 25, 2023
**Published:** April 28, 2023

## Abstract

E-administration is performing administrative works via computer and its associated technologies such as the Internet. It is administrative efforts that center on the exchange of information and providing services to people and the business sector at high speed and low cost through computers and networks with the assurance of maintaining information security. It is based on the positive investment in information technology and communication in administrative practices. This paper presents the design of the e-administration platform that adopts the concept of cryptography for identity management. The architectural framework of the platform comprises subcomponents for service and forms identification, business process redesign, service architecture, amalgamation, and deployment. The cryptography model for securing the platform was designed based on the combination of authentication criteria presented in the Rijndael-Advanced Encryption Standard (AES), Lattice-based cryptography (LBC), and Secure Hash Algorithm (SHA512). It is required that a record be encrypted prior to its commitment to the database via a double encryption method. The AES algorithm-based encryption's output will form the input to the LBC algorithm to obtain the final output.

## Keywords

E-Administration, Cryptography, Management System, Encryption and Decryption

## 1. Introduction

The authors in [1] defined administration as organizing and maintaining human and fiscal resources to attain organizational goals. Public administration consists of all those operations that are concerned with the fulfillment or enforcement of public policy and it involves the detailed and systematic application of law, policies, practices, rules, and regulations [1] [2] [3]. The school administration has also been taken as one of the most central aspects of administration and the most paramount in some communities. Its contributions range from the implementation of educational policies and objectives to raising future generations and qualifying them in a rapidly changing era. School administration through unswerving contact with the community, provides care, education, and a proper environment that would academically qualify students, leading eventually to the upgrade and progress of the community. School administration involves the management of all school operations with a view to achieving a safe learning environment and effective implementation of the school budget. School administration at the postsecondary level has become a little more intricate as the size and number of colleges and universities are typically increasing with much larger and more organized activities. The school administration may be splinted into areas like admissions, student affairs, the registrar's office, and academic affairs. Each of these areas has its established administrative duties that are needed for students and staff services and keeping the school running [4] [5] [6].

The administrative formations and mode of operations of universities in Nigeria differ and depend to some extent on their stated objectives, the orientation of their managers, and the areas of specialization. Structural and operational details are usually plainly specified in a document that is enacted into the Enabling Law or Decree (ELD) of the particular university by the national or state government that owns it. The ELD defines the governance structure and clearly spells out the responsibilities and limitations to the powers and authority of each of the organs and the officers of the institution [4]. Despite the diversities, there are several common areas in the ways of administering the affairs of the universities [7]. Many universities in Nigeria function through the office of the Visitor who is usually the head of the organization that owns the institution, which is the President in the case of federal universities and the Governors, for state-owned universities. There is an office of the Chancellor who is the titular or ceremonial head of the university. He oversees the awards of degrees at Convocation ceremonies. The Pro-Chancellor is the Chairman of the Governing Council as well as some Committees of the Council such as the Finance and General Purposes Committee and Tenders Board. His office oversees the critical operations of the institution in synergy with the Visitor or Chancellor. The Governing Council (GC) is a team of those appointed by the proprietor(s) usually from outside the institution representing the public interest, ex-officio members, and those elected from the university representing the Senate and Congregation. Its mandate is to oversee the smooth running of the university vis-à-vis general control and superintendence of the policy, finance, and property of the university, including its public relations.

The Vice-Chancellor is the administrative head of the university and is responsible for its day-to-day management. The individual in this office and other very highly placed officers of the institution, such as the Deputy Vice-Chancellor (s), Registrar, Bursar, and University Librarian are often referred to as Principal Officers whose mandate is to ensure a smooth running of the affairs of the university. The Senate of a university serves as the supreme body on academic matters and is charged with the responsibility of initiating and supervising courses of studies and organizing as well as controlling teaching, admission, and discipline of students and the promotion of research. It is chaired by The Vice-Chancellor or its representative. The Convocation is the assemblage of the staff and students of the university that oversees the award of degrees and diplomas as approved by the Senate. It comprises a graduate staff of the university who meet to express opinions on various issues in the institution. The Vice-Chancellor presides over Congregation and also Convocation, in the absence of the Chancellor. Colleges, Schools, Faculties, and Departments are academic units that all report to the Senate and have different levels of responsibilities. The teaching, learning, and research activities of a university are carried out through them. Related Schools or Faculties make up a college while related Departments constitute a faculty. Most universities operate the "Committee System" in the decision-making process in which issues are freely debated at scheduled meetings and democratically decided upon. In some cases, such decisions may need ratification by higher bodies, like Senate on academic matters and Council, prior to implementation [7] [8] [9] [10].

### 1.1. E-Administration

The e-administration is performing administrative works via computer and its associated technologies such as the Internet. It is administrative efforts that center on the exchange of information and providing services to people and the business sector at high speed and low cost through computers and networks with the assurance of maintaining information security. It is based on the positive investment in information technology and communication in administrative practices [11] [12] [13]. In the contemporary world, technology is evolving and the educational system is seeking to use electronic administration for the attainment of set goals. The technological transformations in the educational sectors have become fait accompli with the acceptance of the Internet and Information and Communication Systems (ICTs) [14]. Technology-based education is now one of the ways of growing education with the appropriate administrative system [15]. According to the authors in [16], organizational transformation involves transforming and changing the existing corporate culture to achieve a competitive advantage or address a significant challenge. It is a visible action engaged by organizational leaders to move from the present manual data management to the emerging computer-based data administration with a view to reaching a specific target or goals. Hence, the adoption of technology in education administration and management is key for its development and expansion [17] [18]. The growing trend of the adoption of technology in administration is attributed to its ease of design and operation [19] [20] [21] [22]. E-administration as a modern alternative keeps pace with recent developments for providing relief and satisfaction to customers and meeting management demands [23]. The orientation towards e-administration is an urgent need for societies and a strong motivation for administrators to engage in self-development which is required for solving peculiar management issues through avoidance of traditional and bureaucratic styles in favor of a more flexible and friendlier electronic style [24]. E-administration brings different changes to administrative works and methods as well as provides timely and low-cost information for better quality and performance [11] [25].

The functions of e-administration include electronic planning by using modern information systems, regulation of activities that contribute to achieving organizational purposes, and instant control via the help of internal networking which increases the possibility of following up on various operations, decisions, error handling, and effective leadership. E-administration also helps in the effective management of huge data required for daily operations [26] [27] [28] [29] [30]. The challenges to the smooth implementation of e-administration include regulatory as well as technical obstacles such as hardware specifications, lack of experience among principal actors, poor infrastructure, and apathy to dealing with such modern systems by workers. There are also financial obstacles such as the cost of acquisition, installation, and training. According to the authors in [31]-[36], e-administration is connected to the understanding of competencies and effectiveness in administrative tasks, and its success is greatly associated with the organizational culture and adoption of technology. The most prominent requirements to apply e-administration are developing a strategic plan and the exploitation of human and material resources which need training to achieve effort minimization, expanding administrative work, and easiness of operation [24] [37]. Based on needs and interests, the categories of e-administration services include government agencies, businesses, citizens, and employees [38] [39]. The four types of e-government based on their missions and tasks performed are Government to Citizen (G2C), Government to Business (G2B), Government to Government (G2G), and Government to Employees (G2E) [40] [41] [42]. Security is the pillar of building a strong relationship of trust between individuals on communication or administrative platforms. Such platforms are expected to establish the security and integrity of data, ensure compliance with the expectations of citizens, as well as strengthen a climate of trust between the system and the users. The fight against cybercrime and fraud is costly measured and weighs heavily on public trust in e-administration [43]. Hence, the protection of the e-administration system against accidental or intentional disclosure to unauthorized access, modification, or destruction has been of great concern. In this context, several studies have focused on issues related to IT security for citizens and administrations, and a common agreement has been reached that IT insecurity is a barrier that limits the development of e-administration worldwide [43] [44] [45].

### 1.2. Cryptography

Cryptography is the discipline of encrypting and decrypting information or data such that it is secured. It is a concept of keeping information or data in secret during the course of its transmission over an unsafe or untrusted network [46] [47] [48]. The basic model of a cryptographic system is conceptualized in **Figure 1**. The original unenciphered text is called plaintext. The conversion of a plain text message to its cipher text is called enciphering or encryption [49] [50].

Cryptography is often used to establish a secured communication between two parties or private storage such that data is made to appear unintelligible to third parties. It is closely associated to encryption, which is a rescindable process of translating data into non-understandable and unintelligible form, otherwise known as ciphertext. The reverse of encryption is decryption which is used to transform a ciphertext into its original, clear and intelligible data. Based on its hash-proof and intrusion resistant formation, cryptography promotes data confidentiality, integrity and non-repudiation [50] [51]. These gains explain the reason why cryptography is mostly adopted for securing most e-administration platforms. For guiding against teardrop, IP spoofing, man in the middle attack among others, cryptography is being prominently used as security backbones in shopping and banking systems and any other system that utilizes the website advantages [46].

Modern cryptography has shifted from the linguistic and lexicographic patterns to mathematical theory and computer science practice. Its recent algorithms are designed around computational hardness assumptions, such as the integer factorization or the discrete algorithm that is easy to state but hard to solve. Algorithms are considered computationally secure even if they are theoretically possible to break by any adversary but unfeasible to do so by any known practical means in useful time [49] [52]. The modern field of cryptography is divided into symmetric and asymmetric cryptography. Symmetric cryptography is based on key sharing between both parties and on an encryption algorithm that uses the shared key to transform intelligible data into unintelligible data and vice-versa. The use of a secure channel to distribute the key is mandatory coupled with the assumption that the encryption/decryption algorithm is known by both parties. The drawbacks of symmetric cryptography include the compromise of

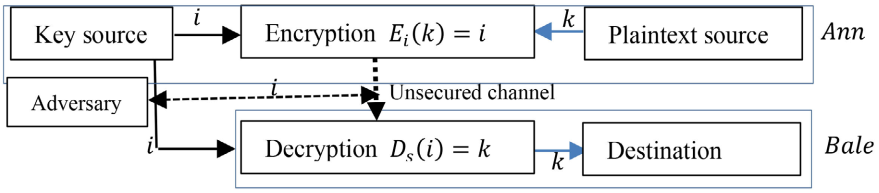

**Figure 1.** Two-party communication using encryption, with a secure channel for key exchange.

all communications by key disclosure to third parties and the ability of both sides to falsify communications. Asymmetric cryptography uses cryptographic algorithms that need duo related keys. It sometimes offers enhanced security that depends essentially on the size of the key used, though symmetric encryption is much faster. On this ground, asymmetric cryptography is mostly used to supplement symmetric cryptography [49] [50] [53] [54] [55].

The Advanced Encryption Standard (AES) (20001) represents state-of-the-art symmetric cryptography that traces back to the end of the 20th century. It was raised for countering and achieving fast integrated circuits required for protecting secret and sensitive information [56]. Other cryptography algorithms include the Rivest Shamir Adleman (RSA), Secure Hash Algorithm (SHA), keyed hashing, authenticated encryption, secret key, public key, and hash function. The RSA algorithm was presented as a breakthrough in asymmetric cryptography. Its security derives from the difficulty of factorizing large integers that are the product of two large prime numbers [57] [58]. Cryptographic hash functions are operations that map a dynamic-sized input to a fixed-size output through mathematical properties, called the hash value or digest. These functions are one-way functions and are impracticable to inverse. Their supporting algorithms must be fast on the hash value computation and must be deterministic. For any given input, the hash function must always produce the same output [59] [60]. The SHA is a family of cryptographic hash functions that are universally adjudged as the most suitable substitutes for the Message Digest 5 (MD5) algorithm that is susceptible to collision attacks [61] [62]. Keyed hashing is used to confirm that the message came from the stated sender and has not been changed and it is achieved through Message Authentication Code (MAC). MAC protects a message's integrity and authenticity by creating a value $T = \mathrm{H}(K, M)$, called the authentication tag of the message $M$, using the secret key $K$ [49] [63] [64].

Authenticated Encryption (AE) is a type of cryptographic technique that promotes the protection of a message's confidentiality and authenticity. It is based on the combination of a symmetric key block cipher to encrypt the message with a MAC algorithm, to produce the authentication tag. AE is based on encrypt-and-MAC, MAC-then-encrypt composition, and encrypt-then-MAC construction. These three approaches can be used to obtain an authenticated encryption algorithm and they differ in the order in which encryption is applied and the authentication tag is generated [59] [65] [66]. In secret key cryptography, encryption is done by converting the message (plain text) into unintelligible data by using a single key. The unintelligible data produced as a result of encryption is equal in length to the plain text. Decryption is consequently performed to obtain the plain text by using the same key as shown in **Figure 2**. Public key cryptography is asymmetric cryptography that uses an exclusively kept and confidential private key and a public key that is possibly identifiable [46].

## 2. Related Works

The authors in [67] proposed a digital signature (DS) and RSA encryption model

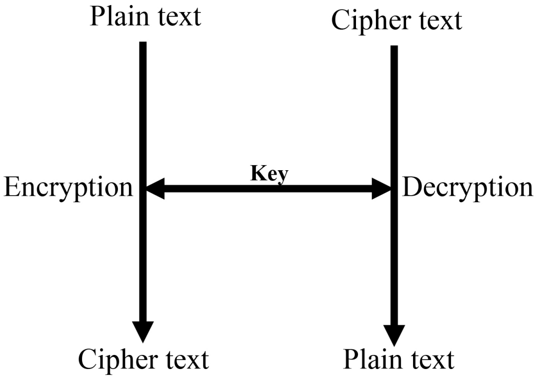

**Figure 2.** Flow diagram secret key cryptography.

for enhancing cloud data security. The RSA encryption algorithm was used for the encryption of data-in-transit while a digital signature was used to sign-in and message verification. The model addresses some of the prevalent cloud security challenges though no record of its implementation with real cloud or financial data. The authors in [68] used digital signature and Rijndael Encryption Algorithm to enhance the security of data in cloud computing towards promoting data privacy and user authentication. The research established a cloud data security framework for clients' data and cloud networks, but its practical function with online cloud data transmission could not be established, thus lacking in the areas of integrity and reliability. A model for securing data in the cloud using a digital signature mechanism was presented in [69]. The model was formulated as a means of protecting data privacy and managing compliance during cloud data transfer. No consideration was given to some cryptography enhancing schemes like hash function which may subject its key exchange to attack. A cloud-based model for preserving privacy and detecting suspicious cases in online financial transactions was presented in [70]. There is a data aggregation subcomponent of the model used for perturbation or data disguising and distortion prior to mining with a view to maintaining data integrity and performance. It also incorporated a support vector machine, correlation analysis, histogram analysis, and clustering for financial pattern analysis. The model could minimize the various types of risk or threats posed to online financial dealings though, its operation may violate individual privacy when they access and analyze real datasets. The authors in [71] established an ensemble of digital signature and encryption algorithms for cloud user authentication. The AES algorithm was used for data encryption while Secure Hash Algorithm (SHA) was used to obtain the hash value. An experimental study revealed the model could provide a reasonable level of cloud data security though with efficiency and brute force attack issues. A secured cloud data service access privacy-preserving model was presented in [72]. The model was formulated for the prevention of unauthorized data access and sharing in the cloud storage. An AES algorithm was used to achieve data anonymity and protection in multiple-user cloud real-time storage. The model offered centralized management of secret keys for data sharing but was susceptible to brute-force attacks due to data symmetry. The authors in [73] proposed a digital signature and advanced encryption standard framework for achieving very reliable cloud data security and user authentication. The model requires the data owner (sender) who intends to store the original documents in the cloud for sharing with the data users (recipients) to first create a digital signature for the document based on SHA-based computation of a hash value representation of the original document. The laboratory study of the model justified its extensive data authentication and encryption capability, though with key management issues.

The authors in [74] presented a password, RSA algorithm, hash algorithm, and digital signatures model for ensuring the integrity of data stored in the cloud. The RSA encryption algorithm was used to achieve data encryption while password, hash algorithm, and digital signature were used to promote data confidentiality and user authentication. The hash function established a key derivation function for deriving the encryption keys and a unique fixed-size hash value or message digest which is encrypted with the private key of the originator to produce the digital signature. The model offered a proven platform for securing cloud storage, though not without brute force attack issues. It also lacks terminal security which makes it unfit for the implementation of end-to-end security. An RSA digital signature and image steganography mechanism for cloud data security was proposed in [75]. RSA algorithm was used to model digital signature and image steganography transactions over the cloud as well as to encrypt and decrypt the data. The digital signature was used to sign and verify the data while image steganography was used to conceal the presence of the data in the course of its transmission in the cloud. The simulation of the model established its working principle and ability to provide the intended services in cloud data management. A high computational overhead for image encryption and decryption was also noticed. The author in [76] proposed the design and implementation of a multilevel secure system for data and information exchange on the website. The system provides a multi-tier web server system for protecting its streamed data from possible security attacks. The system uses authorization and authentication mechanisms to provide a secure environment for real-time data, file, and page content transfer. The password hashing algorithm is also robust and crack-proof in addition to the RC4A and Secure Sockets Layer/Transport Layer Security (SSL/TLS) security-enabled communication between Web browsers and servers. Investigation of the practical function of the system established its suitability for securing online communications, though with a major drawback that the key should be as long as the plaintext, which increases the difficulty of key distribution and management. In [77], an identity-based encryption and filtered equality test model for smart healthcare information control and management was presented. The model is focused on securing outsourced to the cloud infrastructure. The model is fit to verify if a ciphertext belongs to a message set without decryption. The elimination of the decryption process promotes time conservation in healthcare information control and management in real-life scenarios. Investigation revealed the model satisfies one-way security against the chosen identity and ciphertext attack in the adopted backend and achieves greater functionality than most previous schemes, though its total computational cost increases linearly with the number of messages.

The authors in [78] proposed an encryption-classes model for database information sharing and management. The model provides data encryption as an advanced measure for consolidating database security. The model offers a complete set of security mechanisms to date compared to some existing models but failed to consider the access limit for database users belonging to specific categories. The authors in [79] proposed a Multi-faceted Smart Card (MSC) and Multi-purpose Electronic Card (MEC) security model for e-governance. The focus of the model is the prevention of cross-border infiltration which is at present one of the major security threats. It was also designed for the improvement of security during the transmission of sensitive information and data between citizens and the government via the Internet. Unified Modelling Language was used to describe the deployment of information to the citizens based on an e-governance model that is based on a Multipurpose Electronic Card (MEC) in Citizens to Government (C2G) type of transaction. The e-governance model applied digital signatures and elliptic curve encryption for the security of information. The model suffers from major drawbacks in areas of expansive implementation and its validity for broad applications. In [80], the design and implementation of a customized encryption algorithm for authenticated and secured communication between devices was proposed. The algorithm sought to provide a platform for securing relevant information against intrusion, eavesdroppers, attackers, and unauthorized users. The encryption algorithm and the authentication scheme were customized for safe data and information transmission. The usefulness of the algorithm in IoT-based communication was stated with how it can achieve prominence in secured robotic communications, although with extensive computation.

In [81], a cryptography-based multilevel protection scheme for visualization of the network security situation is presented. The scheme adopts Region Incrementing Visual Cryptography Scheme (RIVCS) for encoding secret situation images in network security and encoding matrices for sharing secret pixels. The experimental study of the model is justified by its ability to guarantee data integrity as well as its multi-level security privacy protection capability. An architecture for information hiding in image steganography, by using genetic algorithms and cryptography was presented in [82]. The main point of the architecture is the possibility of proffering a solution to the leakage of secretive and sensitive information communicated through the Internet and media. The architecture enhanced the stenographic data potency by integrating the soft-computing facet in its feature selection and used a compression algorithm to squash or reduce the size of the input file leading to fewer periods and less room in encryption and memory transfer in a suitable order. However, the experimental study of the architecture could not be established.

The limitations of the works reported in [61]-[82] include lack of integrity and reliability, violation of individual privacy, susceptible to brute force attack due to data symmetry, lack of terminal security leading to inability to implement end-to-end security and high computational cost that increases linearly with the number of messages. These limitations provide a research gap that served as motivation for the research being reported.

## 3. The Design of an E-Administration Platform

An e-administration platform that adopts the concept of cryptography for identity management is proposed. The architectural framework of the platform is shown in Figure 3 with six processes; namely service identification, identification of forms, business process redesign, service architecture, integration and deployment.

### 3.1. Service Identification

The service identification unit will be used for prioritizing e-services in an iterative pattern, guided by both transaction criteria and the perceptions of stakeholders. The procedure for ordering the services will be based on an unbiased assessment of significance, picturing the finest approach for vindicating, organizing, and ordering activities for recording indigenous acquaintances and preliminary

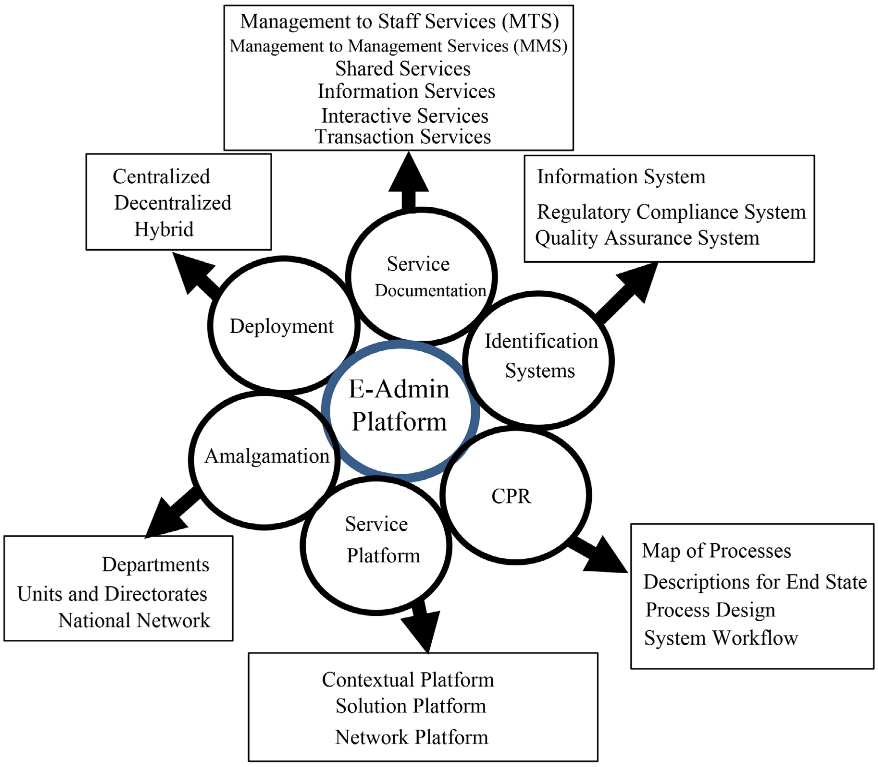

Figure 3. Proposed architecture for e-administration system.

circumstances. It will do with collating information from subordinate channels to identify the main services and stakeholders. The various categories of services include management to staff (M2S), management to management (M2M), shared, information, transaction, and iterative services. M2S represents transactions between staff and their units and could be information management (intranets), knowledge management (content management systems), and collaborative and communication management (e-mail, messaging systems). M2M is amenities or transactions at management, faculty, unit, and departmental levels. Shared Services represent e-services and other stakeholders' support such as payment online and any customer-oriented service. Informational Services include general information in the form of directives in the regular sequence of events as well as those that connect to the different users. Interactive Services are concerned with complex and official communications between participants in which message is directed through email, and online feedback, among others. It also includes the capability to hunt for chronicles, move files and requests as well as submissions. The transactional Services unit is functionally interactive and is concerned with providing a widespread group of facilities through connected transactions like housing and car loan applications for staff support. The integrated Services unit ensures the system offers smooth, hitch-free, and focused services that are bunched alongside collective requirements and connected for easiness.

### 3.2. Identification System

This unit is designed to help stakeholders to keep an organized and simplified procedure in efficient, timely, secure, achievable, and cost-saving manners. The unit comprises information gathering, transaction processing, regulatory compliance, quality assurance, and evaluation and assessment subsystems.

### 3.3. Corporate Practice Reformat (CPR)

The CPR unit is designed to handle a thorough assessment and detailed re-formatting of activities and events across units and departments. It is expected to guarantee the redesign of processes towards ensuring effectiveness and optimality in service delivery by the management, employees, and the immediate community. Some of the activities covered by this unit include process mapping, defining end-state, data analysis, and process redesign and workflow. The unit will be useful for achieving lower operational costs, higher system efficiency and reusability scale, customer satisfaction, and boosting revenue.

### 3.4. Services Platform

This unit is designed to be service-centric with a web-based interface as well as some other important features of the architecture such as business functionality, and extensible support to multiple access devices such as desktop computers, mobile devices, and so on. It will be used to achieve interoperability between the institution-based portals, integrate all departmental service-oriented applications and websites of all existing units, and for content hosting. The unit will provide easy access to management information and services, support focused service delivery channels, and provide information, applications, and services in a single consolidated browser view as well as a secured and personalized view of multiple online resources and interactive services. In addition, the service platform will offer a mono entree unit to important and classified information with fundamental presentations required for availing the services. In a simplified manner, the platform will present an interface between the management and other units as conceptualized in **Figure 4**.

### 3.5. Amalgamation

This unit will be used for the interconnection of discrete and independent subsystems. The amalgamation will foster better services and present a solitary source of information for all the subsystems as well as give a running platform or start point for all the services provided by the various subsystems. The functionality of the applications and amenities of the various units is also made available as services using web technologies. This promotes reusability, ease of integration, interoperability and ease of access to services, data and information. **Figure 5** summarizes the amalgamation method for the system.

### 3.6. Deployment

The deployment of the proposed system will follow the centralized architecture that standardizes all the amenities and services on the platform. The deployment model will optimize the gains and spear-head increased integration of the various units. It will also provide centralized control, one-time unified infrastructure, the basis for the management team to concentrate on their core business and duties, centralized control and a unified business model among all units and departments. Furthermore, the deployment model will help to achieve cohesive workflow across the management units, reduction of redundancy and duplication of effort, resources and expertise. The data flow diagram of the proposed university e-administration system is shown in **Figure 6**.

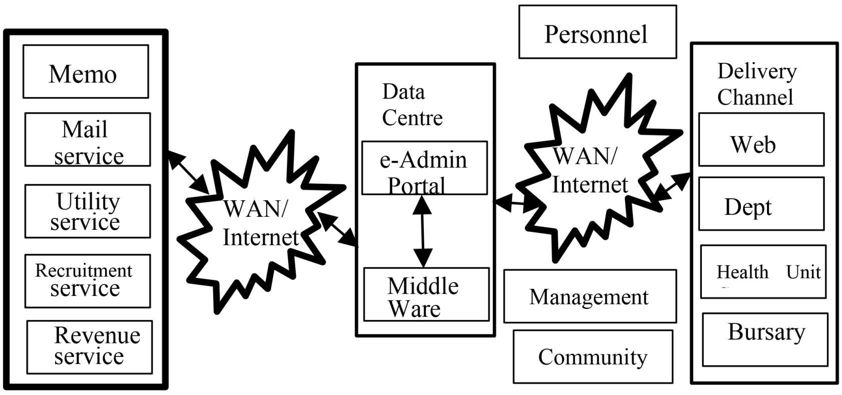

**Figure 4.** E-administration portal.

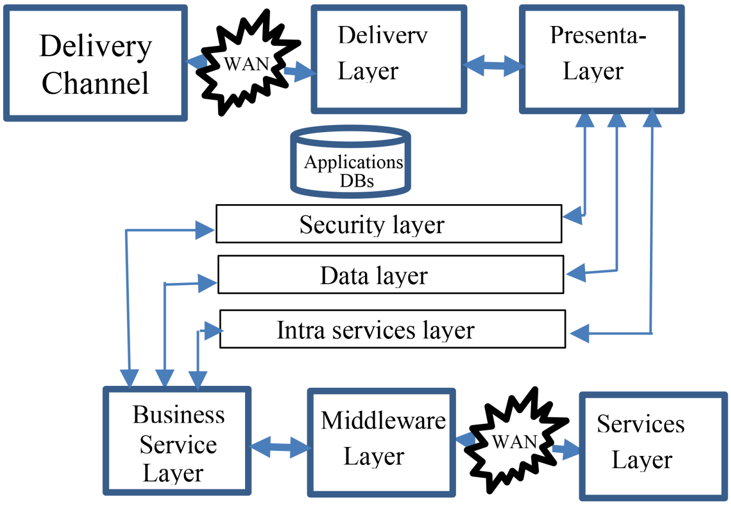

**Figure 5.** System amalgamation.

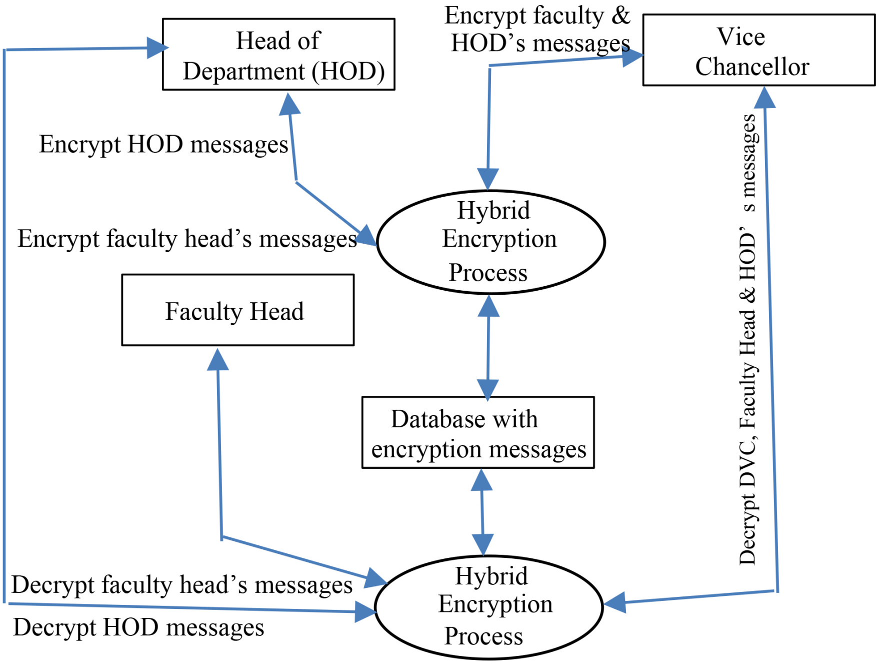
Head of Department (HOD)
Encrypt faculty & HOD's messages
Vice Chancellor
Encrypt HOD messages
Encrypt faculty head's messages
Hybrid Encryption Process
Faculty Head
Database with encryption messages
Decrypt DVC, Faculty Head & HOD' s messages
Decrypt faculty head's messages
Decrypt HOD messages
Hybrid Encryption Process

**Figure 6.** Data flow diagram of a university e-administration system.

### 3.7. Cryptography Model for Securing the System

The model for securing the proposed system combines the authentication criteria presented in Rijndael-Advanced Encryption Standard (AES), Lattice-based cryptography (LBC) and Secure Hash Algorithm (SHA512) cryptography techniques. The record will be encrypted prior to its commitment to the database via a double encryption method. The encryption will be based on the AES algorithm whose output will form the input to the LBC algorithm to obtain the final output to be stored in the database. For every record in the database, there is a unique passphrase that is encrypted using the record. The encryption is based on the SHA512 algorithm which is a secured hash algorithm for the enactment of password storage policy alongside randomly generated salting techniques. A hybrid AES encryption process with a secret key 1 will be used for encrypting the information and re-encrypting the encrypted information using an LBC algorithm with a secret key 2 as shown in Figure 7. The LBC algorithm is first encrypted as a *key* 1 based on the steps presented in [83]. The information stored in the database is further decrypted using the decryption process for LBC with a Secret Key 2 to decrypt the data for authorized users only before decrypting the output of the LBC decryption using the decryption algorithm for AES with secret key 1 as shown in Figure 7.

The hashing technique involves the storage of users' passwords and authorization in the form of a digital fingerprint of a fixed length in the database. The hashing operation requires a one-way process of encryption such that the password or authorization code cannot be decrypted by the system administrator or whoever has access to the database. Hashing the user password requires the SHA512 algorithm in combination with a random number as shown in Figure 8.

The authentication of user access to the database will be based on comparing the hashes stored in the database and user supplied as shown in Figure 9. The SHA-512 hashing algorithm is in the stages presented in (Rossi, 2020). The input formatting stage involves bits padding where the input message is taken and

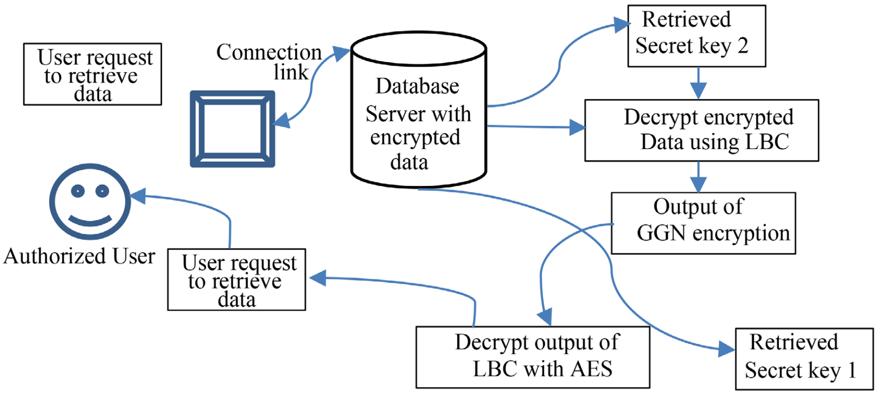
User request to retrieve data
Connection link
Database Server with encrypted data
Retrieved Secret key 2
Decrypt encrypted Data using LBC
Output of GGN encryption
Authorized User
User request to retrieve data
Decrypt output of LBC with AES
Retrieved Secret key 1

Figure 7. Proposed architecture of the decryption process.

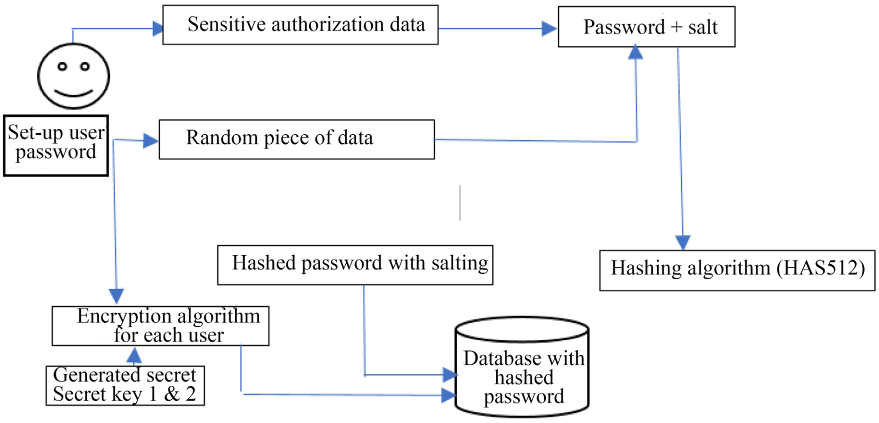
Sensitive authorization data
Password + salt
Set-up user password
Random piece of data
Hashed password with salting
Hashing algorithm (HAS512)
Encryption algorithm for each user
Generated secret Secret key 1 & 2
Database with hashed password

Figure 8. Proposed architecture of the hashing and salting process.

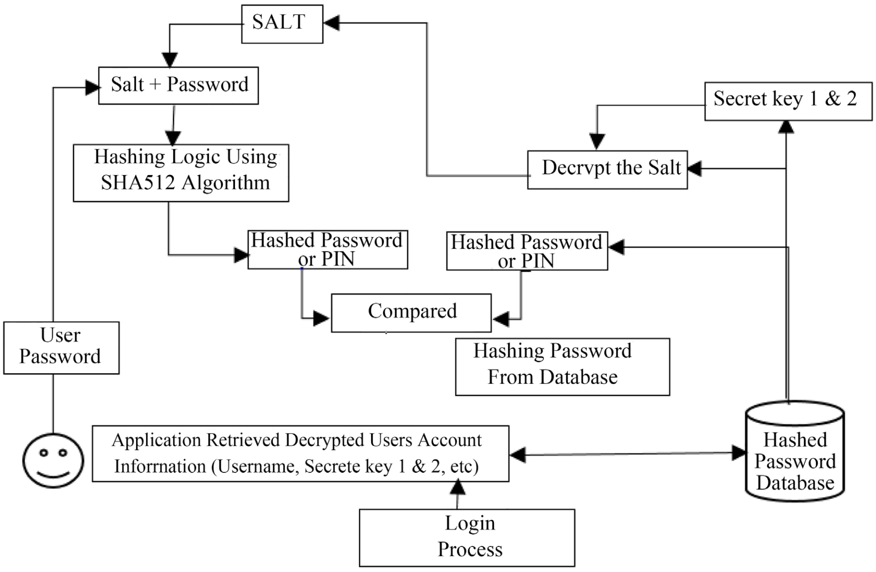
SALT
Salt + Password
Secret key 1 & 2
Hashing Logic Using SHA512 Algorithm
Decrvpt the Salt
Hashed Password or PIN
Hashed Password or PIN
Compared
User Password
Hashing Password From Database
Application Retrieved Decrypted Users Account Inforrnation (Username, Secrete key 1 & 2, etc)
Hashed Password Database
Login Process

**Figure 9.** User authentication system.

some padding bits are appended to it in order to get the desired length. This is followed by size padding in which the size of the original message given to the algorithm is appended and represented in 128 bits. Following is the hash buffer initialization in which each block of 1024 bits from the message is processed using the result from the previous block. In some cases, to overcome the inability to use the result from previous processing, a default value is used for the first block in order to start off the process.

The next stage is Message Processing which is done upon the formatted input by taking one block of 1024 bits with the result from the previous stage. This stage consists of several circles of operations in which each circle contains one Word, the output of the previous round, and an SHA-512 constant. The first round lacks a previous round and hence it uses the final output from the previous message processing phase of the previous block of 1024 bits. For the first round of the first block of the formatted input, the initial vector is used. SHA-512 constants represent pre-known values used for each round in the message processing phase. Next is the output phase in which the intermediate results are all used for each block for processing the next block. Upon the conclusion of the last 1024-bit block processing, there is the final result of the SHA-512 algorithm for the original message. The SHA-512 algorithm presents a group of SHA-2 hashing algorithms such as SHA-256 and SHA-384 that is very similar to SHA-512.

A combination of the systems presented above led to a hybrid system that combines both encryption and hashing techniques to achieve higher reliability and security of the content of the database for the proposed e-administration system as shown in **Figure 10**. The system adopts the Goldreich, Goldwasser, and Halevi (GGH) algorithm for message encryption. The algorithm relies on the Closest Vector Problem (CVP) which is a one-way function for implementing

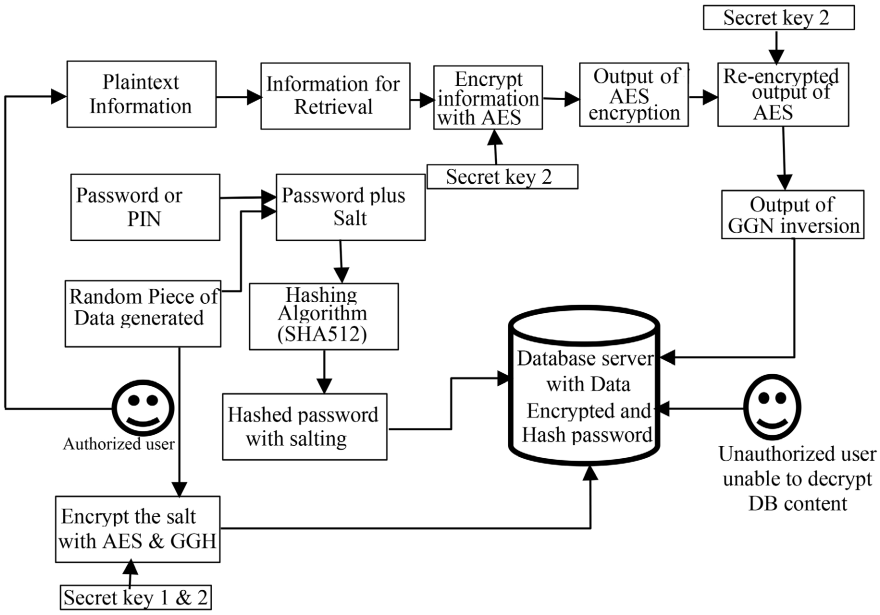
Secret key 2
Plaintext Information
Information for Retrieval
Encrypt information with AES
Output of AES encryption
Re-encrypted output of AES
Secret key 2
Password or PIN
Password plus Salt
Output of GGN inversion
Random Piece of Data generated
Hashing Algorithm (SHA512)
Database server with Data Encrypted and Hash password
Authorized user
Hashed password with salting
Unauthorized user unable to decrypt DB content
Encrypt the salt with AES & GGH
Secret key 1 & 2

**Figure 10.** The identity-based cryptography platform for the system.

a public key cipher by leveraging on the effort of lattice reduction [84]. For the enforcement of the salient security features, the GGH algorithm uses a public key that hinges on the power of the lattice to obtain a trapdoor function. The message is encoded as a lattice vector via the public basis, followed by the addition of a small error vector. During the implementation of the decryption process, the private basis is also used to efficiently compute the closest lattice vector using the parameters presented in **Table 1**.

The matrices, $R$ and $B$ are the private key and the public key respectively. $R$ serves a good basis for the reducible lattice (Λ), while $B$ encompasses a depraved foundation for irreducible Λ, such that $\left(\Lambda \subset Z^n\right)$ and the foundation contains the short vector. An arbitrary matrix that consists of short vectors will be used to generate $R$ as follows:

$$R = K \cdot \tau + E \tag{1}$$

$K$ is an integer with a medium size exceeding 1, $\tau$ is the $n * n$ identity matrix and $E$ represents a random matrix of short vectors. In addition, multiplying $R$ by a random uni-modular matrix ($U$) gives the public matrix $B$ as follows:

$$B = U \cdot R \tag{2}$$

Given that $m$, $e$, and $c$ represent the message, error, and cipher matrices respectively, then the encryption process on the tree is presented as follows:

$$c = m \cdot B + e \tag{3}$$

The decryption process is performed thus:

$$\text{round}\left(c \cdot R - 1\right) = \text{round}\left(\left(m \cdot B + e\right) \cdot R - 1\right) =$$

$$m \cdot U \cdot R \cdot R - 1 + \text{round}\left(e \cdot R - 1\right) = m \cdot U + \text{round}\left(e \cdot R - 1\right) \tag{4}$$

$$= m \cdot U, U - 1 \tag{5}$$

Table 1. GGH parameters [85].

| Parameter | Description | Knowledge |
|---|---|---|
| $n$ | Dimension | Public |
| $\sigma$ | Security Parameter | Public |
| $R$ | $N^*$ $n$ Integral Matrix | Private |
| $B$ | $N^*$ $n$ Integral Matrix | Public |

### 3.8. Generation

The key generation is based on the primitive root theory [86] which assures that for any large prime number (*p*), there exists an integer number $\left(\alpha | 1 \le \alpha \le p-1\right)$, such that all remainders are distinct. The integer number $\left(\alpha^t \left(\text{mod } p\right) | 1 \le t \le p-1\right)$ are distinct. The integer number (*α*) is known as a primitive root modulo (*p*). Preceding the selection of *p* is the computation of a random parameter $\left(d | 1 < d < p-2\right)$. Hence, $\beta = \alpha^d \left(\text{mod } p\right)$, such that the encryption key $\left(p, \alpha, \beta\right)$ Is the public key that will be used to encrypt the message. *d* is also used to compute *β* which is necessary for decryption.

### 3.9. The Encryption Standard

Given that Ann needs to send a message, M to Bale. The encryption process involves Ann obtaining the public key $\left(p, \alpha, \beta\right)$ from Bale, converting the message (*M*) into a numerical representation as a set of integer numbers $\left(m_1, m_2 \ldots | 1 \le m \le p-1\right)$. These numbers will be encrypted one by one. Ann will then select a random integer number (*k*), that must be secret, compute the public key $r = \alpha^k \left(\text{mod } p\right)$ and encrypt the message (*M*) to the ciphertext (*C*) such that $\left(c_i = m_i * \beta^k \left(\text{mod } p\right)\right)$, where (*C*) represents the set of every $\left(c_i | 0 < i < |M|\right)$. Finally, Ann sends the ciphertext (*C*) to Bale together with the public key (*r*).

### 3.10. Hashing and Salting Algorithm

The key fact of a mono-directional hash function is that any encrypted text cannot be decrypted. Choosing the non-invertible matrix from the cipher is therefore required. Firstly, a non-invertible matrix is multiplied by a plaintext as a column vector with modular value to obtain the hash value *H*. The sender of the message computes the hash value or message digest by using the model and then sends the message and the hash value to the receiver who does an equivalent computation to achieve a message hash value. Lastly, the receiver weighs between the message digest from the sender and the obtained hash value as follows:

$$H\left(V\right) = V \cdot R \text{ mod } N \tag{6}$$

*R* is a non-invertible and irreversible matrix used to generate a hash value. $d = |R|$ Is the determinant of R and does not relatively prime to N which implies the non-existence of $R^{-1}$ and $(H(V))^{-1}$.

### 3.11. Encryption Model Description

For the decryption process, Bale must use the ciphertext (*C*) and the public key $r = \alpha^k \left(\bmod p\right)$. The decryption process goes with the computation of the shared key via a combination of the private number of Bale (*d*) and the random number of Ann (*k*), such that $\left(\left(\alpha^k\right)^{p-1-d} = \left(\alpha^k\right)^{-d}\right)$. This is followed by the decryption of the ciphertext (*C*) such that $\left(m_i = \left(\alpha^k\right)^{-d} * c_i \bmod p\right)$, where $\left(m_i\right)$ is the plaintext part corresponding to the ciphertext part $\left(c_i\right)$. The message (*M*) that is sent by Ann can then be read by Bale after combining all plaintext parts $m_i$.

## 4. Conclusion

The paper presents the design of an e-administration platform and its cryptography-based security model. The service identification unit of the platform is designed to prioritize e-services in an iterative pattern, guided by both transaction criteria and the perceptions of stakeholders. Its identification system unit comprises information gathering, transaction processing, regulatory compliance, quality assurance, evaluation, and assessment sub-systems and will guaranteed organized and simplified procedures in efficient, timely, secured, achievable, and cost-saving manners. The CPR unit focuses on systematic learning and complete re-formatting of activities and events across units and departments. It will guarantee effectiveness and optimality in service delivery by the management, employees, and the immediate community. The services platform unit is a service-oriented and web-based interface that comprises features like business functionality, and extensible support to multiple access devices such as desktop computers and so on. It promotes interoperability between the institution-based portals and integrates all departmental service-oriented applications and websites of all existing units for e-administration contents. The amalgamation unit will be useful for connecting several discrete and independent operational units to attain a solitary source of information for all the subsystems as well as give a running platform or start point for all the services provided by the various units. The deployment model will optimize the gains and serves as a catalyst for increased integration of the various units. It will also provide centralized control, one-time unified infrastructure, the basis for the management team to concentrate on their core business and duties, centralized control, and a unified business model among all units and departments. The security model for the proposed system combines the authentication criteria presented in AES, LBC, and Secure Hash Algorithm (SHA512) cryptography techniques. The encryption will be based on the AES algorithm whose output will form the input to the LBC algorithm to obtain the final output to be stored in the database. The implementation of the framework is ongoing with Python, Visual Studio 2015 (Integrated Development Environment), Microsoft.Net Framework 4.0 and Java providing the programming terrains while Microsoft SQL server 2008 express edition provides the platform for the creation and management of the system databases.

The programming trains will adopt Java Database Connection (JDBC) for communication with the resources at the database level. Suitable data on the feasibility of the proposed system will form a very substantial part of the implementation stage.

## Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

## References

[1] Lamidi, K.O. (2015) Theories of Public Administration: An Anthology of Essays. *International Journal of Politics and Good Governance*, **6**, 1-35.

[2] White, D.L. (1926) Introduction to the Study of Public Administration. Macmillian Company, New York.

[3] Agulhon, S. and Mueller, T.M. (2022) Between Fairness and Efficiency: Testing Wilson's Theory of Public Administration. *Journal of the History of Economic Though*, SocArXiv. https://doi.org/10.31219/osf.io/nzjsv

[4] Zahran, I. (2012) The Role of School Administration in the Face of Crisis of Values among Second Grade Primary Students in Light of the Twentieth Century Variables. *The Scientific Conference*, Zagreb, 29-30 May 2012, 15-17.

[5] Faulkner, C. (2015) Women's Experiences of Principalship in Two South African High Schools in Multiply Deprived Rural Areas: A Life History Approach. *Educational Management Administration & Leadership*, **43**, 418-432. https://doi.org/10.1177/1741143215570306

[6] Hulpia, H., Devos, G. and Van Keer, H. (2009) The Influence of Distributed Leadership on Teachers' Organizational Loyalty. *Journal of Educational Research*, **103**, 40-52. https://doi.org/10.1080/00220670903231201

[7] National Universities Commission (NUC) (2011) Theories and Practice of Public Administration.
https://www.researchgate.net/publication/277621342_The_Role_Of_The_National_Universities_Commission_Nuc_In_The_Development_Of_University_Education_In_Nigeria_Reflections_And_Projections

[8] Ajayi, I.A. and Akindutire, I.O. (2017) The Unresolved Issues of Quality Assurance in Nigerian Universities. *Journal of Sociology and Education in Africa*, **6**, 43-50.

[9] Al-Sharari, K. (2008) The Role of Principals in the Face of the Phenomenon of Violence among High School Students. Yarmouk University, Irbid.

[10] Al-Shehab, S. (2013) The Effective Role of the Principals to Curb the Phenomenon of Willingness to Commit Suicide from the Perspective of Students. *College of Basic Education Research Journal*, **12**, 25-51.

[11] Enaam, K.A. (2019) Electronic Learning and its Benefits in Education. *EURASIA Journal of Mathematics, Science and Technology Education*, **15**, 1-8.

[12] Al-Arishi, M (2008) Possibility of Applying the Electronics Management in the General Directorate of Education at Holy Makkah. Umm Al-Qura University, Mecca.

[13] Abu, A.K. and Al Nemry, D. (2013) The Level of Applying Electronic Administration at Yarmouk University as Perceived by Administrators and Faculty Members. *The Jordanian Journal of Educational Sciences*, **9**, 199-220.

[14] Khlouf, E. (2010) The Reality of Electronic Management in Government Schools in the WEST from the Point of View of Managers and Directors. An-Najah National University, Nablus.

[15] Almer, E. (2007) The Requirement of Human Resource Development for Application of Electronic Management. Naif Arab University for Security Sciences, Riyadh.

[16] Amoneh, A.Y. (2009) E-HRM Regular Palestinian Universities Unpublished. Islamic University, Kushtia.

[17] Al Dhowan, A. (2008) The Role of the Administrative Development Administration in the Application of E-Administration. King Saud University, Riyadh.

[18] El-Sherif, H. (2014). Applications of Management Theory. https://www.researchgate.net/publication/271530940_Applications_of_Management_Theory

[19] Shivetts, C. (2011) E-Learning and Blended Learning: The Importance of the Learner: A Research Literature Review. *International Journal on E-Learning*, **10**, 331-337.

[20] Al-Furaih, S. and Al-Kanderi, A. (2014) Using Technology Acceptance Model (TAM) to Investigate the Effectiveness of a Learning Management System in University Teaching. *Journal of Educational and Psychological Sciences*, **15**, 111-138. https://doi.org/10.12785/jeps/150104

[21] Liu, S.-H., Liao, H.-L. and Peng, C.-J. (2005) Applying the Technology Acceptance Model and Flow Theory to Online ELearning Users' Acceptance Behavior. *Issues on Information Systems*, **6**, 175-181.

[22] Almaghrebi, A. (2004) Requirements of Applying E-Administration Service Delivery, Trends towards Workers: An Empirical Study on the Damietta Port. A Paper Introduced to the Twentieth Annual Scientific Conference, The Service Industry in the Arab Future Vision. Mansoura University, Mansoura.

[23] Mellivell, L. (2007) British University E-Management in Hong Kong Setting. *Higher Education in Hong Kong*, **6**, 32-77.

[24] Jackson, H. (2006) Perceived Technological Processes in Texas Technical University. *Higher Education*, **9**, 292-329.

[25] Abdulnaser, M. and Quraishi, M. (2011) The Contribution of E-Governance in the Development of the Administrative Work of Higher Education Institutions: A Case Study of Faculty of Science and Technology, University of-Biskra Algeria. Elbahith Review, Kasdi Merbah University of Ouargla-Algeria, **9**, 87-100.

[26] Allami, A. (2008) Reality Using Computer Applications in the Areas of School Management. Gulf University, Sanad.

[27] Felck, C. (2010) Using Computers in Croatia National University Divisions. *Journal of Research in Higher Education*, **2**, 111-169.

[28] Alhasanat, S, (2011) Obstacles of Applying Electronic Management in the Palestinian Universities. Arabic Studies and Research Institute, Cairo.

[29] Gadiesh, O. and Liglbeert, J. (2001) Transforming Corne-Office Strategy in to Frontline Action. *Harvard Business Review*, **79**, 72-79.

[30] Alsahi, A. (2006) Imagine a Proposal to Employ Educational Technology to Develop Educational Programs to Develop Open Education Programs. Institute of Seas and Arabic Studies, Alexandria.

[31] Alomari, S. (2003) Administrative Requirements Application Security Management. Naif Arab University for Security Sciences, Riyadh.

[32] Almoghirah, A. (2010) Obstacles to the Application of E-Administration in the

Procedures of Admistrative Work from the Standpoint of the Ministry of Interiors Staff. Naif Arab University for Security Sciences, Riyadh.

[33] Hammawa, M.B., Owolabi, O., Abdulganiyu, A. and Amit, M. (2019) Building Information Security Using New Expanded RSA Cryptosystem. *International Journal of Research in Advanced Engineering and Technology*, **5**, 65-68.

[34] Sendi, H. (2002) E-Management in the Arab World between Reality and Aspiration. A Paper Introduced to E-Government Conference. Sultanate of Oman, Muscat.

[35] Seresht, H. (2009) E-Management: Barriers and Challenges in Iran. Dollamed Tabateebe University, Iran.

[36] Taybe, A. and Al-Qasimi, M. (2013) Diagnosis of Obstacles of the Application Electronic Management Models in Educational Institutions: Exploratory Study of the Views of Staff in Anumber of Private Schools in the City of Mosul. *Tanmeah Alrafdayn Journal*, **114**, 10-29.

[37] Bkhesh, F. (2007) E-Management in Colleges of Education for Girls in Saudi Arabia in Light of Contemporary Transformations. Umm Al-Qura University, Mecca.

[38] Lowery, B.S., Hardin, C.D. and Sinclair, S. (2001) Social Influence Effects on Automatic Racial Prejudice. *Journal of Personality and Social Psychology*, **81**, 842-855. https://doi.org/10.1037/0022-3514.81.5.842

[39] World Bank (2017) World Bank Development Report. https://www.worldbank.org/en/publication/wdr2017

[40] Yildiz, M.A. (2017) Emotion Regulation Strategies as Predictors of Internet Addiction and Smartphone Addiction in Adolescents. *Journal of Educational Sciences & Psychology*, **7**, 66-78.

[41] Seifert, J.W. and Bonham, G.M. (2003) The Transformative Potential of E-Government in Transitional Democracies. https://www.yumpu.com/en/document/view/18924147/the-transformative-potential-of-e-government-in-transitional-

[42] Gil-García, J.R. and Pardo, T.A. (2005) E-Government Success Factors: Mapping Practical Tools to Theoretical Foundations. *Government Information Quarterly*, **22**, 187-216. https://doi.org/10.1016/j.giq.2005.02.001

[43] Colesca, S.E. (2009) Understanding Trust in E-Government. *Engineering Economics*, **3**, 7-15.

[44] Fakhri, M., Ekawati, A.W., Nasrullah, B.A., Ating, Y. and Anik, M.H. (2019) Effect of Probiotics on Survival Rate and Growth Performance of *Clarias gariepinus*. *Journal of Nature Environment and Pollution Technology*, **18**, 313-316.

[45] Almarabeh, T. and Abu Ali, A. (2010) A General Framework for E-Government: Definition Maturity Challenges, Opportunities, and Success. *European Journal of Scientific Research*, **39**, 29-42.

[46] Peter, A., Kronberg, M., Trei, W. And Katzenbeisser, S. (2012) Additively Homomorphic Encryption with a Double Decryption Mechanism, Revisited. In: Gollmann, D. and Freiling, F.C., Eds., *Information Security. ISC* 2012. *Lecture Notes in Computer Science*, Vol. 7483, Springer, Berlin, 242-257. https://doi.org/10.1007/978-3-642-33383-5_15

[47] Das S., Balmiki A.K. and Mazumdar, K. (2022) A Review on AI-ML Based Cyber-Physical Systems Security for Industry 4.0. In: Banerjee, J.S., Bhattacharyya, S., Obaid, A.J. and Yeh, W.-C., Eds, *Intelligent Cyber-Physical Systems Security for Industry* 4.0, Chapman and Hall/CRC, New York, 203-216. https://doi.org/10.1201/9781003241348-11

[48] Luciano, D. and Prichett, G. (1987) Cryptology: From Caesar Ciphers to Public-Key Cryptosystems. *The College Mathematics Journal*, **18**, 2-17. https://doi.org/10.1080/07468342.1987.11973000

[49] Jafar, Q. (2019) Data Encryption Using Hash Function for Generating Secret Keys (DEH). AUS Revista, 26. https://www.researchgate.net/publication/338753082_Data_Encryption_Using_hash_Function_For_Generating_Secret_KeysDEH

[50] Stallings, W. (2005) Cryptography and Network Security Principles and Practices. 4th Edition, Prentice Hall, Hoboken. http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014-1/Stallings/Stallings_Cryptography_and_Network_Security.pdf" www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014-1/Stallings/Stallings_Cryptography_and_Network_S

[51] Zimmermann, V., Henhapl, B., Gerber, N. and Enzmann, M. (2017) Promoting Secure Email Communication and Authentication. *Proceedings of International Conference*: *Mensch & Computer* 2017, Dresden, 2-5 September 2017.

[52] Katz, J. and Lindell, Y. (2014) Introduction to Modern Cryptography. 2nd Edition, Chapman & Hall/CRC, New York. https://doi.org/10.1201/b17668

[53] Diaa, S., Abd, E., Hatem, M.A.K. and Mohiy, M.H. (2010), Evaluating the Performance of Symmetric Encryption Algorithms. *International Journal of Network Security*, **10**, 216-222.

[54] Agrawal, M. and Mishra, P. (2012) A Comparative Survey on Symmetric Key Encryption Techniques. *International Journal on Computer Science and Engineering*, **4**, 877-882.

[55] Chandra, S., Bidisha, M., Safikul, A. and Siddhartha, B. (2015) Content Based Double Encryption Algorithm Using Symmetric Key Cryptography. *Procedia Computer Science*, **57**, 1228-1234. https://doi.org/10.1016/j.procs.2015.07.420

[56] Daemen, J. and Rijmen, V. (2002) The Design of Rijndael. Springer, Berlin. https://doi.org/10.1007/978-3-662-04722-4

[57] Rivest, R.L, Shamir, A. and Adleman, L. (1978) A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communication ACM*, **21**, 120-126. http://portal.acm.org/citation.cfm?doid=359340.359342 https://doi.org/10.1145/359340.359342

[58] Al Hasib, A., Ahsan, A. and Haque, M. (2008) A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography. 2008 3*rd International Conference on Convergence and Hybrid Information Technology*, Busan, 11-13 November 2008, 505-510. https://doi.org/10.1109/ICCIT.2008.179

[59] Jha, R. and Saini, A.K. (2011) A Comparative Analysis & Enhancement of NTRU Algorithm for Network Security and Performance Improvement. 2011 *International Conference on Communication Systems and Network Technologies*, Katra, 3-5 June 2011, 80-84. https://doi.org/10.1109/CSNT.2011.23

[60] Bakhtiari, M., Zainal, A., Bakhtiari, S. and Kutty, H. (2015) Lightweight Symmetric Encryption Algorithm in Big Data. *International Journal of Advances in Soft Computing and Its Applications*, **7**, 46-55.

[61] Eastlake, D. and Jones, P. (2001) US Secure Hash Algorithm 1 (SHA1). IETF RFC3174. https://doi.org/10.17487/rfc3174

[62] Schneier, B. (2005) Applied Cryptography. John Wiley and Sons, Inc., Hoboken.

[63] Alallayah, K.M., Amin W.F.M. and Hamami, A.H. (2010) Attack and Construction

of Simulator for Some of Cipher Systems Using Neuro-Identifier. *International Arab Journal of Information Technology*, **7**, 365-372.

[64] Smirnoff, P. and Turner, D. (2019) Symmetric Key Encryption—Why, Where and How It's Used in Banking. https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking

[65] Bellare, M. and Namprempre, C. (2000) Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. In: Okamoto, T., Ed., *Advances in Cryptology—ASIACRYPT* 2000. *ASIACRYPT* 2000. *Lecture Notes in Computer Science*, Vol. 1976, Springer, Berlin, 531-545. https://doi.org/10.1007/3-540-44448-3_41

[66] Georgiana, M. and Marius, V (2013) A Hybrid Approach of System Security for Small and Medium Enterprises: Combining Different Cryptography Techniques. *Proceeding of the* 2013 *Federated Conference on Computer Science and Information Systems*, Krakow, 8-11 September 2013, 659-662.

[67] Somani, U., Lakhani, K. and Mundra M. (2010) Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing. 2010 *First International Conference On Parallel*, *Distributed and Grid Computing* (*PDGC* 2010), Solan, 28-30 October 2010, 211-216. https://doi.org/10.1109/PDGC.2010.5679895

[68] Rewagad, P.P. and Pawar, Y. (2013) Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. 2013 *International Conference on Communication Systems and Network Technologies*, Gwalior, 6-8 April 2013, 437-439. https://doi.org/10.1109/CSNT.2013.97

[69] Rajak, S. and Verma, A. (2012) Secure Data Storage in the Cloud Using Digital Signature Mechanism. *International Journal of Electronics Communication and Computer Engineering*, **3**, 763-766.

[70] Le-Khac, N.A., Jacobs, D., Nijhoff, J., Bertens, K. and Choo, K.-K.R. (2020) Smart Vehicle Forensics: Challenges and Case Study. *Future Generation Computer Systems*, **109**, 500-510. https://doi.org/10.1016/j.future.2018.05.081

[71] Sivasakthi, T. and Prabakaran, N. (2014) Applying Digital Signature with Encryption Algorithm of User Authentication for Data Security in Cloud Computing. *International Journal of Innovative Research in Computer and Communication Engineering*, **2**, 456-459.

[72] Suguna, M., Prakash, D. and Cynthia. J. (2018) Secure Data Access Privacy Preserving Using Cloud Services. *International Journal of Recent Technology and Engineering*, **7**, 321-324.

[73] Nair, N.K. and Navin, K.S. (2015) An Efficient Group Authentication Mechanism Supporting Key Confidentiality, Key Freshness and Key Authentication in Cloud Computing. 2015 *International Conference on Computation of Power*, *Energy*, *Information and Communication* (*ICCPEIC*), Melmaruvathur, 22-23 April 2015, 288-292. https://doi.org/10.1109/ICCPEIC.2015.7259477

[74] Mathews, C. (2016) Cloud Data Integrity Using Password Based Digital Signatures. *International Journal of Computer Science and Information Technologies*, **7**, 101-103.

[75] Abdulkarim, A.I. and Boukari, S. (2017) An Enhanced Cloud Based Security System Using RSA as Digital Signature and Image Steganography. *International Journal of Engineering Research*, **8**, 16-21.

[76] Harba, H.S. (2015) Design and Implementation of Multilevel Secure Database on

Website. *Journal of Information Engineering and Applications*, **5**, 11-18.

[77] Ming, Y. and Wang, E. (2019) Identity-Based Encryption with Filtered Equality Test for Smart City Applications. *Sensors*, **19**, Article No. 3046. https://doi.org/10.3390/s19143046

[78] El Bouchti, K., Ziti, S., Omary, F. and Kharmoum, N. (2019) A New Database Encryption Model Based on Encryption Classes. *Journal of Computer Science*, **15**, 844-854. https://doi.org/10.3844/jcssp.2019.844.854

[79] Roy, A. and Karfoma, S. (2013) Coupling and Cohesion Analysis for Implementation of Authentication in E-Governance. *ACEEE Conference Proceedings Series*, **2**, 544-554.

[80] Daddala, B. (2017) Design and Implementation of a Customized Encryption Algorithm for Authentication and Secure Communication between Devices. A Thesis Submitted to the Graduate Faculty as Partial Fulfillment of the Requirements for the Master of Science Degree in Engineering. The University of Toledo, Toledo.

[81] Hua, H., Liu, Y., Wang, Y., Chang, D. and Len, Q. (2018) Visual Cryptography Based Multilevel Protection Scheme for Visualization of Network Security Situation. *Procedia Computer Science*, **131**, 204-212. https://doi.org/10.1016/j.procs.2018.04.204

[82] Pratiksha, S. and Kapoor, V. (2016) A Proposed Novel Architecture for Information Hiding in Image Steganography by Using Genetic Algorithm and Cryptography. *Procedia Computer Science*, **87**, 61-66. https://doi.org/10.1016/j.procs.2016.05.127

[83] Rossi, M. (2020) Extended Security of Lattice-Based Cryptography. Cryptography and Security [cs.CR]. Équipe CASCADE, Department d'Informatique de l'ENS de Paris; Université PSL, Paris.

[84] Nguyen, P. (1999) Cryptanalysis of the Goldreich-Goldwasser-Halevi Cryptosystem from Crypto '97. In: Wiener, M., Ed., *Advances in Cryptology—CRYPTO'* 99. *CRYPTO* 1999. *Lecture Notes in Computer Science*, Vol. 1666, Springer, Berlin, 288-304. https://doi.org/10.1007/3-540-48405-1_18

[85] Massoud, S.B.S. (2018) The GGH Public Key Cryptosystem via Octonion Algebra and Polynomial Rings. *International Journal of Information Technology Security*, **10**, 77-86.

[86] Mohit, P. and Biswas, G.P. (2015) Design of El Gamal PKC for Encryption of Large Messages. 2015 2*nd International Conference on Computing for Sustainable Global Development* (*INDIACom*), New Delhi, 11-13 March 2015, 699-703.