UTM
UNIVERSITI TEKNOLOGI MALAYSIA
INTERNATIONAL JOURNAL OF
INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

Citizens’ Data Protection in E-government System

Musa Midila Ahmed[1] & Aishatu Musa Ahmed[2]
Faculty of Education
Modibbo Adama University, Yola, Nigeria
Email: ahmedmm4me@yahoo.com[1], aishatma79@gmail.com[2]

Submitted: 11/10/2022. Revised edition: 31/7/2023. Accepted: 17/9/2023. Published online: 24/11/2023
DOI: https://doi.org/10.11113/ijic.v13n2.389

***Abstract*—E-government is the use of information and communication technology for public service provision in governance. Nowadays, E-government facilitates transparent, accountable, efficient and all-inclusive governing process for improved service delivery to citizens. However, the emergence of this novel innovation opened up new security vulnerabilities to citizens’ data. Comprehensive security plan for secure linkage of people, process and technology is crucial to ensure that data and network channel is protected from potential security threats. The purpose of this study is to provide a security model for protection of citizens’ data in E-government system. This paper propose information security stack, a data protection model for efficient data protection in E-government system. The information security stack comprised of citizens’ identification, authentication of identities, data confidentiality and data integrity in E-government system. First, this paper classified citizens’ identification into international, national and purposive identification. Second, acceptable form of identification for authentication of identities in E-government system depends on the security restriction imposed on the requested information. Consequently, user authentication is classified into single factor authentication, two-factor authentication and multifactor authentication depending on the use case in the E-government system. Third, data confidentiality implemented by data encryption is an information security goal for preserving the privacy of information in E-government system. The authors categorised data encryption in E-government into symmetric encryption and asymmetric encryption. Finally, ensuring the accuracy and completeness of citizens’ data is crucial for preserving data integrity in E-government system. This can be achieved by digital signature, an electronic version of handwritten signature.**

***Keywords*—Data protection, identification, authentication, confidentiality, data integrity**

I. INTRODUCTION

Nowadays, the popularity of information and communication technology (ICT) for service provision in all aspect of life is evident. The important role of ICT in modern society has significantly changed the ways people interact to gain information and learn quickly and conveniently. The effective use of ICT in governance promotes the societies in many ways such as increase in workers efficiencies, promote innovations and collaborations as well as reduces information sharing cost. According to Zahid, *et al.* [1], the adoption of E-government systems promotes the efficiency of public service delivery worldwide. E-government is the use of communication technology to enhance the efficiency of governance by provision of government services online. However, a study by Ayyash, *et al.* [2] discovered that central control of distance services and uncertainty avoidance are some of the factors that affects the adoption of E-government system in Arab cultural dimensions. According to the author, face-to-face interactions and nepotism are part of the factors that positively contributes to employees’ adoption of E-government services by government agencies. In a nutshell, E-government has the capacity of modernizing all sectors of governance by promoting accountability and enhanced transparency. E-government enables integration of various government agencies as well as enhances security especially in federated government system.

E-government as a service system requires service-oriented architecture (SOA), an approach for efficient integration of autonomous services into a large software system. Barakat and El-baqqati [3] proposed a database design by extract–transfer-load (ETL) process for interoperability of E-government service. Also, Nakonechnyi and Kolisnichenko [4] proposed a user model for effective collaboration of E-government participants by the analysis of information flow and technological infrastructure. Qusef, *et al.* [5] provide a deployment architecture for E-government by analysis of digital e-services and parties interaction in E-government system. An architectural model for enhanced data validation and fast communication as well as easy logistics development by Suzuki and Suzuki [6] uses case study of large cargo in transport management system. To integrate independent government services in Sidoargo regency, Utama *et al.* [7] uses SOA to integrate databases, services and their implementations for amalgamation of regional governments. Similarly, Almahmoud [8] proposed a solution for integration of regional systems by SOA framework to extract data from the regional services.

A similar focus on integration by Sasono *et al.* [9] uses government service bus (GSB) for management of e-government services to integrate services in government-to-business (G2B), government-to-citizens (G2C) and government-to-government (G2G), which results into smart city. Fajar and Shofi [10] designed E-government service system to solve the heterogeneity problem by service-oriented design and analysis to integrate services in Indonesian government. The author realised an integrated E-government service by enterprise service bus (ESB) technology. An effort to develop a model that can handle citizens' complains for Sri Lanka's E-government system, Jayawickrama [11] use business process execution language (BPEL) to depict the process to develop an e-complains model based on SOA. In a case study for performance analysis of government offices, Hodijah, *et al.* [12] use SOA approach for integrating business process in E-government system. The author discovered that the open group architectural framework (TOGAF) provide adequate service innovation for good government governance (GGG). To transform peer-to-peer system into one-big public service platform, Sofian [13] used RESTFUL web service to integrate both local and external services by ESB. The author discovered ESB as an efficient integration middleware.

Apparently, E-government where telecommunication networks by mobile devices and computers have dominated public services provision worldwide. This innovation provide easy access to information and services of governments. In addition, the innovation promotes fast and efficient interaction between citizens, government and businesses. Despite the numerous benefits of E-government system, its adoption renders public information and services vulnerable to security challenges. The security issues emanated from the open and heterogeneous nature of E-government services. In order to increase citizens' trust and confidence in E-government services globally, there is the need to ensure adequate privacy and protection of citizens' data for enhanced security in E-government system.

Data protection are measures taken to make sure that data is used properly and fairly as well as prevents the data from damage, loss or corruption. In today's modern data-driven world, innovative software applications are developed to ease sharing data making life easier, more convenient and integrates all stakeholders both at home and at work. However, as the size of data in an E-government system increases, so does the importance of data protection. Therefore, it is important to ensure that data privacy and data integrity are adequately protected. Furthermore, there should be measures to ensure that corrupt and loss data are quickly recovered. A robust data protection model for E-government system should have strong data back-up, data retention, data monitoring and auditing. E-government security policies should ensure strong data access control is properly formulated and implemented. Finally, citizens and other E-government system users be educated on data protection measures by regular security awareness and training programme.

Data back-up and recovery is the practice of keeping duplicate data in a secure location for use in case of loss or damage. Modern data back-up and recovery solutions are supported by cloud-based technology that automates the process for efficiency and speedy data recovery. Data retention is the quantity of data an organization keep as long as it is useful. In other to efficiently achieve data retention requirement in E-government system, there is the need for constant monitoring and auditing of stored data. Monitoring refers to maintaining regular surveillance to observe and check movement of data. Whereas, auditing is the examination or inspection to ensure that policy requirements are adhered to. Data encryption is the process of transforming data either at rest or on-transit from its plain text (unencrypted) to cipher text (encrypted) form. This is to protect sensitive information from hackers. For instance, sensitive information such as personal identification numbers (PIN) and passwords can be encrypted making it unreadable by authorized entities to prevent identity theft and fraud.

The aim of this study is to provide a comprehensive security plan for E-government systems that will ensure citizens' data both stored and on network channels in E-government systems are protected from potential security threats. The remaining part of this paper is organized as follows; section 2 discusses on the components of E-government service systems, section 3 is for information security model for E-government system and section 4 concludes the paper.

II. E-GOVERNMENT SERVICE SYSTEM

The essence of E-government is to deliver public service electronically. E-government is an indispensable technological innovation for transforming the relationship between government, businesses and citizens. This is to make operational processes of governance more efficient and speedy. E-government facilitates exchange of information and data among citizens, businesses, and agencies of government online. E-government is recognized as the means of public service provision by integration of autonomous services to enable seamless interactions between government and citizens (G&C), government and businesses (G&B) as well as government and government (G&G) [14]. According to Chipeta [15], the communication channels of E-government systems establishes interaction between key components for effective and efficient public service provision. This improves the administrative efficiency of E-government services as well as enhance the governance operations in a robust, flexible, agile and systematic manner. The implementation model of E-government is described by three key aspects; governance, services and citizens as shown in Fig. 1. It is important to separate regulatory duties of governance from public service delivery to adequately align business requirements with capabilities of modern technologies. Overall, the actual interactions in E-government system takes places between service providers and the citizens. Security protection of data exchanged online on the channels between services and citizens is crucial.

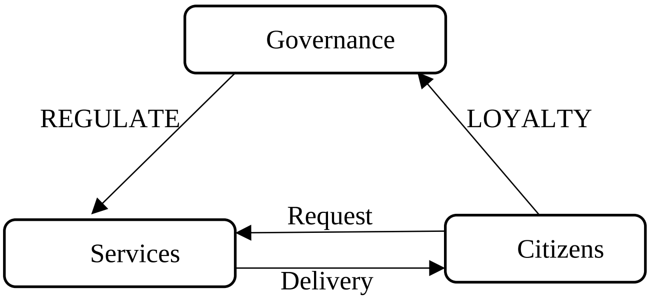

Fig. 1. E-Government Service Implementation

a) Governance

Governance is one of the key aspect of public service delivery in the E-government service implementation. The main functions of governance is the approval, regulation and services' integration by increasing reliance on technology for effective service delivery to citizen. The use of E-government for public service delivery has lots of benefits. Particularly, it enhances the effectiveness and efficiency of decision making in governance. Furthermore, E-government promote efficient use of resources and strengthens accountability, transparency and inclusiveness. A field survey by Jameel, *et al.* [16] discovered that good governance promotes trust, which extensively influences citizens' behaviours to government. According to the author, citizens' trust is regarded as one of the important components of governance. Also, public trust enhances citizens' loyalty to governance. In other word, citizens with high trust tends to be more loyal to the governance. A study by Thompson, *et al.* [17] found out that fundamental security protection is not widely implemented in the development of E-government portal in both Thailand and Australia with potential high security risks. The author recommends implementation of standard security best practices to boost conformance and citizens' trust in E-governance globally. Clearly, citizens' trust and data security protection are crucial issues for success of E-government system.

b) Services

The main business of government is to render services to its citizens. The delivery of these services is either directly by establishment of government agency or indirectly by non-governmental organization. The services provided by government agency or private establishment include but not limited to education, health, transportation, immigration, commerce and industries. Government may establish agencies for approval and regulation of service providers' activities. So that citizens' consumes services from the service providers, while government approves, set standard and monitors the quality of services renders by the service providers. Therefore, secured interactions between citizens and service providers is an important aspect of data protection in E-government systems. Government need to have keen interest in the standard of services provided to public in order to earn the trust and loyalty of the citizens. Troshani, *et al.* [18] found out that technological innovations digitises business reporting facilitating efficient exchange of information between service providers and regulators. Generally, government will make use of the revenue and taxes generated to provide and promote desired services to the citizens through corporate organization in collaboration with government professionals. The digitized reporting in E-government system is crucial because it is important for government to collect information from business organizations to ensure the safety and security of citizens.

c) Citizens

A citizen is a person who gained membership of a country, state or local government by fulfilling specified legal requirements. The legal requirements may be place of birth, parents' nationality, or authorized nationality. A citizen is entitle to certain rights including but not limited to protection, services, political rights and freedom as contained in the national constitutions. It is mandatory for citizens to obey the established laws, pay taxes and consume services approved by government agencies. Citizens have the responsibility of participating in governance by registering for services including to vote and be voted for in elections as well as be loyal to the governance authorities. Modern technological advancement and the popularity of internet promotes citizens' engagement and consumption of online services boosting inclusiveness, transparency, fast, efficient and cheap governance. Silal, *et al.* [19] identified E-government as an important tool for mitigating corruption by government as well as establishing direct connection between public services and citizens for good governance. The author recommend harnessing the electronic participation of citizens as a potential tool for good governance attainment. Looking at E-government from the information security perspective requires adequate protection of citizens' data both at rest and on transit in the communication channels. Ultimately, citizens have to be loyal to governance as well as request and enjoy public service rendered by or on behalf of government in an honest manner. However, lot of security issues including impersonations, identity theft, privacy and data integrity violations need to be protected to earn citizens' trust and confidence in governance.

III DATA PROTECTION MODEL FOR E-GOVERNMENT SYSTEM

E-government system is an efficient approach to promote public service sectors' service delivery using modern technological facilities. However, security is a major issue in E-governance network where citizens' interact with services connected to share information easily, fast and in transparent manner. As the E-government technology develops, so also attacks advances in using similar sophisticated intelligent technologies to exploit E-government service systems. Although, the adoption of E-government systems positively changed the ways citizens consumes public services in most countries in the world. It is necessary to ensure security protection of physical facilities, software systems and E-government networks' communication channels. Physical facilities need to be protected from damage and/or theft. Also, software systems both at rest and on transit need to be protected from any form of violation and unauthorized access. Finally, E-government networks' communication channels be protected from man-in-the-middle attacks. Efficient data protection in E-government system could adequately be realised by the E-government information security stack. The information security stack comprise of four components. The components are identification, authentication, confidentiality and data integrity. These components built on one another as shown in Fig. 2.

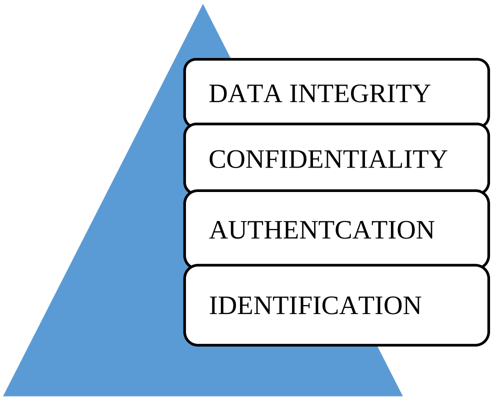

Fig. 2. Information Security Stack

3.1 Citizen's Identification

Identification is any means that can be used to prove a person is an indigene of a community, state or country. It is usually issued in the form of a document, standard identity or passport card. Identification is a trusted means of managing domestic as well as cross-border protection for both human and material resources. Identification of human and material resources lays solid foundation for establishing trust and privacy of citizens' data and facilities. Both traditional and electronic identification usually follows the same pattern. Electronically, a central database uniquely stores identification numbers that are issued to citizens and material resources. This can subsequently be used to support the processes of authentication, confidentiality and data integrity. Identification is a crucial aspect of information security in E-government system since authentication, confidentiality and integrity of information can only be realised on the basis of proper citizens' identity. Authentication is the verification of citizens' identity to ensure that he is who he claim to be. Confidentiality is the state of keeping the privacy of information. Whereas, data integrity goal upholds the honesty of all interactions. The main goal of citizen identification is to prove the identity of citizens and control movement of people within as well as across borders.

Identification system serves as the foundational trusted source that provides the basis for secure identity verification and other security goals for government and non-governmental organization users. In other word, an efficient identification system is a vital source of identity information for identity proving process of government and private sectors. Identification system serves as an authoritative source of identity proving as such it must be trusted by all parties. To earn the trust of citizens and other stakeholders, the credentials collected must be efficient, accurate and stored in a secured database register. Citizens' identification in E-government system takes different forms guided by the need to prove the legal identity of individuals for accessing services and other basic rights and protection. Citizens' identification should be uniquely assigned to a person and not transferable to another entity. Citizens' identification can be broadly classified into general purpose covering the entire population or specific purpose covering the scope of a functional system. General identifications' coverage is broad as a means of citizens' identity within a country or worldwide. Purposive identification usually covers a subset of the population, for instance to identify citizens eligible to vote or those who passed drivers' test. In order to create a functional system for management of identification in E-government, citizens' identification system is hereby classified into; international identification, national identification and purposive identification as follows.

a) International Identification

International identification is an identifier assign to people different from the national identification number to identify citizens of several countries in the world. An international identification number uniquely identifies person's nationality recognized by the international standard organization. It is legally recognized as security identifiers for global transactions. International identification usually assign to citizens on a passport booklet issued to eligible people to verify their identity and nationality. The passport book serves as a security document for the purpose of international travels and transactions. The popularity of internet and modern technology greatly ease issuance and verification of passports worldwide. In other word, the use of E-government system greatly improves application and verification process of passport documents within the country and in the diaspora.

b) National Identification

National identification is a means of tracking citizens and other residence within a country for efficient governance. National identification is used for many purposes including but not limited to taxation, work, education, security and health services consumption. It is used for identification of citizens' status by government and non-government organization in transactions and public service consumption. In other words, national identification form the foundation on which citizens of a country is recognized for public services and entitlements. It forms the basis of national planning and development as well as policy-making to improve efficiency of public services. Nowadays, the popularity of E-government system is responsible for enhanced security challenges. This necessitate the need for efficient national identification system to recognize potential fraudster and threats. Improving security protection for E-government by preventing impersonations and identity thefts promotes citizens' thrust in online services. Ultimately, recognition of thrusted identity electronically is an important aspect of a well-functional E-government system.

c) Purposive Identification

In addition to national identity, which is based on establishing citizens' identity in a specific country. Purposive identification focused on certain characteristic, right or services associated with the country. For instance, issuance of voters' identification, tax payers' identification, driver's licence identification and students' identification numbers.

i) Voters' Identification

Advancement in modern technology and E-government system leads to the existence of electronic voter register. The technology uses digital voter identification in election process that depends on voters' information stored in voters' database. These technologies nowadays used smartcard that has records of voters' biometric information such as fingerprint and other biometric data.

ii) Tax Payers' Identification

Payment of tax is mandatory for all citizens and business organizations in a country. Tax identification number is a unique number assigned to all eligible tax payers for the purpose of paying taxes. The purpose of tax identification is to ease the administration of tax returns, statements and other related documents.

iii) Driver's Licence Identification

To drive a car in a country, an individual must have a valid driver's licence issued by an authorized organization to those that are eligible and passed the required driving test. The valid driver's licence serves as a primary identification document in most countries. Nowadays, the ever-evolving use of mobile technology has transformed the task of issuance and verification of driver's licence.

iv) Students' Identification

Students' identification is a unique number assigned by authorities in learning institutions to genuine students. This number serves as the primary key for accessing individual student's record in the register. Students' identification is connected to the students' personal identifiable information such as student's name, parent's name, student's address, and national or international identification number. Student can use students' identification number to gain access to their education records and other system resources. However, this may require one or more additional factors that authenticate users to curtail impersonation and identity theft.

Other methods of citizen's identification in E-government system include username and password, biometric identification, smart cards, digital certificates and one-time password. Username is a unique set of characters assigned to computer system or online account users as prove of individuals' identity. Whereas, password is a secret word or numbers used by authorized users as identity prove for getting access to sensitive information. In username and password combination, the username serves as means of identification and password is for authentication to verify the users' true identity. Nowadays, biometric identification is gaining increase in popularity, particularly in situations involving automated recognition of users by using physical characteristics and biological data for security purpose. Smart cards is a physical card like driver's license and credit card with embedded integrated chip containing user's data, which serves as a security token. Digital certificate is an aspect of public key infrastructure (PKI) that cryptographically assigned ownership of public to the entity that owns it. The main function of digital certificate is to share public key for encryption and authentication. One-time-password (OTP) is similar to password to password only that it is automatically generated and is valid for only one login session and it expires within a short period of time. This is to reduce the risk of fraudulent login attempts and enhance E-government system's security.

3.2 Authentication of Identity

Authentication is the process of verifying peoples' identity. Authentication technology verifies one or more identification factors for controlling access to system resources. The security system check if the identification evidence provided by user match the one stored in the database of authorised users. Authentication enables organizations maintained secure network by allowing only authenticated user getting access to systems' resources. Subsequent to successful authentication, authorization process commences. Authorization determines the specific system resources an authenticated user is permitted to access. This is because an authenticated user might have permission granted to access specific systems' resources only. Authentication and authorization are closely related but they performs distinct functions. In a nutshell, authentication validates the identity of registered system user by verifying that he is who he claim to be. While authorization validates that the authenticated users has been granted permission to access specific system resources. Usually, authentication process serves as the prerequisite to successful authorization. The authentication and authorization processes enforces the required restriction to system resources generally refers to as access control.

An acceptable forms of identification depends on the restrictions and security imposed on the services requested by the citizen. Authentication factor is a piece of data or attribute acceptable for user authentication process to gain access to system resources. Traditionally, authentication factors can be something user know, something user have and something user is. User authentication can be implemented by single factor authentication (SFA), two factor authentication (2FA) or multi-factor authentication (MFA) depending on the use case of the system. A security critical or highly restricted services may require multi-factor identity verification. Whereas, a less secured and restricted services may admit only one factor identification. For instance, multi-factor authentication may imposed on financial transactions, where citizens may be required to provide their account number and national identification number. An example of one-factor authentication is a students may use only his matriculation number to access news bulletins and announcements in the college portals.

a) One-factor Authentication

The most common authentication use case is the SFA, which require one credentials to sign-in and gain access to the system. SFA is a system protection mechanism that requires only one category of credential for getting access to network, website or software system. The most common example of using SFA for securing access to a given system is password-based authentication mechanism. This security mechanism requires systems users to create a strong password making it difficult for someone crack. Unfortunately, creating a strong password as well as keeping the single credential secure is the main challenge in SFA. The single credential should be protected from hackers' discovery and less predictable by machines. A strong credentials is difficult to crack through guessing, dictionary attack, brute force attacks or any other identity theft methods. However, despite using strong credential, social engineering attack (SEA) proved to be a difficult information security threat. This is because SEA attackers psychologically exploits peoples' intelligence as a trick for getting confidential information. Ahmed [20] suggested intensive training and awareness programmes for citizens on detection and prevention of SEA to reduce its success in E-government system.

b) Two factors Authentication

Two factor authentication is an authentication system that requires users to present two distinct kinds of identification to gain access to information resource. This is to provide additional ability of monitoring and safeguarding the most vulnerable information and network from disclosure and violation. Two factor authentication is also referred to as two steps verification double the security protection of applications and network environment. It is the simplest multifactor authentication that provides the most effective means of user verification to improve authentication in E-government system. Two factor authentication is a specific type of multifactor authentication that strengthen access security by requiring two methods to verify users' identity. The factors can be something users' know such as username and password, something users' have such as smart card or something user is like biometric or biological data to fulfil authentication requirements.

d) Multi-factor Authentication

Multi-factor authentication require users to present two or more credentials as evidence to authentication mechanism for getting access to system resources. Access to systems' resources such as network, website or software system is granted to users only after successful authentication of all credentials presented. MFA provide additional security by requiring more than one factor. In case of MFA system that require two factors is referred to as two-factor authentication (2FA). MFA drastically reduce identity theft and other related network frauds. However, nowadays MFA may be ineffective against the dynamic nature of modern threats like ATM skimming and social engineering attacks. Although, Ahmed [20] suggested use of MFA as ways of reducing SEA, because requesting for many credentials from users might discourage citizens and raise their awareness on potential SEA.

There are other ways of authenticating users in E-government system. This include public key infrastructure (PKI), single-sign-on (SSO) and risk-based authentication. PKI is a set of technology and processes that supports asymmetric encryption to preserve privacy and authenticates digital communication. PKI is a kind of internet encryption that help to authenticate systems' user to ensure secure digital communications. It preserve the privacy of messages as well as verify that the sender is a genuine entity. SSO is an authentication service that permits users to use one login credentials to access multiple applications. This is to ease management of multiple credentials by individuals and organizations. Whereas, Risk-based authentication is an authentication method that makes it easier for the right people to gain right level of access and prompts potential malicious users to complete additional verification stage(s) according to the organizations' security policy. Generally, the choice of authentication method to use depends on the level of security required and the kind of users.

3.3 Data Confidentiality

Confidentiality is an information security goal for keeping sensitive data secret to unauthorized entities. It is an ethical principle or legal requirement for professionals to keep secrets of all information of their service consumers. For instance, health service providers should keep all information collected from their patient in secret. Disclosure of such information is unethical or illegal unless the patient authorize such disclosure. Similarly, the academic records of learners in educational institutions should be protected secret to unauthorized entities. Therefore, confidentiality is an important legal and ethical duty for all professionals and public service providers in E-government system. Managing data confidentiality ensures that only those authorised get access to sensitive information by use of encryption algorithm.

Encryption is an information security protection mechanism where data is encoded and can only be decoded to gain access by authorised user with the right encryption key. The encrypted data appears meaningless, scrambled or unreadable to unauthorised entities. Data encryption is an important cybersecurity protection, which makes it difficult for unauthorised access to data both at rest or on-transit. Encryption algorithm scrambles human-readable plaintext to an unreadable cipher text so that only authorise parties using the correct key can understand the information. Encryption algorithm uses a set of mathematical manipulations with a cryptographic key that both the sender and the receiver of the cipher text is aware of. Basically, there are two main kinds of encryption; symmetric encryption and asymmetric encryption.

a) Symmetric Encryption

Symmetric encryption is a category of encryption whereby interacting parties uses the same secret key for encoding plain text into cipher as well as decoding cipher text back to plain text. In other word, symmetric encryption is a kind of encryption where a single key is use for both encryption and decryption of protected data. Therefore, interacting parties must have a secured channel of exchanging the secret key used for encryption to the receiver for successful decryption of the data. Popular examples of symmetric encryption algorithms include but not limited to Data Encryption Standard (DES), Triple DES and Advanced Encryption Standard (AES). The advantage of symmetric encryption is that it is faster and more efficient especially for huge quantity of data than asymmetric encryption. However, secure exchange of the secret key is identified as its major challenge. This is because exchanging the secret key over unsecure communication channel renders the transmitted data vulnerable to attacks.

b) Asymmetric Encryption

Asymmetric encryption (also known as public key encryption) uses two keys, public key and private key. The public key is expose to the world generally, whereas the private key is kept secret. In this kind of encryption algorithm, the sender encrypts the message by the public key, so that the receiver decrypts the message with his private key at the receiving end. In practice, every entity can encrypt a message with the public key of the receiver. However, only the receiver using his private key can decrypt the message. The most popular examples of asymmetric encryption algorithms are; Rivest, Shamir and Adleman (RSA) and Elliptical Curve Cryptography (ECC) algorithms. The main advantage of asymmetric encryption is that it requires no key sharing between message sender and its receiver. However, it is slower than symmetric encryption due to the complex calculations in the algorithm. Asymmetric encryption is particularly suitable for encryption in large, open and distributed network, especially if every participating entity maintains the privacy of the secret keys.

3.4 Data Integrity

Data integrity is an information security goal for the overall accuracy, completeness and consistency of data. Data integrity requirement ensures the safety and reliability of data both at rest and in transit. Data integrity is important in protecting data from the threats of both internal and external malicious users. Furthermore, maintaining data integrity enrich decision-making by protecting the validity and reliability of citizens' data in E-government system. According to Botchwey [21], protection of citizens' data in E-government system is not an option but a necessity. This is because of the increase in digital service provision worldwide, which is accompanied with new risks and information security challenges. Data integrity maintains the quality of information set used in focused and lawful decisions in E-government system. Protecting the integrity of electronic data in E-government is achieved by digital signature. Digital signature is a cryptographic algorithm to ensure the integrity and authenticity of data.

a) Digital Signature

Digital signature is an electronic equivalent of the handwritten document signature or stamp. Digital signature is a mathematical technique to protect the integrity and authenticity of a message and other electronic documents. It might serve as an evidence of electronic contracts and online legal documents. Digital signature supports E-government initiative by providing alternative legally binding contract and official document in E-governance equivalent to that of face-to-face interactions. The main benefit of digital signature is enhanced security features in electronic transactions to ensure that the document or message is not altered and it originate from a legitimate source. In other word, digital signature enables the message receiver be sure of the sender's identity and the message is intact.

Similar to handwritten signature, digital signature algorithm aims at establishing the uniqueness of the signer. Digital signature algorithm uses a two-stage encryption process called hash and data encryption. The hash algorithm creates message digest in such a way that the digest is irreversible and no two messages hashed to the same digest. In addition, no two digests can be hashed from the same message. At the data encryption stage, the message digest is encrypted to form an electronic signature of the message. The message sender sends both the message digest and its electronic signature to the receiver. At the receivers' end, the receiver decrypts the electronic signature to obtain a message digest and compare with the accompanied message digest. If the two message digests are identical means the message is authentic and intact.

b) Digital Signature with Asymmetric Encryption

Modern digital signature uses asymmetric encryption for signing and verifying messages. The integration of digital signature with public key cryptography provide message authentication, message integrity and non-repudiation. Non-repudiation is achieved since the signer cannot deny signing the document by his unique keys. The algorithm binds the public key with an identity of a particular person or entity whose private key signed the document. In practice, digital signature with asymmetric encryption works with two different keys; public key and private key. The public key is broadcast to everyone and the private key is kept as secret. An amalgamation of digital signature with asymmetric encryption results into strong, secure and reliable system. In addition, the amalgamation is adequate for the protection of large, open and distributed system.

Digital signature with public key cryptography such as RSA is similar to the digital signature with symmetric encryption except it uses public key and private key infrastructure for encryption and decryption of message digest. In digital signature with RSA, the sender creates message digest by hash algorithm, then encrypt the message digest with his private key to form an electronic signature of the message. The only way to decrypt the electronic signature is by the use of signer’s public key. In a nutshell, the sender encrypt the message digest with his private key and the recipient decrypt the data with the sender’s public key. Sequel to decryption of the data to obtain the digest, the recipient compare the decrypted digest with the accompanied digest. If the two digests are identical shows that the message is authentic and reliable.

Ensuring the accuracy and completeness of citizens’ data is a critical aspect of preserving data integrity in E-government system. This goal can be achieved through many other ways such as data validation, data verification, data integration, data audits, data quality checks and data governance, Data validation refers to checking the accuracy, completeness and genuineness of data source to warrant consideration for usage. Data verification refers to checking the accuracy of migrated data. There are two categorise of data verification; full data verification and sampled data verification. Full data verification is where the whole data is verified and sampled data verification is where a sampled representation of the whole data is checked. Data integration is a process of combining related data from difference sources to provide a unified view to users. Whereas, data audits is the process of examining the quality of data in its lifetime to ensure that it is accurate and efficient for specific usage. Data quality checks is the examination datasets to ensure it meets required criteria for accuracy, completeness, validity, consistency, uniqueness, timeliness and fit the purpose of E-government system. Consequently, data quality checks is a critical aspect of data governance in E-government system, since data governance is every action taken to ensure adequate security in E-government system including data accuracy and completeness, data privacy, data availability and usability.

IV. CONCLUSION

Nowadays, E-government system has globally dominated public service provision. This innovation enhanced the quality of governance. It leveraged on the popularity of mobile devices, networks and computer services to provide fast, efficient and easy access to information and services of government. This paper proposed information security model to protect citizens’ data from damage, loss or corruption. The security model ensures adequate privacy, data integrity and general protection of citizens’ data in E-government system. It is recommended that citizens be well educated on data protection measures and policies by regular security awareness and training programme. Further research is recommended on data back-up, data access control, data monitoring and auditing for enhanced security protection in E-government system.

ACKNOWLEDGMENT

We are grateful to Faculty of Education of Modibbo Adama University, Yola, Nigeria for the support and encouragement on the conduct of this research.

REFERENCES

[1] Zahid, H., Ali, S., Abu-Shanab, E., & Javed, H. M. U. (2022). Determinants of intention to use e-government services: An integrated marketing relation view. *Telematics and Informatics, 68*(1), 1-17.

[2] Ayyash, M. M., Herzallah, F. A., & Al-Sharafi, M. A. (2022). Arab cultural dimensions model for e-government services adoption in public sector organisations: an empirical examination. *Electronic Government, An International Journal, 18*(1), 9-44.

[3] Barakat, O., & El Beqqali, O. (2020, September). Business intelligence and SOA based architecture for E-government system interoperability. *Proceedings of the 13th International Conference on Intelligent Systems: Theories and Applications, 40*(1), 1-5.

[4] Nakonechnyi, A., & Kolisnichenko, N. (2020). Service-oriented architecture of E-Government: Characteristics of the Anglo-American model and peculiarities of its implementation in Ukraine. *Public Administration and Local Government, 47*(4), 39-48.

[5] Qusef, A., Ayasrah, A., & Shaout, A. (2021). Comprehensive approach to implement E-Government backend in Jordan using service-oriented architecture. *International Journal of Software Innovation (IJSI), 9*(2), 122-135.

[6] Suzuki, T., & Suzuki, L. (2020). On the benefit of 3-tier SOA architecture promoting information sharing among TMS systems and Brazilian e-Government Web Services: A CT-e case study. *arXiv preprint arXiv:2005.13047, 1*(1), 1-14.

[7] Utama, A. P., Asmara, R., & Hasim, J. A. N. (2019). E-Government integration of Sidoarjo Regency using Service Oriented Architecture (SOA*). IJNMT (International Journal of New Media Technology), 6*(2), 109-115.

[8] Almahmoud, A. A. (2020, September). E-Services integration framework based on SOA. *Proceedings of the 2020 12th International Conference on Information Management and Engineering, 12*(1), 1-6.

[9] Sasono, D. S., Setyohadi, D. B., & Santoso, A. J. (2018). E-Government integration based on SOA for supporting Sleman Smart Regency (A Case Study of Sleman Regency Special Region of Yogyakarta). *ICCSET 2018, October 25-26, 1*(1), 360-366.

[10] Fajar, A. N., & Shofi, I. M. (2019, August). Service oriented design for Indonesian E-Government system using SOA. *InIOP Conference Series: Materials Science and Engineering*. IOP Publishing. *598*(1), 1-5.

[11] Jayawickrama, G. I. U. (2021). Customer complaint management system using SOA. Doctoral dissertation. University of Colombo. 1-93.

[12] Hodijah, A., Sundari, S., & Nugraha, A. C. (2018, May). Applying TOGAF for e-government implementation based on service oriented architecture methodology towards good government governance. *Journal of Physics: Conference Series*. IOP Publishing. *1013*(1), 1-8.

[13] Sofian, A. R. (2019, November). Designing SOA-based BATAN Public Services with Restful Web Service. *2019 IEEE International Conference on ICT for Smart Society (ICISS),* 7(1), 1-6.

[14] Burlacu, S., Patarlageanu, S. R., Diaconu, A., & Ciobanu, G. (2021). E-government in the era of globalization and the health crisis caused by the covid-19 pandemic, between standards and innovation. *SHS Web of Conferences EDP Sciences, 92*(1), 1-8.

[15] Chipeta, J. (2018). A review of e-government development in Africa: A case of Zambia. *Journal of e-government Studies and Best Practices*, *2018*(1), 1-13.

[16] Jameel, A., Asif, M., & Hussain, A. (2019). Good governance and public trust: Assessing the mediating effect of E-government in Pakistan. *Lex Localis*, *17*(2), 299-320.

[17] Thompson, N., Mullins, A., & Chongsutakawewong, T. (2020). Does high e-government adoption assure stronger security? Results from a cross-country analysis of Australia and Thailand. *Government Information Quarterly*, *37*(1), 1-9.

[18] Troshani, I., Janssen, M., Lymer, A., & Parker, L. D. (2018). Digital transformation of business-to-government reporting: An institutional work perspective. *International Journal of Accounting Information Systems, 31*(1), 17-36.

[19] Silal, P., Saha, D., Bose, I., & Jaikumar, S. (2022). Studying the Role of E-Government in enabling Good Governance Unpublished doctoral dissertation. Indian Institute of Management, Calcutta.

[20] Ahmed, M. M. (2022). Social engineering attacks in E-Government system: Detection and prevention. *International Journal of Applied Engineering and Management Letters (IJAEML), 6*(1), 100-116.

[21] Botchwey, G. (2018). E-governance and cybersecurity: User perceptions of data integrity and protection in Ghana. *5th Biennial Social Science Conference of the University of Education, Winneba, Ghana*.