Research Output Journal of Engineering and Scientific Research 4(1): 60-70, 2025

ROJESR Publications Online ISSN: 1115-9790

https://rojournals.org/roj-engineering-and-scientific-research/ Print ISSN: 1115-6155

https://doi.org/10.59298/ROJESR/2025/4.1.6070

Survey of Cryptography models for Security of Computer-based Integrated School Information Management System

[1]Chinenye P. Ikeagwu; [2]Virginia E. Ejiofor; [3]Orji Everistus Eze and [4]Godspower Akawuku

[1,2,4]Department of Computer Science, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria
[3]Department of Computer Science Federal Polytechnic Ohodo, Enugu, State, Nigeria
Email: Cp.ikeagwu@gmail.com

ABSTRACT

This survey examines cryptography models for securing computer-based integrated school information management systems. The study reviews symmetric and asymmetric key cryptography, hash functions, and digital signatures. Cryptography techniques, including encryption, decryption, key exchange, and digital certificates, are also discussed. The application of these models and techniques to school information management systems is explored, highlighting benefits such as confidentiality, integrity, and authenticity. Thus, the work adopted systematic literature review (SLR) methodology: extensively on books, e-books, internet, compendium, journals and research papers published in symposia, seminars and conferences organized in and beyond Nigeria were exploded. Nevertheless, challenges abound in critical areas, including key management, performance, user education, and regulatory compliance, are also identified. This survey provides a comprehensive overview of cryptography models and their potential to enhance the security of school information management systems.

Keywords: Cryptography, School Information Management System, Security, Confidentiality, Integrity, Authenticity.

Conceptual Framework

This study adopts and derives its theoretical review electronically from peer reviews, grey literature, and the researcher's current state of knowledge on the topic. Thus, the work focused extensively on books, e-books, internet, compendium, journals and research papers published in symposia, seminars and conferences organized in and beyond Nigeria. The reviews outline various functional areas and the different information technology tools used for e-governance, e-learning among others. It further gives details of the account of the research carried out on the development of cryptographic model for the security of computer based integrated school information management system. It will exceptionally help in the planning of research and investigations for the proposed work to a greater level.

Concept of Cryptography

Cryptography is the study and implementation of processes, which manipulate data for the purpose of hiding and authenticating information. According to [1], Cryptography is the art and science of protecting stored and transmitted information from undesirable individuals by converting it into a form non-recognizable by its attackers. In other words, Cryptography is the study of art and science of preparing protected and secure data communication. The word cryptography is derived from the two Greek words; "kryptos" means "secret or hidden" and "graphos" means "to write" [2]. Generally, cryptography is a technology whose use and implementation is rapidly increasing. This is because it is a very good method of ensuring information safety. Through cryptography, any piece of information can be encrypted or written in such a manner that it can be very difficult for another person to read if he or she is not able to decrypt it. In addition, Cryptography is keeping information in secret or hidden. In other words, cryptography is a process in which data are stored securely on cloud and transmit it in unreadable form so only authorized person can access the data [3]. There are a number of features associated with cryptography. One is confidentiality which basically means that we need to be sure that nobody will see our information as it travels across a network. Authentication and access control is also another capability provided by cryptography. Some other capabilities provided by cryptography are non-repudiation and integrity [4]. Data cryptography mainly is the scrambling of the content of data which may be in form of text, image, audio, video and so forth to make the data unreadable, invisible or unintelligible during transition or storage stage. The main goal of cryptography is securing data from unauthorized users. It is made up of encryption which can be reversed and refer to as data decryption. In modern days, cryptography is no longer limited to securing sensitive military information but recognized as one of the major components of the security policy of any organization and considered industry standard for providing information security, trust, controlling access to resources, and electronic financial transactions. A system or product that provides encryption and decryption is called cryptosystem. Cryptosystem uses an encryption algorithm which determines how simple or complex the encryption process will be, the necessary two (2) software component, and the key (usually a long string of bits), which works with the algorithm to encrypt and decrypt the data. Encryption is a process of transforming information that usually are in plaintext using an algorithm (known as cipher) to make it unreadable to anyone except those who have the special knowledge known as the key [5]. The output from the process is known as cipher text. According to [6], Encryption is the technique where a series of data is converted into a cipher text, making it difficult for any arbitrary user to read it in plain text. It is further observed in encryption process that cryptography uses concealed messages, codes and codebooks. In conceal messages, plaintext is written with invisible ink. This invisible ink is usually lemon or orange juice. When it is dry, it looks like a plain paper, but if you put this paper in sunlight or pressed by iron, the message is prominently shown on that paper. But now this type of technique is not used for encryption because it is easily interpreted. There is preset order codebook made, in which, numbers, symbols or letters, rearranged by another number or letter, are used and a code message is written, which is secured for small time period. Cryptography also includes the use of computerized encryption to protect communication [2]. It is the most significant way of ensuring that highly sensitive information is not altered and its integrity remains unaffected [2]. In the reverse, the process to make the information readable is decryption. Cryptography is a technology whose use and implementation is rapidly increasing. This is because it is a very good method of ensuring information safety. Through cryptography, any piece of information can be encrypted or written in such a manner that it can be very difficult for another person to read if he or she is not able to decrypt it [7]; [8]. [4] noted that the original message or text before going to any process is called plaintext or clear text. The process of changing plaintext into secret form is called encryption. Once the original text has been encrypted, the resultant text is known as cipher text or cryptogram. The process of converting cipher text into plaintext is known as decryption [2]. Mostly nowadays, in encryption process, some mathematical algorithms are used. Basically, encryption algorithm is the set of instructions that have particular method of encrypting plaintext into cipher text. Cryptography plays an important role in todays and future's confidential data communication. For example, communications over telephone lines including faxes and e-mail messages, financial transactions, medical histories, e-banking and even other types of important information need secure communication medium. Sometimes, the medium is hacked by intruders and gets all of your information. Therefore, cryptographic applications provide the secure communication medium to transfer your data reliably, so that if any one tries to hack data, then it is not useful to him because the data is in encrypted form. Cryptography is one of the tools, which ensures more privacy. The ability to encrypt data, communications and other information, gives individuals, the power to restore personal privacy. Cryptography protects the world's banking systems as well, which is the requirement of today's world. Many banks and other financial institutions conduct their business over open switched networks like Internet. Without the ability to protect bank transactions and communications, criminals could interfere with the transactions and rob banks without a trace [2].

Types of Cryptographic Algorithms

There are two types of Cryptography algorithms such as Symmetric and Asymmetric Encryptions. Symmetric algorithms is one of the cryptography algorithms that uses secret key for data encryption and decryption. Examples are: AES, DES, IDEA, TDES and Blowfish. There are also asymmetric algorithms which uses two keys: public key for data encryption and private key for data decryption. Examples are: RC6, RSA and ECC. Symmetric and asymmetric encryptions are both data encryption methods being used in today's networks and computers. Symmetric encryption is a kind of encryption where one uses the same key to encrypt and decrypt the same information. This means that the same information is required or used during the encryption and decryption process. Being the same encryption key for both ends, it must be kept secret. This therefore means that if a person gets the key, that person can read all the information that is encrypted.

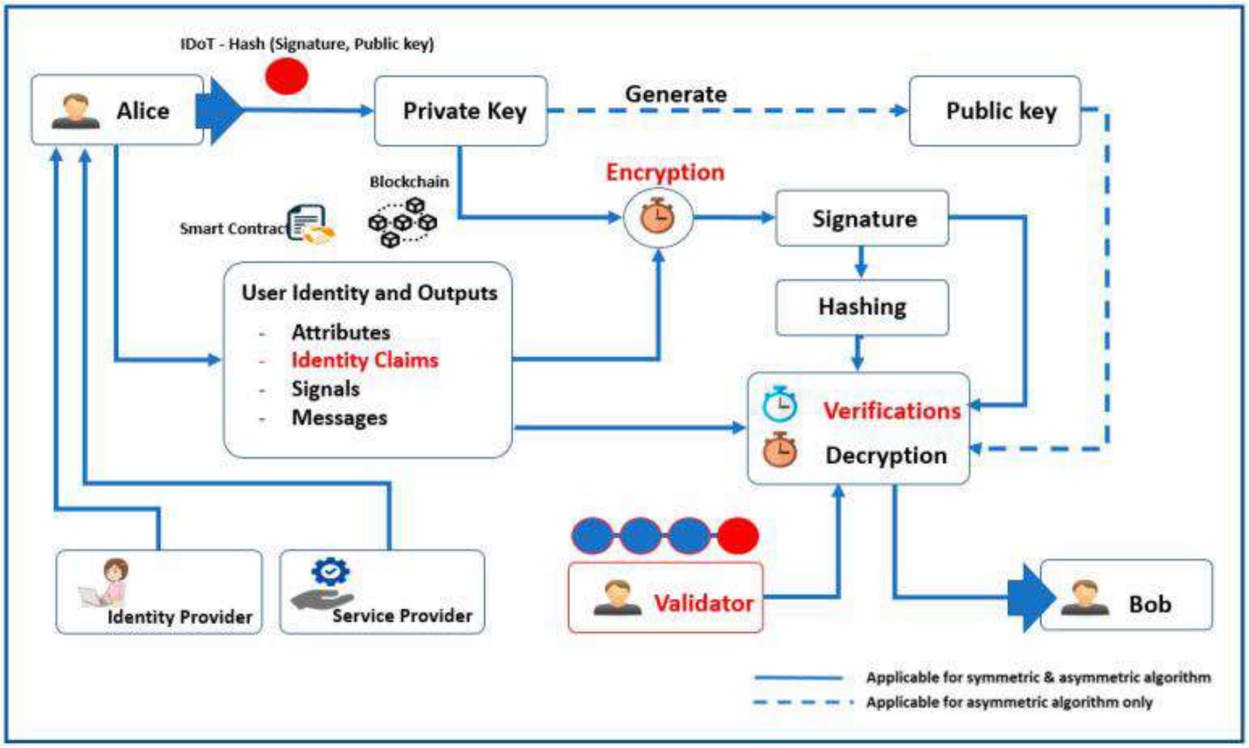

Figure 1: *Diagrammatic Representation of the Conceptual Framework of* Symmetric and Asymmetric Cryptography Algorithm [9].

Symmetric Encryptions

Symmetric encryption also known as *Secret Key Cryptography (SKC):* is currently being heavily used due to the fact that it is very fast to use. This is because of the fact that very few resources are required. With respect to this aspect, many people tend to combine both symmetric and asymmetric not only for security but also for a quick and efficient working. *Secret Key Cryptography (SKC):* This algorithm uses a single key for both encryption and decryption; also called symmetric encryption. Primarily it's been used for privacy and confidentiality of data, the sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. The receiver then applies the same key for message decryption and recovers the plaintext. In this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret [2].

Asymmetric Encryptions

Asymmetric encryption is another kind of encryption that one will come across. It is commonly referred to as *Public Key Cryptography (PKC)*. This algorithm uses one key for encryption and another for decryption; also called asymmetric encryption. Primarily it's been used for authentication, non-repudiation, and key exchange. Public key cryptography is known as the most significant new development in cryptography. The Generic PKC employs two keys that are mathematically related although knowledge of one key does not allow someone to easily determine the other key. Here the one key is used to encrypt the plaintext and another key is used to decrypt the cipher text. The important thing to keep in mind is that it does not matter which key is applied first, but both the keys are required for the process to work. Usually in PKC, one of the keys is designated as the public key and may be advertised as widely as the owner wants. Another key is designated as the private key and is never revealed to another party [2].

Blowfish

Blowfish was first published in 1993 [10]. Blowfish is one of the symmetric key block cipher with key length variable from 32 to 448 bits and block size of 64 bits. Its structure is fiestal network. Blowfish is a symmetric block cipher that can be used as an informal replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and commercial use [11]. Blowfish was designed by Bruce Schneier as a fast, free alternative to existing encryption algorithms. From then, it has been analyzed considerably, and it is slowly gaining popularity as a robust encryption algorithm. It's 26 suffers from weak keys' problem; no attack is known to be successful against. Blowfish is not patented, has free license and is freely available for all users [11]. Blowfish is another symmetric-key encryption technique designed by Bruce Schneier in 1993 as an alternative to the DES encryption algorithm. Therefore, it is significantly faster than DES and provides a good encryption rate. Its key length is 446 bits, and way better than DES, and 3DES. Therefore, it's more difficult to crack the key of Blowfish. It also has a block size of 64 bits. It can be used in software as well. However, AES receives more attention today, nevertheless, Blowfish and Twofish was recommended by Schneider as an alternative due to free license, easy, faster and available for all uses. It is also efficient in both software and hardware [12].

DES

This is developed by IBM and based on a design by Horst Feistel. It was one of the widely used and publicly available cryptographic systems when it was first released. Even though its first debut is in the 70s, it was later adopted by the National Institute of Standards and Technology (NIST). It's a symmetric-key algorithm for the encryption of digital data. It has a block size of 64 bits and uses the Feistel network as a structure. It's slow and not used in the software. It had a high impact on the advancement of cryptography. However, it's insecure for applications due to the short key length of 56 bits. In 1999, distributed.net break a DES key in 22 hours and 15 minutes. After these kinds of events, NIST withdraws this algorithm as a standard. However, 3DES emerged after the vulnerabilities in DES.

3DES

3DES otherwise known as Triple DES, 3DES, or TDES is officially the Triple Data Encryption Algorithm. It's a symmetric-key block cipher and it applies the DES algorithm three times to each block. It has a block size of 64 bits and a key length of 112 or 168 bits. It also uses the Feistel network since it's based on DES. Due to the modern cryptology techniques and supercomputing, like the DES, 3DES has also some serious vulnerabilities. That's why the NIST has deprecated DES and 3DES for new applications in 2017 and for all applications by 2023.

Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is another type of cipher that protects the data from malicious parties. This is a symmetric block cipher design to protect classified information. AES combines speed and security properly, thus, allows to carryout online activities without any interruption. AES uses the same key to both encrypt and decrypt data; it is also a symmetric type of encryption. There are three types of lengths of AES encryption keys 128, 192, and 256 bits. Each key length has different possible key combinations. It has a different structure than other encryption algorithms, it uses the substitution-permutation network [12].

Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) is one of the Asymmetric Key Cryptography, it is a system for public-key cryptography that makes the use of elliptic curve equation. The algorithm was designed and proposed by Neal Koblitz and Victor s. Miller. ECC method is considered more superior than other methods, because it uses a key that is much smaller, but it can provide the same level of security with an asymmetric algorithm using larger keys. With the smaller size of the key and the same high level of security, the implementation of ECC becomes more efficient [12].

Rivest, Shamir and Adelman (RSA)

This is an asymmetric cryptographic algorithm named after its founders Rivest, Shamir & Adelman [13], [14]. RSA is one of the best-known public key cryptosystems for key exchange or digital signatures or encryption of blocks of data used by modern computers in data encryption and decryption. RSA uses two keys, one being the public key which is used for encryption and the private key used for data decryption hence it being an asymmetric algorithm. The encryption key is always made public and can be accessed by anyone while the decryption key is kept private. RSA uses a variable size encryption block and a variable size key. It is an asymmetric (public key) cryptosystem based on number theory, which is a block cipher system. It uses two prime numbers to generate the public and private keys size is 1024 to 4096 bits. These two different keys are used for encryption and decryption purpose. Sender encrypts the message using Receiver public key and when the message gets transmit to receiver, then receiver can decrypt it by using his own private key [15]. RSA operations can be decomposed in three broad steps; key generation, encryption and decryption. Although, RSA have many flaws in its design therefore not preferred for the commercial use. When the small values of p & q are selected for the designing of key then the encryption process becomes too weak and one can be able to decrypt the data by using random probability theory and side channel attacks. On the other hand, if large p and q lengths are selected then it consumes more time and the performance is degraded in comparison with DES. Further, the algorithm also requires of similar lengths for p and q, practically this is very tough conditions to satisfy. Padding techniques are required in such cases increases the system's overheads by taking more processing time [14].

SHA-256

SHA-256 is one of cryptographic hash functions designed by the NSA (U.S National Security Agency). SHA stands for Secure Hash Algorithm. Cryptographic hash function is a mathematical operation is performed on a digital data; by comparing the computed "hash" (the output of the execution algorithm) to the hash value that is known and expected, one can determine the integrity of data. SHA-256 hash computed by the words of 32 bits [16].

Hash Functions

This algorithm uses a mathematical transformation to irreversibly "encrypt" information, providing a digital fingerprint. Primarily used for message integrity. Hash functions, also called *message digests* and *one-way encryption*, and are algorithms that, in essence, use no key. Usually, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are mainly used to provide a *digital fingerprint* of a file's contents which ensures that the file has not been altered by an intruder or virus. Hash functions are widely and commonly used for password encryption by many operating systems. Hash functions, thus provide a mechanism to ensure the integrity of a file. A cryptographic hash is a way of taking existing data, a file, picture, email or text that one have created and create a string of message digest from it. If one wants to verify a cryptographic hash, one can send the message to another person and ask him to hash it and if the hashes match, then the file is the same on both sides. An important characteristic of hashing is a one-way trip. This means that one cannot look at the hash and figure out what the original text was. This is a method that is used to store passwords since if someone gets the hash, he or she cannot figure out the original password. A hash can also act as a digital signature in that it can offer some authentication of one's files and data. It also ensures that the data one receives has integrity. This therefore means that one does not have to encrypt all one's information. One should also make sure that the hashes have no collision. This basically means that two different messages containing different information cannot have the same hash.

Steganography

Steganography is an ancient Egyptian technique of hiding the message using liquid like invisible inks, microscopic writing and hiding code words within sentences of a message. Cryptographers may apply steganography to electronic communications and that application is called transmission security. This is a way to secure things by making them obscured which in reality is not security. Messages appear invisible but it is right there before one. In other cases, it may be embedded within pictures, sounds and documents. This means that in such a case, all that we see is the cover text of that is above the hidden information. One way of implementing steganography is by hiding the information in network packets. It is obvious that packets move really fast and therefore it is possible to send a lot of information that is embedded in the packets. One can also use an image in steganography. This means that one can embed one's information in the image itself.

Cipher

The word "cipher" means "secret" and it is the most popular and secure technique as compared with codes and codebooks as well as steganography. Ciphers are the secret codes used to encrypt plaintext messages. There are two general types of ciphers, namely Substitution and Transport ciphers [17]. In substitution cipher, an alphabet is to replace plaintext with another letter or symbol. In transposition ciphers, the mix up of letters in a word or sentence is made to convert it into unintelligible form. We also have computer ciphers that are used for digital messages encryption. Computer ciphers differ from ordinary substitution and transposition ciphers in which a computer application performs the encryption of data. Below is the more detail description of substitution and transposition ciphers [2].

Digital signatures

In cryptography, digital signatures are used to check for non-repudiation. This basically means that we are digitally signing a message or file. In this case, no type of encryption on the message is required since with the digital signature, an individual is in a position to verify that the message came from one and was not changes in the course. One can sight it with one's private key and people to whom one has sent the message will use one's public key so as to verify that the message was from one. This is the important bit of having public keys in that one are in a position to verify the senders of the various messages one receives. If one verifies a digital signature with its source, then one is assured that the file or piece of information has not undergone any changes in between the sender and the receiver [18].

Cryptography and Its Capabilities

There are many different ways through which people can implement cryptography. In most case, people might not be familiar with the most cryptographic technologies and in this case, they are advised to use proven technologies to encrypt their data. In this case, people reduce their over reliance on the most common data encryption types. In addition, with the use of proven encryption technologies, one is able to have a wide range from which one can choose from. The Elliptic curve cryptography is an emerging technology in cryptography. This is a technology that was created so as to deal with the numerous constraints associated with asymmetric encryption such as numerous mathematical numbers. This cryptography method uses curves instead of numbers where each curve has a mathematical formula associated with it. Quantum cryptography is also another emerging technology in cryptography. Just as the name suggest, this is a technology that employs the use of quantum physics and applying that into the calculations and methods of encryption we are doing inside of our cryptography. Ephemeral keys are special types of cryptographic keys that are generated so as to execute each key establishment process. There are cases where an ephemeral key is used more than once in a single session especially in cases where only one ephemeral key pair is generated for each message. Perfect forward secrecy is also another kind of cryptographic technology whose main aim is to ensure that information or rather data packets being sent across a network are sent with top level secrecy so as to avoid detection. In this case, such packets are normally sent when there is a lot of traffic travelling through a network since it is very difficult to identify a specific packet if the transmission is fully loaded [18]. Block cipher encryption entails taking one full block of information and encrypting it as a full block all at the same time. In most cases, the blocks are normally of 64-bits or 128-bits. This means that their size is predetermined and remains the same during encryption and decryption. When using the block cipher method, one needs to ensure that to have some confusion so that the encrypted data seems far much different. When using the block ciphers one can also implement the diffusion concept where the output becomes totally different from the input [18]. Stream cipher is another kind of encryption that is used with symmetric encryption. Contrary to block where all the encryption is done all at once, encryption in stream ciphers is done one bit at a time. This is a type of encryption that can run at a very high speed and requires low hardware complexity. An important aspect to know when using stream ciphers is that the initialization vector should never be the same when one is starting to do some of the streams because someone may easily figure out the initialization vector and encryption key one are using and use it every time one send data across the network. Make sure that one's initialization vector is always changing while using it to encrypt information. Transport encryption is an aspect of cryptography that involves encrypting data that is in motion. In this case, one has to ensure that data being sent across a network cannot be seen by other people. In addition, the encryption keys should not be visible to others. Transport encryption can be implemented with the use of a VPN concentrator. If one is outside one's office, one will use some software to send data to the VPN concentrator where it will be decrypted and then sent to one's local network in a manner that it can be understood. With this kind of encryption, it becomes very difficult for an individual to tap into one's network and look into a conversation between two workstations since the information is already scrambled up. Session keys: Session keys are special types of cryptographic keys that can only be used once. This means that if a session key encrypts some information at a particular time, it cannot be used again to encrypt any other information Key Escrow: In the context of cryptography, Key escrow refers to the encryption keys. In this case, it requires that a third party stores the encryption key so that we can decrypt information in case the original key gets lost. In this case, the encryption key should be kept in a very safe place so that it is not accessed by others. Key escrow also helps when it comes to the recovery of data. Symmetric encryption in the context of key escrow means that one is keeping one's key somewhere making sure that it is put in a safe so that no one can get access to it. There are number of *trust models* used for various cryptographic schemes. The trust models in cryptography requires trust and secure. Even though secret key cryptography can ensure message confidentiality and hash codes can ensure integrity. It cannot perform without trust.

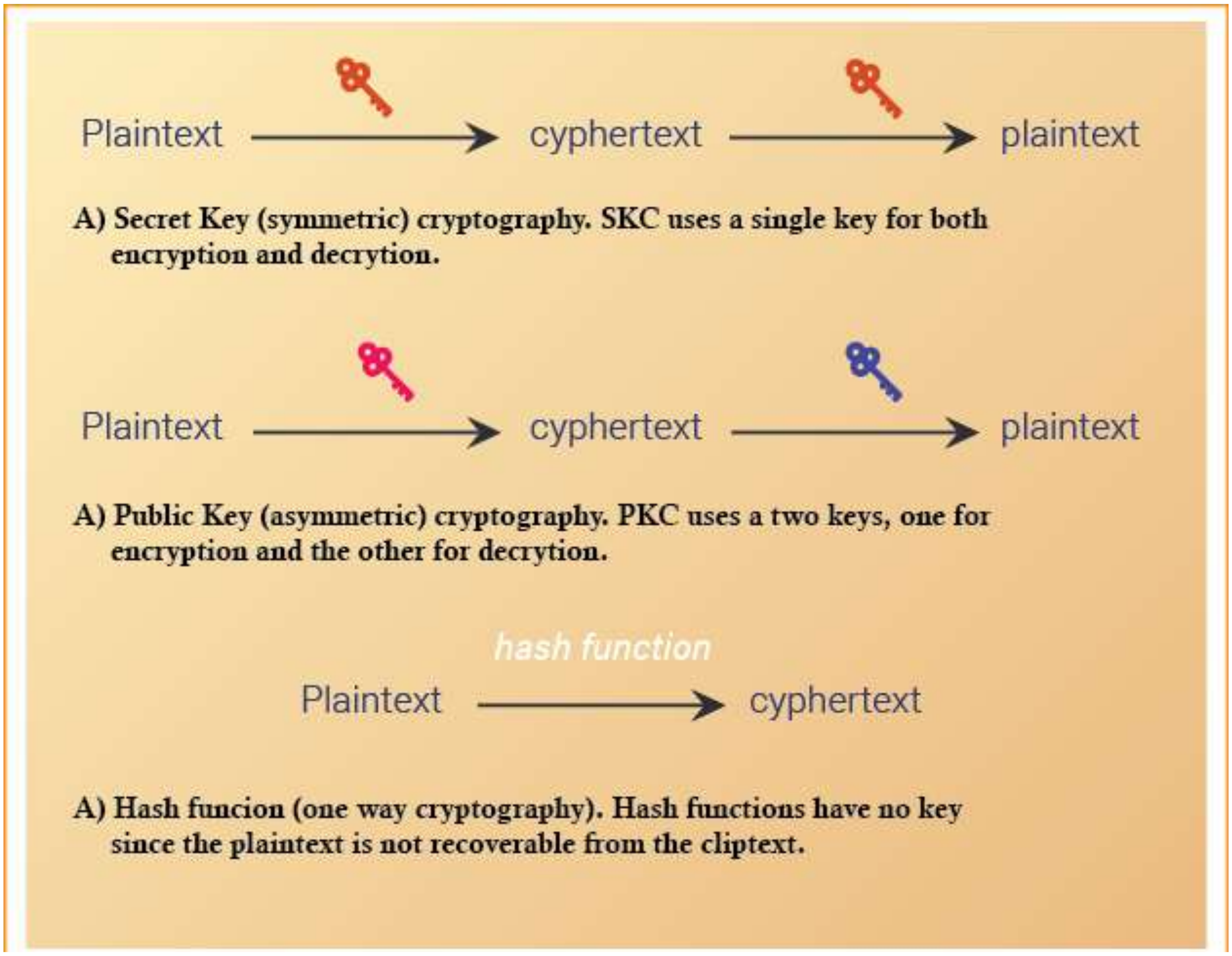
Plaintext
cyphertext
plaintext
A) Secret Key (symmetric) cryptography. SKC uses a single key for both encryption and decrytion.
Plaintext
cyphertext
plaintext
A) Public Key (asymmetric) cryptography. PKC uses a two keys, one for encryption and the other for decrytion.
hash function
Plaintext
cyphertext
A) Hash funcion (one way cryptography). Hash functions have no key since the plaintext is not recoverable from the cliptext.

Figure 2: Diagrammatic representation of Cryptography Algorithms

Cryptographic-based model for CISMS

In recent years, with the development of science and technology, as an emerging data security especially in the school information management system. Cryptography is one of the key techniques used widely for the security of large data transmission over the internet. This is evidence as many significant factors such as continuous developments in information technologies, information exchange, increasing expectations of the society, and modern management systems cause organizations all over the world to develop new applications in order to survive. This priority in modern societies on Information Technologies have reached a state of high priority in education sectors [19]. Thus, calls for the development of a cryptographic-based model of Computer-based Integrated School Information Management System to computerize, integrate and control all the activities involved in the collation and processing of student data especially the academic records. Studies have reported globally that, the use of computerised school management system has become very important for the management of educational organisations [20]. [21], described school management information systems as "a management information system that is meant for the structure, task management, instructional processes and other needs of the school". Many educational institutions including post primary schools are constantly trying to improve the quality of education and one of the aspects of such improvement is the management of school resources [22]. The explosive growth of computer-based integrated school information management system technologies has left a tremendous impact on educational institutions [23]. Technology has had an increasingly significant impact and broad implications for everyone-individuals, institutions and the entire nation alike [19]. A school management system is a collection of computer instructions, to manage the day-to-day administrative tasks of schools [7]. School management systems allow schools to digitally monitor their daily activities along with managing all their resources and information on a single platform. Development of a cryptographic-based model of computer-based integrated school information management system will enable the School management system have multiple applications throughout the education cycle; they are capable of eliminating increased work load on school's finances and general administration. Development of a cryptographic-based model of computer-based integrated school information management system will provide School management system opportunities to enhance the performance of the schools with the use of some materials for effective service delivery [24]. Cryptographic-based model of computer-based integrated school information management system provides solution to the problems encountered in school management. There are numerous challenges and difficulties faced by school managers in making sure they come up with vital decisions and quality services to her valued students and customers. These things cannot be achieved through manual operations. Though, the use of paper works in school administration cannot be completely written off, the School Management System is developed to enhance and boast the general school administration. The System is implemented to specifications using NET Beans IDE 8.1 at the front end and SQLite database at the back end. Symmetric data encryption model is used to ensure maximum security, since the validity and integrity of information depends on who had an access to it. School Management System is able to generate academic results, transcripts, timetable, and registration of students, matters regarding welfare of students among other things [25].

Cryptographic-Based Model and Educational System

Nowadays, education plays a great role in development of any country. Many of education institutions try to increase education quality by being effective and efficient in the management of their day-to-day duties. One of the aspects of this improvement is managing of school information system using electronic system [26]**.** For the last two decades the themes of governance and management of school systems have continuously been on the top of education policy agendas in most countries in the world particularly in Nigeria, and a great number of educational problems were attributed to bad management or inappropriate mechanisms of governance. Furthermore, information has become a critical resource to organizations and individuals and should be managed in a suitable way to ensure its cost-effective use, and every aspect of management relies on information to succeed. So, to improve the performance of the organization, the management must be economical, efficient and effective and secured. Development of cryptographic-based model information systems is essential to modern education, notably because of numerous possibilities and advantages which information technology brought forward like effectiveness and efficiency for education sectors, as well as for better achievement of setup in the education goals. Cryptographic-based model of computer-based integrated school information management system has most of the facilities that a modern school requires to computerize its day-to-day jobs. It provides facilities to keep the records of student, fees, teaching and office staff with all their required details along with all required transaction handling. It has facilities to generate various types of reports, which are required by the management during normal business operations to operate the business effectively [19]. The deployment of information systems in organizations has been highly interconnected with each other and the development and the use of a school management system (SMS) leads to better planning, better decision-making and better results. Encryption is a secure process for keeping personal and confidential information private. It is a process by which bits of data are mathematically jumbled using a password key. The encryption process makes the data unreadable unless or until decrypted [19].

Cryptographic-Based Model and Integrity of Data in the Educational System

Security services are intended to protect a system from security attacks, to prevent attacks, or both by utilizing different security model. Thus, in this era of universal electronic connectivity, communication is no more confined to transfer of data from one end to the other; rather it aims at secure data transfer and ensure the integrity of the data. Evidences abound that cryptographic-based model of computer-based integrated school information management system will ensure the security of data by preventing unauthorized interceptors from accessing the data while being transferred to the intended receivers [18], [2]. With the advancements in the field of electronic commerce, the data being transferred over networks should be kept confidential and required to be prevented from any unauthorized access or modification [27]. Thus, data integrity is the need of the hour when it comes to the present form of communication. Each bit of information carries a certain value which needs to be retained and any modification by the intruder can lead to disasters [27]. Various methods have been applied to authenticate data in the past. A data authentication scheme is proposed which helps in privacy preservation and is based on encryption scheme, 'pseudonym technology' and Message Authentication Code [27]. Authentication refers to confirmation, that the data has been received from the projected sender and this is usually verified using secret keys which are known to either ends. Various models have been applied to authenticate data in the past. A data authentication scheme is proposed which helps in privacy preservation and is based on encryption scheme known as, 'pseudonym technology' and Message Authentication Code. User authentication is the process of verifying the identity of a user. In the case of a user-to-user communication, both users have to be checked. Traditionally, in the client–server domain, the authentication is focused on the client side, since the system should be protected from users and not vice versa. Nevertheless, the present study is thus, an attempt like other related work to develop cryptographic model for the security of computer based integrated school information management system. To achieve this, the researcher adopted the use two models namely, Blowfish and RSA algorithm. Moreover, to the best knowledge of the researcher, these two models of cryptographic (Blowfish and RSA algorithm) have not been combined by other researchers for the development of the security of computer based integrated school information management system [18].

Database Theoretical Studies of the Two Models

Database security encompasses three main properties: confidentiality, integrity and availability. Roughly speaking, the confidentiality property enforces predefined restrictions while accessing the protected data, thus preventing disclosure to unauthorized persons. The integrity property guarantees that the data cannot be corrupted in an invisible way. Finally, the availability property ensures timely and reliable access to the database. To preserve the data confidentiality, enforcing access control policies defined on the database management system (DBMS) is a prevailing method. An access control policy, that is to say a set of authorizations, can take different forms depending on the underlying data model (cryptographic model), and the way by which authorizations are administered, following either a Discretionary access control (DAC), Role Based Access Control (RBAC) or Mandatory Access Control (MAC). Whatever the access control model, the authorizations enforced by the database server can be bypassed in a number of ways. Hence, the need to develop a cryptographic model for the security of computer based integrated school information management system. There is probably no single best information system solution that can meet the needs of all public schools, school districts, private schools, and numerous education agencies in Ebonyi State. However, the development of cryptographic model for the security of computer based integrated school information management system for public or government-owned secondary schools in Ebonyi State will help all education organizations to determine the best solution for their particular management challenges. This model can lead education organization decision-makers through the process of making the best and most cost-effective decisions about information management systems devoted to individual schools and student records.

Summary of Literature Review and Research Gap

From the foregoing review of related literature, it was found that this era of technological age, the biggest risk that an organization could take is to stay insensitive to change. Many significant factors such as continuous developments in information technologies, information exchange, increasing expectations of the society, modern management perceptions and applications cause organizations all over the world to develop new applications in order to survive. Because of their priority in modern societies, Information Technologies have reached a state of high priority in education, too. Thus, education plays a great role in development of any country. Recently, contributions of information technologies to education have been among the mostly emphasized. Many of education institutions try to increase education quality by being effective and efficient in the management of their day-to-day duties. One of the aspects of this improvement is managing of school information system using electronic system. Although, several models have been developed and implemented for this. However, cryptographic-based model information systems are the most essential to modern education, notably because of numerous possibilities and advantages which information technology brought forward like effectiveness and efficiency for education sectors, as well as for better achievement of setup in the education goals. Cryptographic-based model of computer-based integrated school information management system has most of the facilities that a modern school requires to computerize its day-to-day jobs. It provides facilities to keep the records of student, fees, teaching and office staff with all their required details along with all required transaction handling. It has facilities to generate various types of reports, which are required by the management during normal business operations to operate the business effectively [19]. The deployment of information systems in organizations has been highly interconnected with each. The development and the use of a School management system (SMS) leads to better planning, better decision-making and better results. Other researchers have combined, developed and implemented different types of cryptographic model like, digital signature (DS) and RSA encryption model, digital signature and encryption 49 algorithms, signature and Rijndael Encryption Algorithm, digital signature and advanced encryption standard framework, RSA algorithm, digital signature and image steganography amongst others for transactions, for enhancing cloud data security and cloud user authentication. However, none have combined, developed, implemented and used RSA and Blowfish algorithms. Therefore, the present study will design and develop cryptographic model for the security of computer based integrated school information management system using RSA and Blowfish algorithms.

REFERENCES

1. Alanazi, H. O., Zaidan, B. B., Jalab, H. A., Shabbir, M. and Al-Nabhani, Y. (2010). New Comparative Study between DES, 3DES and AES within Nine Factors. Journal of Computing, 2(3): 152-157.
2. Munir, MW (2015). Independent Study Report – Cryptography. Salim Habib University (formely Barrett Hodgson University) Affiliation: SZABIST, Karachi. DOI:10.13140/RG.2.1.2947.9844

3. Fortine M., Michael K. and George O. (2017). "Enhanced Secure Data Storage in Cloud Computing Using Hybrid Cryptographic Techniques (AES and Blowfish*)". International Journal of Science and Research* (IJSR), 6, 3. Available on www.ijsr.net, accessed on 23/4/2023.
4. Stallings, W. (2004). Cryptography and Network Security, 3rd edition, Pearson Education.
5. Charomie, Tat Wi (2010) *Implementation of hybrid encryption method using caesar cipher algorithm*. Faculty of Computer System & Software Engineering, Universiti Malaysia Pahang.
6. Antara M. (2023). Information Security Researcher | Cyber Security Leader/Influencer | IT Lead Auditor| Risk Management | Technical Writer | Trainer/Speaker | Open to Remote OpportunitiesAuthentication for Data Security in Cloud Computing. *International Journal of Innovative Research in Computer and Communication Engineering* 2.(2); 456-459.
7. Peter, A., Kronberg, M., Trei, W. and Katzenbeisser, S. (2012) Additively Homomorphic Encryption with a Double Decryption Mechanism, Revisited. In: Gollmann, D.
8. 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
9. Kairaldeen AR, Abdullah NF, Abu-Samah A. and Nordin R. (2023). Peer-to-Peer User Identity Verification Time Optimization in IoT Blockchain Network. Sensors (Basel). 2023 Feb 13;23(4):2106. doi: 10.3390/s23042106. PMID: 36850701; PMCID: PMC9961683.
10. Mahindrakar MS. (2014). Evaluation of Blowfish Algorithm based on Avalanche Effect. *International Journal of Innovations in Engineering and Technology*, 4(1):99-103.
11. Pratap, CM. (2012). Superiority of blowfish Algorithm. International Journal of Advanced Research in Computer Science and Software Engineering. 2012;2(9):196-201.
12. Amir Mahmud H.1, Bayu Angga, W.1., Tommy, Andi Marwan, E., and Siregar, R. (2018). Performance analysis of AES-Blowfish hybrid algorithm for security of patient medical record data, J. Phys.: Conf. Ser. 1007 012018
13. Sonal S, Prashant S, Ravi Shankar D. (2011). RSA algorithm using modified subset sum cryptosystem. 2nd International Conference on Computer and Communication Technology. 457-461.
14. Preetha M, Nithya M. (2013). A study and performance analysis of RSA algorithm. International Journal of Computer Science and Mobile Computing; 2(6):126-139.
15. Aman K, Sudesh J. and Sunil M. (2022). Comparative Analysis between DES and RSA Algorithm's. *International Journal of Advanced Research in Computer Science and Software Engineering*, 2012;2(7):386-391.
16. Kadam, K.G. and Khairnar, V. (2015). "Hybrid RSA-AES Encryption for Web Services, International Journal of Technical Research and Applications", Special Issue 31(September, 2015), PP. 51-56
17. Mahata, S. K and Dey, M. (2016). A Novel Approach for Cryptography using Modified Substitution Cipher and Triangulation. *International Research Journal of Computer Science* (IRJCS). 4, (3); 2393-9842.www.irjcs.com
18. Ivanova, J. and Jurczyk M. (2003). A Security Services in Encyclopedia of Physical Science and Technology (Third Edition), Computer Networks.
19. Adesina A.O., Ajagbe SA,, Odule, TJ, and Agbele, K.K. (2022). Development of an improved SCHOOL information management system. *FUW Trends in Science & Technology Journal*, 7 (1); 120 – 134.
20. Wachiuri, R. N., Shisha, B., Nonglait, L., and Kimathi, J. N. (2017). To Determine the Effects of the Role of Examinations on the Development of All-Inclusive Learners in Secondary Schools Nyeri County, Kenya. IOSR Journal of Research & Method in Education, 7(3), 62-65. doi:10.9790/7388-0703016265
21. Qazi, A., Hardaker, G., Ahmad, I. S., Darwich, M., Maitama, J. Z., & Dayani, A. (2021). The Role of Information & Communication Technology in Elearning Environments: A Systematic Review. IEEE Access, 9, 45539-45551. doi:10.1109/ACCESS.2021.3067042
22. Fulmer, C. (1995). Information Technology in Educational Management. London: Chapman and Hall: In B. Barta, M. Telem, and Y. Gev (Eds)
23. Manju, G. (2014). school Management Information System: An Effective Tool for Augumenting the School Practices. New Frontiers in education: International Journal of Education & Research, 57-64.
24. Majlinda and Bekins. (2013). Implementation of School Based Management in Creating Effective Schools. International Journal of Independent Research and Studies 1(4), 142-152.

25. Harsha H. K. and Thyagaraja M. A. (2016). Design and Development of School Management System with Database Encryption and Decryption, *International Journal of Research*, 3; (12): 460-472. Available at https://edupediapublications.org/journals
26. Refsnes D. HTML Editors. [online] Available: 2019. https://www.w3schools.com/html/html_intro.asp[Accessed:10 the August 2019]
27. Zhong H. and Shao L. A. (2016). Lightweight and Secure Data Authentication Scheme with Privacy Preservation for Wireless Sensor Networks, International Conference on Networking and Network Applications (NaNA). 2016; 210 – 217.

CITE AS: Chinenye P. Ikeagwu; Virginia E. Ejiofor; Orji Everistus Eze and Godspower Akawuku (2025). Survey of Cryptography models for Security of Computer-based Integrated School Information Management System. Research Output Journal of Engineering and Scientific Research 4(1): 60-70. https://doi.org/10.59298/ROJESR/2025/4.1.6070