Original Manuscript

Information Development
1–14

DOI: 10.1177/02666669221085709
journals.sagepub.com/home/idv
SAGE

Biometric system for protecting information and improving service delivery: The case of a developing country's social security and pension organisation

Emmanuel Owusu-Oware
Department of Information Technology Studies, University of Professional Studies, Accra, Legon, Ghana

John Effah
Department of Operations and Management Information Systems, University of Ghana, Legon, Legon, Ghana

Abstract

The conception of biometric systems as a means of securing sensitive information and enhancing service delivery remains under-researched. To address this knowledge gap, we explore the case of a public-sector social security and pension organisation in Ghana using a qualitative interpretative study approach and the information security model of confidentiality-integrity-availability as an analytical lens. The study's findings indicate that integrating and using biometric identification and authentication as part of delivering social security and pension services can protect availability, confidentiality, and integrity of information. The findings further show that the use of a biometric system for social security and pension information security can contribute to reducing service turnaround time and vulnerability to fraudulent manipulation of benefits payments. The study provides implications for research, practice, and policy. For research, the paper opens up biometric systems' study from the perspective of information security and service improvement. For practice and policy, the study demonstrates the importance of aligning biometric systems' deployment and use with domain application requirements.

Keywords

biometric, CIA triad, information security, interpretive study, social security and pension, Ghana

Submitted: 23 July 2021; accepted: 19 February 2022

Introduction

The purpose of this study is to understand how a biometric system can secure access to restricted information and contribute to social security and pension (SSP) service delivery improvement in a developing country context. Access to information has become a fundamental requirement to societal development and the fourth industrial revolution (Oyediran-Tidings et al., 2021). Increasingly, information and communication technologies (ICTs) are being adopted to fulfil such a fundamental requirement by providing easy and timely access to information and facilitating socioeconomic development. For example, the use of mobile phones by agro-pastoralist communities to access information aids their poverty reduction efforts (Mwantimwa, 2019). In healthcare institutions, e-health systems make medical information readily available to physicians, enabling them to provide timely care to patients (Marutha, 2020). Timely access to information is, therefore, an important requirement in information management and service delivery. In addition, the need to protect personal or confidential information is also important because of potential threat to privacy and abuse (Asani, 2014; Posey et al., 2017).

Corresponding author:
Emmanuel Owusu-Oware, Department of Information Technology Studies, University of Professional Studies, Accra, Legon, Ghana.
Email: emmanuel.owusu-oware@upsamail.edu.gh

In general, the mechanism for protecting restricted information entails authentication of people's identity claims. Authentication confirms the identity claim of an individual (Ogbanufe and Kim, 2018) based on either knowledge (e.g. password and personal identification number (PIN)), a token (e.g. ID card), biometrics, or a combination of these verification methods (Briggs and Thomas, 2015). Among these authentication methods, biometric systems are considered more reliable in securing access to information resources. Biometric systems are superior authentication methods because they establish personal identity through unique physical features such as fingerprints, face, and iris. Not only are these physical features difficult to steal, share, or duplicate, but they also require the owner's presence to verify a claimed identity (Lumini and Nanni, 2017; Rao and Nayak, 2014), such as a username or identity card.

Developing country biometric information systems (IS) studies have focused more on national identification (e.g. Effah et al., 2020; McGrath, 2016), national elections (e.g. Effah and Debrah, 2018; McGrath and Maiye, 2010) and social protection (e.g. Masiero, 2018; Owusu-Oware et al., 2018). The national identification studies have been on using biometric identification to support socioeconomic development goals such as financial inclusion, taxation, and crime control. Studies on elections examined the use of biometric identification in combating electoral malfeasance, while social protection studies looked at using biometric systems to enhance and control access to government-sponsored social welfare services, such as food subsidies and national health insurance.

However, in all of these empirical studies, the conception of a biometric system as a mechanism for securing access to restricted information and improving service delivery has been overlooked. Thus, our knowledge of the role of biometric systems is limited. This study therefore contributes to filling this knowledge gap by investigating the use of a biometric system as part of providing SSP services. SSP services are government-sponsored social protection arrangements against negative effects of loss of income due to old age, disability, or death (Dorfman and Palacios, 2012; Ramona, 2009). The services include collecting contributions from members, maintaining their financial and personal records, investing the funds, and paying benefits (Ramona, 2009).

The research question guiding this study is: *how can a biometric system improve SSP information security and service delivery*? To answer this question, this study employs qualitative interpretive methodology (Myers, 2013; Walsham, 2006) and confidentiality-integrity-availability (CIA) information security model (Parker, 2010; Warkentin and Orgeron, 2020) as the analytical lens to investigate the case involving the use of a biometric system by the social security and national insurance trust (SSNIT). SSNIT is the government agency in Ghana that administers SSP services. Section 4.1 under the research setting and methodology of the paper provides background information about Ghana and the SSNIT.

The remaining part of the paper is structured as follows: Section 2 reviews relevant literature on information security and biometric systems. Section 3 presents the CIA model as the theoretical foundation for this study. Section 4 discusses interpretive case methodology, the approach used to conduct this study. Section 5 reports the results of the theory-based analysis of the case study based on the CIA model. Section 6 discusses the results in relation to the research question and literature. Section 7 concludes with the study's contribution to research, practice, policy, and suggestions for future research.

Literature review

Information security

The security of organisational information is increasingly being challenged as threats are getting more sophisticated and varied in the era of Industry 4.0 (Bhaharin et al., 2019). Information security, therefore, plays an important role in ensuring that organisational operations and services are not disrupted or compromised. Information security refers to the protection of information from unauthorised access, use, modification, or destruction (Alsmadi et al., 2018; He et al., 2014). The fundamental goals of information security are to ensure confidentiality (i.e. state of being private or secret), integrity (i.e. state of not being impaired), and availability (i.e. state of being accessible) (Alsmadi et al., 2018). These three goals are commonly called the CIA triad, the analytical lens for this study (see Section 3). Because information is a critical asset for organisations, the security goals apply to all of its states, that is, when information is being created or processed, when information is at rest (such as stored on a hard drive), or when information is in motion (such as in transit through a network) (Alsmadi et al., 2018).

Information security is sociotechnical in nature (Samonas and Coss, 2014). The technical aspects relate to implementing and monitoring technologies to prevent or mitigate loss from present or future security breaches (Zafar and Clark, 2009). The social aspects include (Alsmadi et al., 2018; Zafar and Clark, 2009): 1) governance, i.e., developing and enforcing security strategy, policies and procedures to protect information assets; 2) human, i.e., educating personnel in security awareness and code of conduct and 3) legislation, i.e., enacting laws to protect information assets. Finally, risk management, which is both technical and social, entails identifying and mitigating potential threats to information assets.

Threats to organisational information assets are many, diverse, and complex because they involve information, personnel, and systems that process, transport, and store them (Whitman, 2003). Information system threats include: software attacks (e.g. viruses, worms, macros, and denial of service); software failures or errors; acts of espionage or trespass (e.g. hacking and spoofing); acts of sabotage or vandalism (e.g. destroying hardware); hardware failures or errors; acts of theft, and acts of information extortion (Whitman, 2003). Organisations often rely mainly on technology-based solutions as part of their effort to protect information from such threats (Cavusoglu et al., 2015). Technology-based solutions identified in the literature (Caballero, 2017; Cavusoglu et al., 2015; Els and Cilliers, 2017; Safa, 2017; Zhu and Sun, 2018) can be grouped into under three main types: encryption, access control, and intrusion mitigation.

Encryption technologies such as cryptography render information unreadable by unauthorised persons (Caballero, 2017; Els and Cilliers, 2017). Among the security technologies, encryption is the most basic and technical means to protect information (Zhu and Sun, 2018) in all states. Intrusion mitigation technologies are software or hardware that prevent or detect malicious or policy violation activities (Safa, 2017). Examples are firewalls and anti-virus software (Cavusoglu et al., 2015). Firewalls examine and block harmful network and application traffic (Caballero, 2017). In general, intrusion mitigation technologies protect information undergoing processing or in transition (Alsmadi et al., 2018). Access control systems, on the other hand, include passwords and smart cards. A more modern access control system is based on biometrics, which is the focus of this study. Access control systems protect information in storage (Alsmadi et al., 2018).

Biometric systems

Biometric systems are not only for access control of restricted information but also for managing individual identities. As an identity management system, a biometric system can be used to prevent fraud, enhance security, and reduce identity theft (Rao and Nayak, 2014). A biometric system is made up of people's biometric data and ICTs used to collect, store, and process data (Yang et al., 2019). Identity management functions of biometric systems are enrolment, identification, and authentication (Jain et al., 2004; Lumini and Nanni, 2017; Yang et al., 2019). The enrolment function associates individuals with their respective biometric data (Roy et al., 2017). During enrolment, individuals' unique body features (for example, fingerprints) are captured through input devices, such as fingerprint scanners, processed, and then stored in a database (Roy et al., 2017). The identification function determines whether an individual's biometric data is already stored in the database. Thus, when used with the enrolment function, the identification function, prevents individuals from obtaining multiple IDs through multiple enrolments (Yadav and Tadisetty, 2012). The authentication function verifies that a person is who they say they are by comparing his/her biometric sample to the stored biometric data in a database or on a smart ID card. Thus, compared to conventional identification systems that authenticate individuals based on what one knows (e.g. a password) or has (e.g. a plain ID card), biometric authentication is based on what one is (e.g. fingerprints) and what one does (e.g. handwriting) (Lips, 2010; Lumini and Nanni, 2017). In this wise, biometric based identification is difficult to lose, forget, steal, share or duplicate (Lumini and Nanni, 2017).

Although biometric systems provide enhanced security compared to conventional authentication systems, they are not widely accepted because of perceived intrusiveness, privacy infringement, and potential misuse by authorities (Whitley et al., 2014; Zviran and Erlich, 2006). Additionally, a biometric system can wrongly authenticate individuals based on errors referred to as "false matches" or "false non-matches" (Rao and Nayak, 2014). A false match (or false acceptance) is where an individual's biometric sample matches with someone else's stored data. A false non-match (or false reject) is where an individual's biometric sample does not match the stored data. In practice, these two error types, which are inversely proportional, can be adjusted to desired

acceptance thresholds, in line with the access control goals of an application. For instance, a highly secured system will have a higher threshold setting to decrease false matches and increase false non-matches. On the other hand, a lowly secured system will have a lower threshold setting that decreases false non-matches and increases false matches (Beynon-Davies, 2007; Zviran and Erlich, 2006).

In general, biometric authentication errors may arise for several reasons, including manufacturer defects, sensor wear and tear, environmental conditions (e.g. dirt, humidity, and lighting), and target population characteristics (e.g. age and occupation) (Jain et al., 2004; Uzoka and Ndzinge, 2009). Other challenges are security breaches (e.g. spoofing) and high infrastructure costs (Jain and Nandakumar, 2012; Yang et al., 2019). In practice, these challenges can be addressed in several ways, including the use of multimodal biometrics, encryption technologies, and smart cards. Multimodal biometric systems improve the accuracy of authentication by using one or more physical body features (e.g. fingerprints and eye iris) to establish an individual's identity to an acceptable level of confidence (Moses and Rowe, 2016). Encryption technologies complement biometric system security by rendering stored biometric data unreadable to interceptors (Parks and Mead, 2014). Smart cards, on the other hand, are cost-effective offline solutions for biometric authentication (Owusu-Oware et al., 2018).

Biometric systems have been widely deployed in both developing and developed countries. Increasingly, developing countries employ biometric systems for socioeconomic developments, including national identification (e.g. McGrath, 2016), national elections (e.g. Effah and Debrah, 2018), health insurance (e.g. Owusu-Oware et al., 2018), and food subsidy (Masiero, 2018). Thus far, developing country IS literature on biometric systems has given much attention to their role in socioeconomic development. Research on the role of biometric systems in information security for service delivery is therefore under researched. This study therefore seeks to address the knowledge gap using the case of a biometric system deployment and use by an SSP organisation in Ghana.

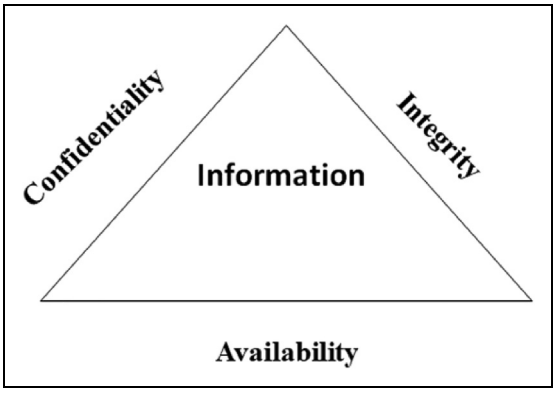

Figure 1. The CIA triad (Qadir and Quadri, 2016).

Theoretical foundation: The CIA triad model

The theoretical foundation for this study is the CIA triad model. The CIA triad is an information security model that considers three fundamental security controls: confidentiality, integrity, and availability. These security controls ensure that restricted information is protected against unauthorised access (Parker, 2010; Warkentin and Orgeron, 2020). The CIA triad originated from Saltzer and Schroeder's (1975) seminal paper, which identified three types of threats to information: unauthorised information release (confidentiality), unauthorised information modification (integrity), and unauthorised denial of use (availability). It was subsequently developed by the National Institute of Standards and Technology, an agency of the United States Department of Commerce) (Neumann et al., 1977). Figure 1 depicts the CIA triad model.

Figure 1 illustrates the CIA triad model as the three protection dimensions of information. Confidentiality relates to protecting data from unauthorised access (Warkentin and Orgeron, 2020). Confidentiality includes the means to protect personal privacy and proprietary information (Parker, 2010). Integrity refers to capturing accurate information and preventing unauthorised changes (James et al., 2013; Samonas and Coss, 2014). Availability ensures timely and reliable access to and use of information (Parker, 2010, p. 14). These three security concepts constitute the fundamental security controls that inform theoretical understanding and practices of information security in organisations (Samonas and Coss, 2014). Availability is the base, as shown in Figure 1, because without information availability, confidentiality and integrity of information cannot be applied (Qadir and Quadri, 2016). In other words, confidentiality and integrity of information are pointless if such information is not available to the intended users (Alsmadi et al., 2018).

The CIA triad has been extensively used in understanding and designing information security in many areas, including electronic health records (Jayabalan and O; aniel, 2017), internet of things (Panchiwala and Shah, 2020), robotic systems (Bhardwaj et al., 2019) and blockchain (Warkentin and Orgeron, 2020). Many authors have proposed modifications to the CIA taxonomy in order to extend its range of application (Parker, 2010; Samonas and Coss, 2014; Thomborson, 2010; Warkentin and Orgeron, 2020). For example, Warkentin and Orgeron (2020) call for inclusion of non-repudiation as an additional concept. However, we chose to use the CIA triad without any additional constructs because of its simplicity and suitability in analysing our field data to answer our research question.

Research setting and methodology

Research setting

SSNIT, the case organisation, is situated in Ghana, a middle-income sub-Saharan African country with a population of about 30 million. The Ghana government first established the SSP scheme in 1965 through an act of parliament (Act 279) to provide income security for workers at the end of their working lives or where they are unable to earn income. Currently in Ghana, SSNIT is the statutory public agency that manages the basic and mandatory SSP scheme for workers in the country. Every worker in Ghana, except employees of security agencies, is required to join and make monthly contributions to the SSP scheme. The SSP scheme is financed through combined contributions of employees (currently 5.5% of basic salary) and employers (13% of the employees' basic salary) as well as returns from investments made by SSNIT. SSNIT is currently the biggest non-bank financial institution in the country, with a membership size of about 5% of the national population (SSNIT, 2021).

SSNIT's services include registering workers as members and issuing them with ID cards with unique social security numbers (SSNs); receiving members' monthly contributions; managing members' personal and financial records; investing the contributions; processing claims and paying benefits for members as they fall due. SSP benefits are paid to qualifying members within the age bracket of 60 to 72 years for a guaranteed period of 15 years. Beyond 72 years, SSP payments are continued upon annual renewal of pensioners' life certificates.

SSNIT's service delivery is decentralised across its branch offices in the regions and districts of the country. Service delivery entails member identity authentication, which precedes service requests. For many years, SSNIT operated a centralised manual authentication system which was inefficient and prone to errors and manipulations in benefit payments. SSNIT responded by replacing the centralised manual system with a biometric system as part of an enterprise system project. The goal of the project was to transform the entire operations of SSNIT for efficient and effective service delivery.

Functionally, SSNIT uses the biometric system to capture, process, and store members' biometric data in a central database for member identification and authentication before services are delivered. The biometric data capturing components include computers (i.e. desktop computers and laptops) and biometric devices (i.e. digital cameras, fingerprint and signature scanners) attached to the computers. An automatic fingerprint identification software (AFIS) runs on the computers. The biometric-based computers are deployed at SSNIT's branch offices. Networks (i.e. local and wide area networks) link the branch offices to SSNIT's data centre at the head office. The network links enable real-time transfer of members' biometric data to the central database for processing. The data processing and storage components consist of servers hosting the centralised AFIS application software and database. The ID card production component is used to print biometric based smart ID cards. The authenticating component includes the biometric smart card readers and terminals deployed at the service points. Section 5 shows how SSNIT used the biometric system to protect SSP information and improve service delivery.

Methodology

We followed a qualitative interpretive case study methodology (Myers, 2013; Walsham, 2006) for this study because the aim was to gain in-depth understanding of the information system phenomenon within its real-life context (Myers, 2013; Walsham, 2006). Moreover, as the study was a longitudinal one, the flexibility of the interpretive approach allowed the researchers to explore and respond to field conditions as the study unfolded.

Data collection

Data for the study was collected between 2016 and 2020. The data was gathered mainly from interview

Table 1. Interview participants.

Interview Participants	Number
1. SSNIT's officers	
Project Manager, Operations Business Suite (OBS)	1
IT Manager, Communications & Networks	1
Biometric Registration Manager	1
Former Records Department Manager	1
Branch Office Manager	1
Benefits Coordinator	1
District IT Officer	1
Sub-total for SSNIT officers	7
2. SSNIT contributing members	6
3. Pensioners	6
4. Academic researchers	2
Total	**21**

participants and was complemented by participant observation and documentary sources. Interview participants were selected based on purposive and snowball sampling (Bryman, 2016). Table 1 shows a summary of the twenty-one interview participants.

As shown in Table 1, the interview participants were: seven (7) officials from SSNIT; six (6) contributing members of SSNIT— two from a public university, one from an NGO, one from an accounting firm, and two self-employed businesspersons; six (6) pensioners from a church; and two (2) academic researchers conversant with SSP services. The interviews were semi-structured and lasted between thirty (30) minutes and one hour. With participants' permission, interviews were tape-recorded and subsequently transcribed. Notes-taking complemented the interview recordings.

With participant's observation, the first author of this study had the opportunity to participate in SSNIT's biometric enrolment and was issued with a biometric smart card. The author also used a self-service biometric terminal at one of the branch offices to gain access and view his SSP information. The biometric terminal is a special ATM kiosk made up of a biometric reader for authenticating a user and a screen for viewing SSP information. Data was also gathered from publicly available information, including annual reports, press releases, and online feature articles. The documents helped to clarify and fill in information gaps from the interviews.

Data analysis

Data analysis was theory-driven. In line with the interpretive study principle of using theories as a sensitising device (Klein and Myers, 1999), the theory-driven analysis used the CIA triad model as themes to generate a theoretical understanding of the biometric system phenomenon. The results of the analysis is presented in the next section.

Results

In this results section, the CIA triad model presented in Section 3 is applied to explain how SSNIT's biometric system protects information for improved SSP service delivery. Figure 2 illustrates integration of the biometric system into SSNIT's information security architecture.

Availability

We start with availability because the other security attributes depend on it, i.e., without information availability, no other security attributes can be applied. Availability of SSP information concerns authorised, timely, and reliable access to SSNIT records. It took days to access SSP information in the pre-biometric era. With the biometric system, information is available to members right away and is more reliable than before. In the pre-biometric area, members' access to their SSP information took days because of inherent delays in authenticating for service (e.g. SSP claims, statements, or change of beneficiaries).

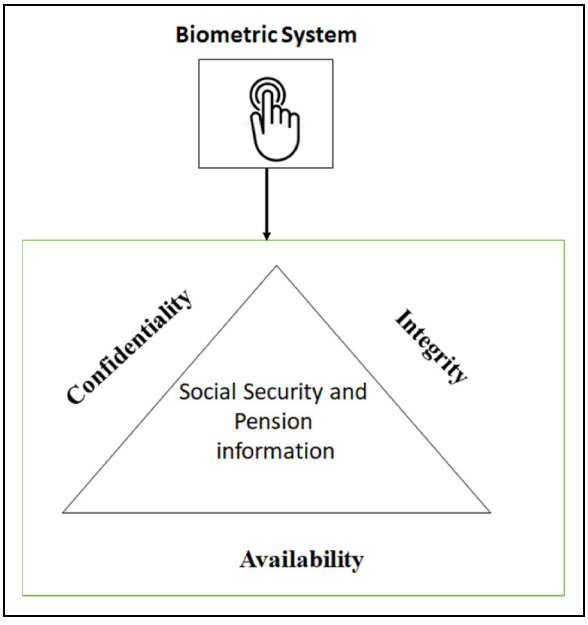

Figure 2. Biometric enabled access control to SSP information services.

During the pre-biometric era, members' service requests were initiated at a branch office, batched, and sent to the head office records department by a vehicle so that their identities could be authenticated. At the records department, members' files were retrieved based on their SSNs. Then, using a magnifying glass, a thumbprint authentication expert compared a member's thumbprint on file with the incoming thumbprint to confirm whether the social security number (SSN) belongs to the member or not. A match confirmed the identity of the member and SSN. The authentication results were then sent back by transport to the respective branches for the services to be provided. Thus, transactions took many days to process. For instance, the average processing time for the payment of benefits to claimants was over 40 days. A former records manager recounted the cause of the delays in information availability:

> The manual central authentication system delayed our processes. Assuming you initiated your claim at Lawra [a town in the northern region of the country], we couldn't start processing payment until you are confirmed as the owner of the number. [a former records manager]

The introduction of the biometric system improved information availability by enabling instant authentication at the service points. Typically, at the branch office, using a biometric card reader or a biometric terminal, a member is authenticated by inserting their smart card into the reader slot and then placing their fingers on the fingerprint scanner. A match between the stored fingerprint on card and live fingerprint confirms the identity of the member. At a biometric terminal, once authenticated, the member goes through various menus shown on the terminal screen to view his or her SSP information and services. A member worker gave his experience with the biometric terminal:

> I always wanted to check on contributions from my employer. So, this self-service ATM [i.e., biometric terminal] makes it easy for me to check on it regularly. It is convenient. [a member worker]

Using the biometric terminals, members could readily access their personal details, lodge complaints, view beneficiaries, view or print statements, and renew life certificates. These were information services that took days to accomplish without the biometric system. A biometric registration officer commented on the ease of use of the system.

> Now with the new system, the authentication has become more easier because now you don't need to send the request to a central point for the member to be authenticated… At the branch level you can tell this is the real owner of the number so whatever request he has is immediately attended to [biometric registration officer]

A benefits coordinator placed the time reduction in perspective with respect to claims lodgement.

> Processing of claims lodgement used to take about 40 days, but now it has been reduced to about 12 to 15 days. This performance is not attributed to the biometric alone but with the improvement of the entire system using the OBS [operation business suite SSNIT's enterprise system). [benefits coordinator].

A branch office manager mentioned the ease with which members, including pensioners, could access their information and services:

> With the former system, we had situations where over 72 year-olds will come to the office every three years to tell us they are still alive so that we can continue paying their pensions. Now with the biometric terminal that has been made easier. [branch office manager]

However, some pensioners were not enthused about the self-service biometric terminal.

> "…as for the biometric terminal I see it more as beneficial to them (i.e. SSNIT) than us (i.e. pensioners). For me, I will want to go to the branch and have my life certificate renewed." [a pensioner over 72 years]

> "I am not aware of such an ATM (i.e. biometric terminal). Even if I am, I will still go to the branch to be authenticated and have my certificate renewed. [another pensioner over 72 years].

Overall, the integration of the biometric system into SSNIT's services improved member information access by enabling authentication in real-time and timely service delivery.

Confidentiality

The confidentiality of SSP information ensures that members get to view their own SSP information. The biometric system enables SSNIT to maintain confidentiality of SSP information through biometric enrolment, identification, card issuance, and authentication processes. These biometric processes link

members' SSP information to their own biographic and unique biometric data. First, the biometric enrolment process establishes the identity of a person by validating and capturing members' biographic details: an applicant completes an enrolment form with his or her biographic data, including name, contact, birthdate, gender, and residential address. The accepted identification credentials for enrolment are birth certificates and national IDs. Date of birth as evidenced by a birth certificate, is a key requirement for enrolment. For applicants without any of these ID documents, a short interview is conducted, and a specially designed date of birth form is completed and thumb-printed with a declaration by applicant. After validation of applicant's biographic details, their biometric data is captured using a fingerprint scanner, digital camera, and signature pad. The biometric data captured during enrolment are ten (10) fingerprints and facial image, in addition to signature. A district IT officer responded to the question of how SSNIT handles instances where the fingerprints of applicants cannot be taken.

> We do have instances where some applicants' fingerprints cannot be used. This may be due to accidents or sick conditions like leprosy. In such cases, at least one good fingerprint can be used. However, if all ten (10) fingerprints cannot be used, the system tags the applicant or member as invalid in our records and only their pictures are taken. With such persons, their pictures and personal details on the card issued are used for identification. [district IT officer]

Second, the biometric identification process prevents multiple registration by a member and thereby ensures confidentiality of members' SSP information. The biometric identification process kicks in after the captured identity data at the enrolment point is transferred over the SSNIT's network links to the data centre. At the data centre, using applicants' biometric data, the backend AFIS server software automatically prevents multiple registrations by matching the presented fingerprint images with the already enrolled ones in the database. With the third process of card issuance, members receive their biometric smart cards within a month of enrolment. The biometric smart card is a chip-based card that shows identity information about the holder, i.e., SSN, picture, name, and date of birth. Two fingerprints miniature of the holder are also stored electronically on the card. The stored fingerprint on the card ensures that the card is not duplicated or shared, and the information remains confidential.

Fourth and finally, to maintain confidentiality, the authentication process ensures that members have exclusive access to their own SSP information after a correct match of the stored biometric data on the smart card and the live fingerprints.

Integrity

The integrity of members' SSP information concerns keeping accurate member identity and SSNIT records for benefits payments. An officer described the problem that SSNIT's information system in the pre-biometric era had in maintaining the integrity of members' SSP information:

> Our systems had outlived their usefulness and were very prone to fraud - you could easily manipulate data and the benefits a person was to collect. [a SSNIT officer]

The biometric enrolment and identification processes enhanced the integrity of members' identities and SSP information. With biometric identification (see details under the confidentiality attribute), the unique biometric data prevents instances of multiple SSNs per member. A former records manager provided insight into how the implementation of the biometric system improves data integrity:

> During the transition from the manual to the biometric system, we identified many multiple SSP records of members who had different dates of birth. The different dates of birth were the result of either multiple registrations from different employers or attempts to reduce age and delay retirement time. [a former records manager]

In line with the need to maintain information integrity, SSNIT did not opt for instant card issuance during biometric enrolments. Instead, applicants collect their biometric cards within a month after enrolment. The IT manager explained:

> We can do instant card issuance during enrolment. But then we need to validate the submitted biographic data on the enrolment forms, which means forgoing instant card issuance. Our operation is such that an error in your name, different dates of birth from different employers, for instance, can delay processing claims. Besides, it is important to double-check personal and employment details to avoid possible impersonation. [IT manager]

To ensure integrity, the biometric authentication (see Section 5.2) ensures that only authorised members can access and alter their SSP records. Members who want to update their SSP information need to be there in person with their biometric card at the service point. Information integrity is also maintained by requiring pensioners over 72 years of age to renew their life certificates annually to ensure that benefits are paid to the right persons. SSNIT's policy stops payments to pensioners who do not renew their life certificates because the assumption is that they have passed on. To renew a life certificate, a pensioner visits a branch office to be biometrically authenticated and is then issued with a life certificate for a year. For pensioners who, for health reasons, cannot visit the branch, SSNIT arranges to have them biometrically authenticated at their homes. A recent newspaper report (GraphicOnline, 2021) indicated SSNIT's plans to delete the names of more than 13,000 pensioners aged 72 and above from its payroll. According to the newspaper report, the affected persons had failed to renew their SSP certificates. The newspaper report further indicated that since 2018, SSNIT had saved about GH¢144 million (about one million dollars) by deactivating 11,478 SSP accounts that had not been renewed.

In summary, SSNIT's biometric system improves SSP services by instantly authenticating members to gain access (i.e. availability) to view their SSP information (i.e. confidentiality) and update their information (i.e. integrity) necessary for proper record-keeping and benefits payments.

Discussion

This section discusses the study's findings in relation to the research question on how a biometric system can improve SSP information security and service delivery. Overall, the study's findings show that using a biometric system to identify and authenticate SSP members can ensure information security through data availability, confidentiality, and integrity. In addition, the system can improve SSP services by reducing service delivery turnaround time and financial leakages. The detailed findings are discussed next.

Information confidentiality, integrity and availability

The study's findings show that the use of a biometric system can facilitate secure access to restricted information by ensuring its confidentiality. In this study, the SSNIT's biometric system ensures that members can access only their own SSP records. The confidentiality of one's SSP record is assured as the biometric authentication requires a member's presence (i.e. their unique live fingerprints), the member's smart card, and a biometric card reader or terminal at the service point.

Additionally, the study's findings indicate that the use of a biometric system can improve the integrity of restricted information by ensuring its accuracy. This study identified three ways in which SSNIT's biometric system improves the integrity of SSP records. First, the enrolment and identification processes contribute to maintaining the accuracy of personal identification information, which is critical for benefit payments. The unique biometric identification links a member to only one SSP record in the database. In the pre-biometric era, multiple SSP records with different SSNs were common, making the SSP system vulnerable to manipulation of benefit payments. Second, SSNIT's biometric authentication system requires members to be physically present with their smart card in order to access and update SSP information.

Thirdly, the biometric system is used to enforce annual life certificate renewals in order to ensure that benefits payments are made to pensioners who are alive. Additionally, smart ID cards are not issued instantly to allow for the validation of applicants' biographic details. This validation contributes to preventing impersonation and minimising errors in personal data.

Finally, the study demonstrates that the use of a biometric system can restrict information only to authorised users. In this study, it was found that the presence of a member with a biometric card at a service point equipped with biometric card readers or terminals ensures that SSP records are available to only authenticated members when needed and in a timely and reliable manner. With the biometric system, a member's identity is authenticated instantly at a service point, compared to the centralised manual system, which involved many days of waiting to be verified. The instant biometric authentication enables members to readily access their SSP information.

Overall, the study's findings affirm the information security literature's observation that a complete protection mechanism requires a combination of organisational and technical aspects (Alsmadi et al., 2018). For instance, in this study, the biometric system was

aligned to SSNIT's operational control of double-checking the accuracy of members' biographic details. As a result, SSNIT does not issue the biometric cards instantly to applicants during enrolment. Instead, the ID cards are collected by the newly enrolled members much later, within a month, to enable personnel to validate the accuracy of their biographic details. Another operational control was that pensioners over 72 years old are required to be biometrically authenticated annually to continue with benefits payments.

SSNIT's biometric system was deployed as part of an enterprise system implementation project. Therefore, the biometric system is not the only technical component that ensures confidentiality, integrity, and availability of restricted SSP records. This is because, as an access control system, a biometric system secures access to information on storage (Alsmadi et al., 2018). Since information security is not limited to information at rest but also information in transmission, biometric systems' protection needs to be complemented with technologies that secure information in transmission as shown in Table 2.

Table 2. Comparison of biometric system security to other technologies using the CIA triad model .

Information Security technologies	Application of CIA Triad	
	Information at rest	Information in motion
Access control systems		
Examples: • Biometric system • Password • Plain ID cards	A biometric system offers higher levels of confidentiality, integrity and availability compared to passwords and ID cards as this study shows.	Not applicable
Encryption technologies		
Examples: • Cryptography • Public key infrastructure	Confidentiality, integrity and availability (Alsmadi et al., 2018; Caballero, 2017; Els and Cilliers, 2017; Zhu and Sun, 2018)	
Intrusion mitigation technologies		
Examples: • Firewalls • Antivirus		Confidentiality, integrity and availability (Alsmadi et al., 2018)

Technologies such as cryptography, firewalls, and intrusion prevention systems, protect information during its transmission (Alsmadi et al., 2018; Sharma and Garg, 2017).

Cryptography technologies encrypt information (whether at rest or in transmission) by making it unreadable by unauthorised persons (Caballero, 2017; Els and Cilliers, 2017). Thus, sensitive data (such as a person's SSP record in this study), while being transmitted, could be encrypted in order to prevent unauthorised persons without a valid private key from seeing the content (Moriggl et al., 2021). In this wise, while a biometric system ensures authentic persons can access their SSP information on storage, cryptography technologies protect the confidentiality, integrity, and availability of content while traversing networks. Further, security threats such as denial of service are attacks on information availability (Alsmadi et al., 2018), which can prevent even authenticated biometric users from accessing their SSP records. In such cases, technologies such as firewalls, which block harmful network and application traffic (Caballero, 2017) can be used.

To conclude this section, using the CIA triad model and the foregoing discussion, we compare biometric system security to other security technologies identified in the literature.

As Table 2 shows, encryption technologies are the most basic technical means to protect information since they secure information in all its states (Alsmadi et al., 2018; Zhu and Sun, 2018).

Impact on service delivery

By improving SSP information security, a biometric system can improve service delivery in several ways. First, instant authentication of biometric data at service points reduces service turnaround time. As the study's findings demonstrate, incorporating biometric authentication into SSNIT's operations eliminated the number of days spent manually verifying a member's identity before providing a service. Also, the self-service biometric terminals or card readers at the branch offices enable members to readily view, update, and print account information. Also, the introduction of biometric systems into SSNIT's operations helped to reduce the claims processing duration from 40 to 15 days.

Second, a biometric system contributes to the integrity of SSP benefit payments by facilitating the

maintenance of accurate information. As the study's findings show, the unique biometric data of individuals prevents duplication of a member's SSP record. Comparatively, the manual system was prone to multiple SSNs with different birth dates per member. Also, the use of biometric-based life certificate renewal reduces the risk of paying pensions to pensioners who have passed on. Evidence from the study shows that SSNIT saved about 1 million dollars by deactivating accounts of those who had not renewed their life certificates. However, the annual life certificate renewals pose challenges to pensioners as they have to present themselves every year at a SSNIT office to renew their life certificates biometrically.

We conclude this section with the limitation of SSNIT's biometric system. Evidence from the study indicates instances where some individuals' fingerprints could not be used. This finding corroborates the literature on the limitation of unimodal biometric systems in excluding some segments of the population due to factors such as age and occupation (Jain et al., 2004; Uzoka and Ndzinge, 2009). In this study, photo authentication was therefore used for such exclusions, although they were rare. Multimodal biometrics such as the use of fingerprints and iris have been suggested as a solution for exclusions (Moses and Rowe, 2016). Alternatively, and perhaps a cheaper and effective option, is to use two-factor authentication by including a verification code sent via SMS to the registered phone of an individual (Moses and Rowe, 2016).

Conclusion

This study sought to understand how a biometric system can improve SSP information security and service delivery using the case of a government agency that administers SSP services in Ghana. The study's findings show that when biometric identification and authentication mechanisms are integrated into SSP service delivery, they can provide SSP information availability, confidentiality, and integrity and reduce service delivery turnaround time. In addition. the study also found that a biometric system can be used to enforce controls against fraudulent manipulations associated with service delivery. The study's findings also indicate that a biometric system alone cannot provide complete information security and should therefore be complemented with other technologies such as cryptography and firewalls.

The study contributes to research, practice, and policy. For research, this study provides in-depth insights into studying biometric systems as information security models for service improvements. In terms of theory, this is the first study to apply the CIA triad model to the study of biometric systems, thereby enhancing the model's utility and our understanding of biometric systems. For practice and policy, this study provides rich insights into how biometric systems can protect restricted information and enhance service delivery using the case of SSP services.

Implications for research

Developing country IS literature on biometric systems has focussed on their role in socioeconomic development (Effah et al., 2020; Effah and Debrah, 2018; Masiero, 2018; McGrath, 2016; Owusu-Oware et al., 2018). However, using the CIA triad model, this study has given attention to the need to examine biometric systems for information security and service improvement in the domain of SSP services. Future studies can also apply CIA triad or the expanded model C-I-A-N-R (Confidentiality, Integrity, Authenticity, and Non-Repudiation) in other biometric application domains.

Implications for practice and policy

The study's findings show the need for practitioners and policymakers to align deployment and use of biometric systems with domain application needs. As the study findings show, SSNIT chose to validate identity data during enrolments at the expense of instant card issuance. In other domain applications, such as health insurance, biometric enrolment is accompanied by instant card issuance because members need to access health services as soon as possible (see Owusu-Oware et al., 2018). Also, the study's findings affirm that a biometric system is limited in covering all individuals. As discussed in the study, either multimodal biometric systems are used or the cheaper option of multifactor authentication involving photoID and SMS code validation is employed. Further, in this study, the biometric system was used to enforce annual life certificate renewals to reduce payments to wrong persons. Some of the pensioners were not enthused by the biometric terminals – they preferred to deal with the branch officers directly. SSP policymakers need to consider the inconveniences such policies cause the aged. Consideration may be given to authenticating pensioners aged over 72 years at their homes at additional fees which may be subsidised by government. On the other hand, for practitioners,

especially manufacturers, there is the need to design systems to cater for the aged.

Limitations of research

The findings from the study are limited by the single experience of a developing country government agency and the domain of SSP services. However, in line with interpretive studies, the findings can be applied to other developing countries with similar context as well as other domains such as payroll and health insurance. Also, the study did not delve into the enterprise system which underpinned SSNIT's digitalisation effort with the biometric system as a subcomponent. Our understanding of the CIA triad can further be enhanced if the enterprise system in conjunction with the biometric system is examined in a future study.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD


Emmanuel Owusu-Oware https://orcid.org/0000-0001-6119-0790

References

Alsmadi I, Burdwell R, Aleroud A, et al. (2018) Introduction to information security. In: *Practical Information Security*. Cham: Springer, 1–16.

Asani EO (2014) A review of trends of authentication mechanisms for access control. *Computing, Information Systems, Development Informatics & Allied Research Journal* 5(2): 1–12.

Beynon-Davies P (2007) Personal identity management and electronic government: The case of the national identity card in the UK. *Journal of Enterprise Information Management* 20(3): 244–270.

Bhaharin SH, Asma'Mokhtar U, Sulaiman R, et al. (2019) "Issues and trends in information security policy compliance", 2019 *6th International Conference on Research and Innovation in Information Systems (ICRIIS)*, IEEE, pp. 1–6.

Bhardwaj A, Avasthi V and Goundar S (2019) Cyber security attacks on robotic platforms. *Network Security* 2019(10): 13–19.

Briggs P and Thomas L (2015) An inclusive, value-sensitive design perspective on future identity technologies. *ACM Transactions on Computer-Human Interaction* 22(5): 1–28.

Bryman A (2016) *Social Research Methods*. Oxford, UK: Oxford university press.

Caballero A (2017) Information security essentials for information technology managers: Protecting mission-critical systems. In: *Computer and Information Security Handbook*, Morgan Kaufmann, 393–419.

Cavusoglu H, Cavusoglu H, Son JY, et al. (2015) Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management* 52(4): 385–400.

Dorfman M and Palacios R (2012) World Bank Support for Pensions and Social Security, available at: http://ideas.repec.org/p/wbk/hdnspu/70925.html.

Effah J and Debrah E (2018) Biometric technology for voter identification : The experience in Ghana. *The Information Society* 34(2): 104–113.

Effah J, Owusu-Oware E and Boateng R (2020) Biometric identification for socioeconomic development in Ghana. *Information Systems Management* 37(2): 136–149.

Els F and Cilliers L (2017) "Improving the information security of personal electronic health records to protect a patient's health information", 2017 *Conference on Information Communication Technology and Society (ICTAS)*, IEEE, pp. 1–6.

GraphicOnline (2021) SSNIT to delete 13,000 names from pensioners payroll", available at: https://www.graphic.com.gh/news/general-news/ssnit-to-delete-13-000-names-from-pensioners-payroll.html (accessed 15 July 2021).

He W, Yuan X and Tian X (2014) "The self-efficacy variable in behavioral information security research", 2014 *Enterprise Systems Conference*, IEEE, pp. 28–32.

Jain A and Nandakumar K (2012) Biometric authentication : system security. *IEEE Computer* 45(11): 87–92.

Jain A, Ross A and Prabhakar S (2004) An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology* 14(1): 4–20. IEEE.

James TL, Khansa L, Cook DF, et al. (2013) Using network-based text analysis to analyze trends in microsoft's security innovations. *Computers & Security* 36: 49–67.

Jayabalan M and O'Daniel T (2017) Continuous and transparent access control framework for electronic health records: A preliminary study", 2017 *2nd International Conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, IEEE, pp. 165–179.

Klein HK and Myers M (1999) A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly* 23(1): 67–94.

Lips M (2010) Rethinking citizen–government relationships in the age of digital identity: insights from research. *Information Polity* 15(4): 273–289.

Lumini A and Nanni L (2017) Overview of the combination of biometric matchers. *Information Fusion* 33: 71–85.

Marutha N (2020) Medical records preservation strategies in improving healthcare service providers' access to patients' medical histories in the Limpopo hospitals, South Africa. *Information Development* 36(1): 174–188.

Masiero S (2018) Explaining trust in large biometric infrastructures: A critical realist case study of India's Aadhaar project. *The Electronic Journal of Information Systems in Developing Countries* 84(6): 1–15.

McGrath K (2016) Identity verification and societal challenges: explaining the gap between service provision and development outcomes. *MIS Quarterly* 40(2): 485–500. Brunel Univ, Dept Comp Sci, Uxbridge UB8 3PH, Middx, England.

McGrath K and Maiye A (2010) The role of institutions in ICT innovation: Learning from interventions in a Nigerian e-government initiative. *Information Technology for Development* 16(4): 260–278.

Moriggl P, Asprion PM and Schneider B (2021) Blockchain technologies towards data privacy—hyperledger sawtooth as unit of analysis. In: *New Trends in Business Information Systems and Technology*. Cham: Springer, 299–313.

Moses S and Rowe DC (2016) Physical security and cybersecurity: reducing risk by enhancing physical security posture through multi-factor authentication and other techniques. *International Journal for Information Security Research (IJISR)* 6(2): 667–676.

Mwantimwa K (2019) Use of mobile phones among agro--pastoralist communities in Tanzania. Information development. *Information Development* 25(2): 230–244.

Myers M (2013) *Qualitative Research in Business & Management* (N. S. Kirsty Smy (ed.), 2nd ed.). London: Sage Publications.

Neumann AJ, Statland N and Webb RD (1977) Post-processing audit tools and techniques. In: *Proceedings of the NBS Workshop*, pp. 36–341.

Ogbanufe O and Kim DJ (2018) Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment. *Decision Support Systems* 106: 1–14.

Owusu-Oware E, Effah J and Boateng R (2018) "Biometric technology for fighting fraud in national health insurance: Ghana's experience", *Americas Conference on Information Systems 2018: Digital Disruption, AMCIS* 2018.

Oyediran-Tidings SO, Nekhwevha FH, Ondari-Okemwa EM, et al. (2021) Access to educational information enabled by ICT tools in the Fort Beaufort Education district (FBED), Eastern Cape, South Africa. *Information Development* 37(3): 402–416.

Panchiwala S and Shah M (2020) A comprehensive study on critical security issues and challenges of the IoT world. *Journal of Data, Information and Management* 2(4): 257–278.

Parker D (2010) Our excessively simplistic information security model and how to fix it. *ISSA Journal* 8: 12–21.

Parks RF and Mead EL (2014) A socio-technical approach to biometric technology deployment in schools", *20th AMCIS* 2014, Georgia, USA.

Posey C, Raja U, Crossler RE, et al. (2017) Taking stock of organisations' protection of privacy: categorising and assessing threats to personally identifiable information in the USA. *European Journal of Information Systems* 26(6): 585–604.

Qadir S and Quadri SMK (2016) Information availability: An insight into the most important attribute of information security. *Journal of Information Security* 7(3): 185–194.

Ramona C (2009) Budgetary means to ensure a decent living standard. The national social security system. In: World Scientific and Engineering Academy and Society (WSEAS) (ed.) *Proceedings of the 8th WSEAS International Conference on E-Activities and Information Security and Privacy*. Puerto De La Cruz: World Scientific and Engineering Academy and Society (WSEAS)Stevens Point, pp. 228–233.

Rao UH and Nayak U (2014) Physical security and biometrics. In: *The InfoSec Handbook*. Apress, Berkeley, CA, 293–306.

Roy S, Matloob S, Seetharam A, et al. (2017) Biometrics data security techniques for portable Mobile devices. *Inae Letters* 2 (3): 123–131.

Safa NS (2017) The information security landscape in the supply chain. *Computer Fraud & Security* 2017(6): 16–20.

Saltzer JH and Schroeder MD (1975) The protection of information in computer systems. *Proceedings of the IEEE* 63(9): 1278–1308.

Samonas S and Coss D (2014) The CIA strikes back: redefining confidentiality, integrity and availability in security. *Journal of Information System Security* 10(3): 21–45.

Sharma M and Garg RB (2017) LIE-Let it encrypt: An encryption algorithm meant for secure transactions. *International Journal of Engineering and Applied Sciences* 4(5): 257471.

SSNIT (2021) "SSNIT - About Us", *Ssnit.Org.Gh*, available at: https://www.ssnit.org.gh/about-us/#:~:text= The Pension Scheme as administered,their monthly pensions from SSNIT (accessed 12 June 2021).

Thomborson C (2010) A framework for system security. In: *Handbook of Information and Communication Security*. Berlin, Heidelberg: Springer, 3–20.

Uzoka FME and Ndzinge T (2009) "Empirical analysis of biometric technology adoption and acceptance in Botswana", *Journal of Systems and Software*. *Elsevier Inc* 82(9): 1550–1564.

Walsham G (2006) Doing interpretive research. *European Journal of Information Systems* 15(3): 320–330.

Warkentin M and Orgeron C (2020) Using the security triad to assess blockchain technology in public sector applications. *International Journal of Information Management* 52(January 2019): 102090. Elsevier.

Whitley E, Gal U and Kjaergaard A (2014) Who do You think You are? A review of the Complex interplay between information systems, identification and identity. *European Journal of Information Systems* 23(1): 17–35. Nature Publishing Group.

Whitman ME (2003) Enemy at the gate: Threats to information security. *Communications of the ACM* 46(8): 91–95.

Yadav AK and Tadisetty S (2012) Iris based De-duplication technology. *IJERA* 2 (1): 164–167.

Yang W, Wang S, Hu J, et al. (2019) Security and accuracy of fingerprint-based biometrics: A review. *Symmetry* 11: 2. available at:https://doi.org/10.3390/sym11020141.

Zafar H and Clark JG (2009) Current state of information security research in IS. *Communications of the Association for Information Systems* 24(1): 34.

Zhu C and Sun K (2018) Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps. *IEEE Access* 6: 18759–18770.

Zviran M and Erlich Z (2006) Identification and authentication: technology and implementation issues. *Communication of the Association for Information Systems* 17(Article 4): 90–105.

About the authors

Emmanuel Owusu-Oware is a senior lecturer at the University of Professional Studies, Accra. Emmanuel holds a PhD in Information Systems from the University of Ghana, MBA in Management Information Systems from the University of Ghana and Vrije Universitéit Brussels, and BSc in Electrical and Electronic Engineering (Telecommunications Major) from Kwame University of Science and Technology. His research interests are in public-sector biometric systems and generally digital innovations in the public and private sectors. He is also an information systems practitioner with many years of working experience in IT management and consulting in the public and private sectors of developing countries.

John Effah is an Associate Professor of Information Systems at the University of Ghana. His research interests span areas of digital innovation in business, government and society as well as biometric systems in developing countries. John holds a PhD in information systems from the University of Salford in Manchester, UK and MBA MIS and BSc in Business Administration (Accounting Option) with First Class Honours both from University of Ghana. John serves on the editorial boards of Electronic Journal of Information Systems in Developing Countries and African Journal of Information Systems as a Deputy Editor-in-Chief. He is also an ICT consultant.