International Journal of Humanities and Social Science Invention (IJHSSI)
ISSN (Online): 2319 – 7722, ISSN (Print): 2319 – 7714
www.ijhssi.org ||Volume 10 Issue 12 Ser. II ||December, 2021 || PP. 17-28

The South African Criminal Justice System: Identifying the challenges of the Information and Communication Technologies

Solani Isaac Mthombothi
(Gauteng Department of Community Safety)
Corresponding Author: Solani Mthombothi

Abstract
The South African Criminal Justice System (CJS) has developed systems for registering the Identity of citizens, investigating crime, prosecuting offenders, case flow management, tracking, profiling offenders and keeping them in correctional facilities amongst other functions. These CJS information technology systems include the Department of Home Affairs National Identification System (HANIS) and the National Immigration Information System (NIIS) used for keeping records of Immigrants as well as the Automated Fingerprints Identification System (AFIS). The aim of this article was to identify the challenges experienced by the Department of Home Affairs (DHA) and the CJS on the newly implemented Information and Communication Technologies (ICT). Furthermore, this process will help in assisting to assess whether these systems are effective and efficient. The Department of Home Affairs as an integral part of the government system also formed part of the study. Furthermore, this article looked at the process of integration of information from end-to-end amongst these CJS agencies and the full utilisation of the IT systems named in the background section. The South African CJS implemented electronic ICT systems for their core functions and other systems used in and out of office.

Method: *The study utilised a qualitative research method to collect data. The qualitative research method included semi-structured interviews (open-ended questions) with officials in various Criminal Justice System (CJS) institutions and ICT experts in Gauteng. Respondents were sampled using the non-probability sampling technique, known as purposive sampling and data was analysed thematically. Data was collected from 46 respondents from the CJS and experts. The study realised a lot of challenges with these systems and the poor utilisation thereof by the intended users. The challenges identified by this study will hamper the process of fully integrating these ICT systems and sharing information amongst the CJS agencies. The study results revealed that most of the systems are not operating as envisaged by the said agencies and the use of paper is still dominant in the DHA and CJS fraternity. Ultimately, the drawn conclusion is that the CJS information and technology systems are not effective and efficient.*

Keywords: Criminal Justice System; Information and Communication Technology and Integration

---

Date of Submission: 08-12-2021 Date of Acceptance: 23-12-2021

I. INTRODUCTION

The Criminal Justice System (CJS) globally, especially the police now utilises technology to perform their core function as mandated by their constitutions (OSCE, 2009, Avalos, 2016 & IACP, 2014). The Department of Home Affairs (DHA) as an integral part of the South African CJS has joined the global quest to use Information Technologies (IT) (DHA, 2019a). The effectiveness of these technologies of the CJS Information and Communication Technologies (ICT) to fight crime is more important considering the high level of crime in countries worldwide (World Crime Review, 2021). The Information and Communication Technologies are used to investigate crime, mobilise community, process and file documents by these CJS agencies Justice departments as well as correctional services departments (Avalos, 2016).

The SAPS use the Integrated Case Docket Management System (ICDMS) and AFIS, the National Prosecuting Authority (NPA) utilises the Electronic Case Management System (ECMS) whilst the Department of Justice and Constitutional Development (DoJ&CD) employs the Integrated Case Management System (ICMS) and Audio-Visual Remand (AVR) System. The Department of Correctional Services (DCS) uses the Integrated Inmate Management System (IIMS) (DCS, 2018, SAPS, 2016; NPA, 2017; DoJ&CD, 2017 & DCS, 2018). All these systems are to be integrated into a single view that enables the systems to be interlinked from end-to-end (from the DHA to the Correctional facilities) through the CJS value chain (DoJ&CD, 2017).

II. AIM OF THE ARTICLE

The aims of this article are to identify the existing gaps and challenges of the Information and Communication Technology (ICT) in the Criminal Justice System of Gauteng and South Africa. Furthermore, the article will assess whether these ICT systems are efficient and effective, as well as integrated as envisaged by the Integrated Justice System (IJS) programmes.

III. OBJECTIVES OF THE STUDY

- To identify the ICT systems utilised by the DHA and the CJS
- To identify the gaps and challenges of these ICT systems
- To determine the level of integration amongst these systems
- To conclude whether these ICT systems are effective and efficient

IV. RESEARCH QUESTIONS

- Which ICT systems are being utilised by the DHA and the CJS?
- What are the existing ICT challenges that are being experienced by the DHA and the CJS?
- What is the level of integration between the criminal justice ICT systems?
- Is the criminal justice ICT systems effective and efficient?
- Is the Integrated Justice System programme a success?

V. LITERATURE REVIEW

This section outlines the account of the documents consulted and analysed in order to identify the functions, challenges, and integration status of the DHA and the criminal justice ICT systems.

5.1 The Department of Home Affairs as an integral part of the CJS

The Department of Home Affairs (DHA) is the most integral part of the CJS because it is mandated to manage the population and civil register of South Africans and immigrants, manage international migration, visitors, the asylum seekers and refugees (DHA, 2019a). These include keeping the unique identity (fingerprints) and civic and immigration status of every citizen globally and every person who has been on South Africa's territory (DHA, 2019a). The identity (including fingerprints) and status of the individuals assist the police and other CJS agencies to identify an offender or suspects appearing in court and those in custody (DHA, 2019a).

Since 2000, the DHA utilised the electronic National Population and Identification System called Home Affairs National Identification System (HANIS) which replaced the old paper system of capturing citizens' identity information manually (DHA, 2019a). The benefits of the HANIS system are that it ensures real-time processing, verification, and accessibility for every new and existing fingerprint (DHA, 2019a). The HANIS system reduces identity fraud and assists in the quick manufacturing of identity documents for SA citizens (DHA, 2019a). The HANIS has a Verification Service which is an online service that provides banks with the opportunity to verify certain information of a client and securely store the information (PMG, 2012; DHA, 2019a & SABRIC, 2020). The HANIS system enables banks and other institutions to manage their security effectively (DHA, 2019a). The DHA also had a plan in 2018 to replace HANIS with the new Automated Biometric Identification System (ABIS) but it never materialised (DHA, 2019a). The ABIS is capable to consolidate other departmental environments such as the National Immigration Information System (NIIS); Multi-modal biometrics; consolidate databases into a single platform and consolidate all stand-alone systems on a standardized platform (Pillay, 2018). Furthermore, the DHA modernization programme was intended to replace the HANIS and probably ABIS with the National Identity System (NIS) (DHA, 2019a).

The NIS as a single view can integrate all (ABIS, NIIS, Permitting System, Movement Control system and the Enhanced Movement Control System) with the DHA systems (DHA, 2019b). In March 2019, the Minister of Home Affairs indicated that ABIS has been installed and fully operating (DHA, 2019a). However, systems like ABIS and NIS were never implemented (DHA, 2019a). In the 2016/2017 financial year, the DHA implemented the Enhanced Movement Control System (EMCS) to enable the capturing of biometric data (fingerprints and facial) of all travellers who entered or exited South Africa legally through all SA's ports of entry (DHA, 2018).

5.1.1 Integration of DHA ICT systems

The DHA also envisaged the integration of its ICT with other government departments and institutions such as health facilities and Law Enforcement Agencies to verify individual or applicant's information through their technologies such as HANIS, AFIS, EMCS as well as NIS (DHA, 2019b).

5.1.2 The DHA challenges with the ICT systems

The HANIS system has experienced massive technical glitches such as the imminent collapse of the over 20-year old biometrics database that was no longer providing adequate service (DHA, 2019a). The NIIS, NPR, Permitting System, the MCS, and EMCS were not at the time of the study integrated and adequately secured (DHA, 2019a). The HANIS is manually operated and is outdated and the software could run only on the specific (product locked) equipment, needs upgrades (DHA, 2019a). Additionally, HANIS could only be maintained by the contracted AFIS supplier (DHA, 2019a). The DHA experiences a huge flow of asylum seekers. These flows resulted in the small asylum system being overwhelmed by economic migrants claiming asylum (DHA, 2019a). The Home Affairs White Paper (2019) indicated that the front-line offices are still battling to utilise digital services at Provincial, large, medium and small offices within municipal boundaries due to poor network and lack of infrastructure (DHA, 2019c). Renting almost all offices became a challenge since the DHA cannot digitise these offices with relevant ICT systems (DHA, 2019b).

During the time of the study, the real situation was that the DHA still operates on a mixed model consisting of paper or manual applications and digital systems for providing smart identity cards and passports in provincial offices within municipalities (DHA, 2019b). The Department of Home Affairs' irregular issuing of documents has put the country at a greater risk of sovereignty since it cannot account for the number and identity of people staying, entering and leaving the country (DHA, 2019a & OSCE, 2009). The DHA's irregular issuing of documents (identity and status) also put the country at risk of national security, migration management – ports of entry, safety and security of citizens and functions of other CJS agencies (Africa Portal, 2006; DHA, 2019a & OSCE, 2009).

5.2 The South African Police Service (SAPS)

The SAPS embarked on utilising digital smart policing and communication technologies to solve crimes, locate perpetrators, investigate crime, crime scene management, protect victims, and ensure successful prosecution (ICAP, 2014, Avalos, 2016 & SAPS, 2017). Smart policing refers to the use of an array of new mobile and stationary technologies like software, hardware and communications networks to fight crime (GDCS, 2016). The quest for sophisticated technologies is not only to keep up with criminals and wrongdoers but stay well ahead of them (Avalos, 2016 & IACP, 2014).

5.2.1 The SAPS migrated from the old CAS to the new ICDMS ICT system

The SAPS implemented the electronic Investigation Case Docket Management System (ICDMS) to replace the old Crime Administration System (CAS) which was used manually to register, manage, control and keep records of opened and reported case dockets at their police stations (SAPS, 2015). The hard copies of the case dockets were scanned and stored electronically into CAS (SAPS, 2015). Thereafter, these case dockets were sent manually (as hard copies) to the NPA prosecutors or courts for adjudication (SAPS, 2015). The ICDMS is used to electronically report and capture investigated cases on the SAPS's computer system and has improved the management and administration of case dockets as well as curb loss and theft of dockets (SAPS, 2015). The e-docket is only available to stations with network infrastructure, while some of the stations still utilise CAS, or both CAS and ICDMS (SAPS, 2013). The SAPS envisaged the full implementation of the ICDMS by 2020, by then, all resources staff will be trained (SAPS, 2013). The three million old case dockets information was scanned into ICDMS (SAPS, 2013).

5.2.2.1 The capabilities and advantages of the ICDMS

The SAPS indicated that the ICDMS is divided into two functions: (1) The Case Administration Section and (2) the Investigate Case Section (SAPS, 2015). Additionally, the ICDMS allows officers and detectives to create e-dockets that would also be connected to the courts (SAPS, 2015). The ICMDS is utilised by the SAPS management, operational and support level and includes the Technical Management System, Supply Chain Management, the Detective Service and can be utilised by other government departments and external service providers (SAPS, 2015). The ICDMS prevents the most common practice by the SAPS of losing and theft of case dockets (SAPS, 2015). The web-based ICDMS can integrate with other SAPS systems such as Vehicle circulation, Criminal Information System (CRIM) / National Photo Identification System (NPIS), Scanners and other SAPS information systems (SAPS, 2015). The Investigation diary can be completed and the contents of the statement can be captured electronically on the ICDMS (SAPS, 2015). The ICDMS provides a single view and updates functionality (SAPS, 2016). Additionally, the system automatically determines if updates are allowed by an authorised user or not – is fully secured (SAPS, 2015). The ICDMS can ensure that complainants are kept informed of the progress of a criminal investigation (SAPS, 2015).

5.2.2.2 Challenges associated with the ICDMS

The SAPS encountered some security concerns when utilising the ICDMS. The system is often confusing different fields, for example, information of police stations would be mixed with the nature of offences (PMG, 2010). The system creates duplicate files and sometimes hides certain fields (PMG, 2010). When the case docket is registered, the ICDMS issues case numbers without following a chronological order, as a result, there would be empty files and the system would still request that they be scanned (PMG, 2010). The system is very slow; the slowness of the system is caused by data lines. To resolve this slowness, the network needs to be upgraded to improve the bandwidth.

5.3 The Electronics Case Management System of the National Prosecuting Authority

The NPA as part of the CJS is currently utilising the Electronics Case Management System (ECMS) to collaborate with private and public sectors (NPA, 2014). The collaboration includes critical partners and stakeholders such as the Financial Intelligence Centre (FIC), the South African Reserve Bank, Special Investigating Unit (SIU), Crime Intelligence, State Security Agency (SSA), the South African Revenue Service (SARS), various state departments, non-governmental agencies and the community to win the war on crime (NPA, 2014). The NPA National server memory and all servers and networks were upgraded to accommodate the new ICT systems (NPA, 2008). The new ICT systems are encrypted further enhancing security and improving efficiency, the ECMS is a secure, portal environment (NPA, 2008).

The NPA uses the ECMS to capture all the case docket information to the Operations Management System (OMS), manage cases and case information electronically with other CJS agencies (ICDMS, ICMS, IMMS) through their respective systems (NPA, 2008). The ECMS allows the community to have access to justice information and also allows the prosecutors and Investigating Officers to share case docket information (NPA, 2014). The ECMS also shares information and documents during relevant forums like, for example, the Case Flow Management (CFM) Forums (NPA, 2017). The Case Flow Management forum is where the ECMS and ICMS of the DOJ play a major role in the management of case dockets in court, as well as sharing of information, exchange of documents (with the private and public sector) and e-filing (NPA, 2017). The court clerks and data capturers (clerks) utilise ECMS to capture and record all information and formal documentation related to a case (NPA, 2017). Prosecutors can screen and update charge sheets, enroll cases, attach appropriate annexures and create a court roll through the ECMS (NPA, 2017). The ECMS provides case/investigation diary functions that are linked to tasks in Electronic Document and Records Management - EDRMS[1] (NPA, 2008).

5.4 The Department of Justice and Constitutional Development (DoJ&CD)

The Department of Justice and Constitutional Development (DoJ&CD) through its sub-branch “Court performance” is responsible for developing and monitoring processes and systems in courts (Government of South Africa, 2020). The DoJ&CD facilitates and runs case-flow management among others through the Court Efficiency Directorate which is supported by the Integrated Case-Flow Management (CFM) (Government of South Africa, 2020). These functions required the DoJ&CD to develop ICT tools and systems and support initiatives for the effective management of court records (Government of South Africa, 2020). The DoJ&CD performs its functions in conjunction with the judiciary, prosecuting authority and the various role players such as SAPS, Social Development, Correctional Services and legal representatives (Government of South Africa, 2020).

5.4.1 The Integrated Case Management System of the DoJ & CD

The DoJ & CD’s Integrated Case Management System (ICMS) was implemented in 2013 to support case-flow management in the South African Courts (DoJ&CD, 2018). The ICMS captures court information that is received from the prosecutors and the judiciary, this includes case numbering, information warehousing and scanning documents, case dockets and case files (e-filing) among others (PMG, 2009). The ICMS is used to track down all criminals from the time the data is entered on the court roll until the departure from the court system (PMG, 2009). The ICMS Web Portals are also used in the Masters’ and magistrate’s offices in the country as deceased estate service points (DoJ&CD, 2018). The ICMS has been improved to add more data elements to give a full representation of how the courts are performing in the country (DoJ&CD, 2018).

The DoJ&CD utilizes the Audio-Visual Remand System (AVR) which is used to link magistrate’s courts to correctional detention centres via closed-circuit television so that the accused in correctional facilities

[1] EDRMS is defined as an automated, electronic document and records management system that enables organisations to manage unstructured information captured in paper and electronic formats, such as emails, word processed and spreadsheet contents (Joseph, 2010).

do not appear in court (CCTV) (DoJ&CD, 2018). The AVR system is used during remands in order to save time transporting inmates and minimising flight risks (DoJ&CD, 2018).

5.5 The South African Department of Correctional Service

The correctional facilities in South Africa (SA) are faced with challenges of safety and security, the cost and efficiency of the transfer of remand inmates, monitoring of gangs and contrabands, over-crowding, allegations of torture and abuse, by both other inmates and staff, and the postponements of cases which increased the flight risk (PMG, 2016). The need to utilise ICT systems that can manage these correctional facilities is a priority and this led to the implementation of the Integrated Inmate Management System (IIMS) (Avalos, 201 & IACP, 2014).

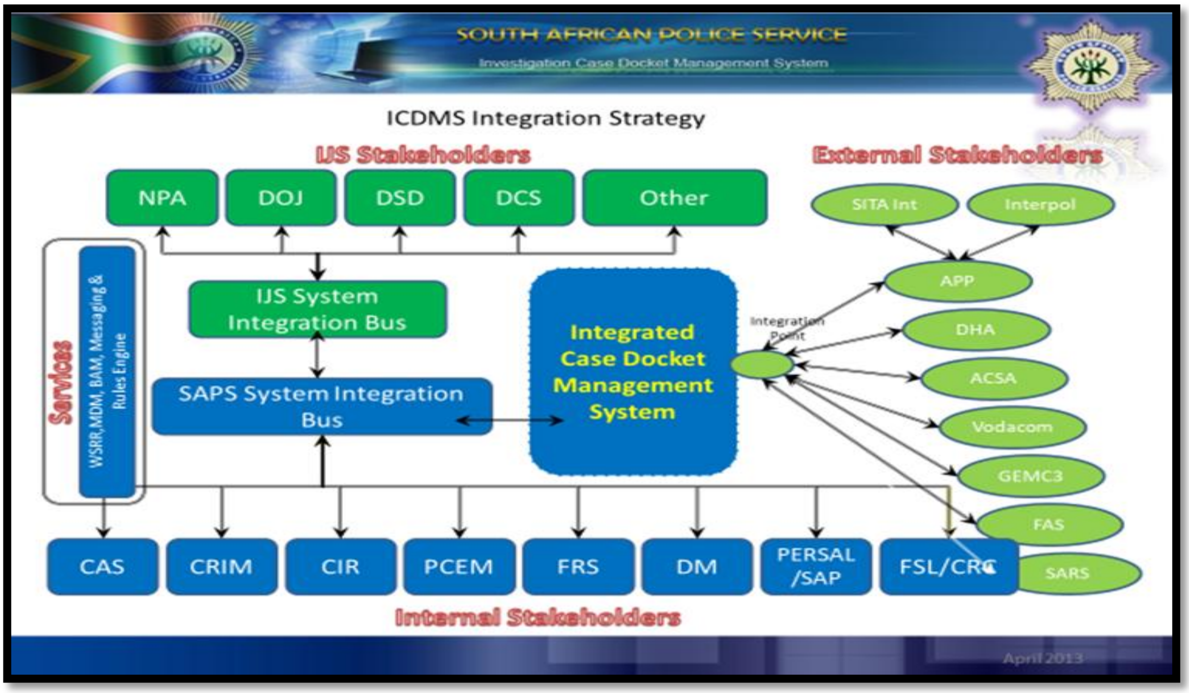
5.5.1 The Integrated Inmate Management System (IIMS)

In 2018, the DCS first implemented the Integrated Inmate Management System (IIMS) as a pilot project at Kgosi Mampuru, Middleburg, Carolina and Johannesburg Female Correctional facilities to capture the offenders and the inmate's information (DCS, 2018). The electronic IIMS replaced the manual performance of the DCS's three main streams of the core business which are remand detention, incarceration and corrections and social reintegration (South African Yearbook, 2017). The IIMS is the single (only centralised place) view of consolidated data and information of all inmates, parolees, probationers and offender registration (PMG, 2016). The IIMS national database does many activities which include biometric identification technology to capture fingerprints during admission and be utilised through the life cycle of incarceration, including attendance of programmes and/or any movement within the justice system and Home Affairs (DCS, 2018).

The IIMS can determine the number of people, age-group and gang-affiliation in all cells as well as a display of the number of beds per cell to make it possible to calculate over-crowding in all facilities (South African Yearbook, 2017). The DCS also intends to provide skills, education and rehabilitation programmes for inmates through the functions of the IIMS (South African Yearbook, 2017). During the time of the study, the pilot project was incomplete and most of the correctional facilities still did all the core functions manually (South African Yearbook, 2017). The IT modernisation project in the DCS includes the Remand Detainee Offender Management System (RDOMS) related dispute, inmate management and contract investigations (PMG, 2016). Besides the IIMS, the DCS also implemented the Electronic Monitoring System (EMS) to track an offender or a person awaiting trial on a 24-7-365 basis with body-scanning equipment, Cellphone detection systems, the Automated Fingerprint and Identity System (AFIS) and Automated Personal Identity System (South African Yearbook, 2017). These systems interface with the Department of Home Affairs' database to verify the identity of offenders (South African Yearbook, 2017).

5.6 INTEGRATION OF THE CJS ICT SYSTEMS

Figure 1: The envisaged Integrated Justice System plan of South Africa's Doj&CD


SOUTH AFRICAN POLICE SERVICE
Investigation Case Docket Management System
ICDMS Integration Strategy
IJS Stakeholders
External Stakeholders
NPA
DOJ
DSD
DCS
Other
SITA Int
Interpol
APP
DHA
ACSA
Vodacom
GEMC3
FAS
SARS
Services
WSRR,MDM, BAM, Messaging & Rules Engine
IJS System Integration Bus
SAPS System Integration Bus
Integrated Case Docket Management System
Integration Point
CAS
CRIM
CIR
PCEM
FRS
DM
PERSAL /SAP
FSL/CRC
Internal Stakeholders
April 2013

The Department of Justice and Constitutional Development 2017

Figure one (1) illustrates the proposed IJS programme, plan, value chain and the interlink of the CJS agencies and other public and private sectors in South Africa.

VI. RESEARCH METHODOLOGY

The study utilised a qualitative research method including semi-structured interviews to collect data. This research method included both primary (interviews) and secondary (desktop) research techniques. The data collection instruments utilised open-ended questions to allow participants to provide answers in their own words.

VII. SAMPLING PROCEDURE AND SIZE

The study made use of the non-probability sampling technique, known as purposive sampling where the selected participants have ample knowledge and experience on the topic (Creswell & Clark, 2011 cited by Palinkas et al, 2015). A breakdown of participants and sample size is as follows: Department of Justice and Constitutional Development (14); Department of Correctional Services (5); Department of Home Affairs (6); NPA (7), SAPS (12), and Council for Scientific and Industrial Research (CSIR) (2). The total proposed sample size for the research was (30) but a total of 46 formed part of the total number of respondents.

VIII. DATA ANALYSIS

Data analysis included transcribing respondents' narratives verbatim, research reports and observations which were considered more valuable or informative to the topic. Thematic analysis was used for data analysis. Open coding was first used to isolate the data into distinct sections, which enabled the researcher to identify differences and similarities (Saldaña, 2009). The second approach was pattern coding which allowed the researcher to identify common themes (Miles & Huberman, 1994). In this process, the themes, inter-related themes, or perspectives were the findings or results that provided answers to the research question.

IX. ETHICAL CONSIDERATIONS

The proposed research project was implemented in accordance with accepted ethical guidelines subsuming anonymity, confidentiality and dignity of participants which was protected. No direct attempts were made to implicate or incriminate any participants. Participants were informed about the purpose and nature of the study, in addition to the intentions of the researcher with respect to the information.

X. FINDINGS OF THE RESEARCH STUDY

10.1 The Department of Home Affairs ICT systems

The Department of Home Affairs (DHA) respondents indicated that their office is the custodian of the population register of all registered South Africans with identity documents (ID), birth and death certificates through the electronic Home Affairs National Identification System (HANIS). The DHA Immigration Office controls all SA ports of entry (sea, land, air) through the electronic National Immigration Information System (NIIS) and issues permits to people who want to enter SA as well as permits to asylum seekers. The DHA registered citizens' fingerprints with the electronic Fingerprint Identification System (AFIS), which includes people visiting and leaving South Africa (SA) as well as immigrants. Before HANIS and AFIS, all the registrations (births, deaths, IDs, passports, etc) were done manually (pen, ink and paper) which creates a lot of work, filing, and is time-consuming. The current electronic model and systems have made registration easy, e-filing saves space and money. The systems made it easy for re-registering for the loss of ID and other DHA documents. The NIIS is located in one centre at Marabastad, Pretoria, in Gauteng, however, there are four in the country.

According to respondents, the anticipated Automated Biometric Identification System (ABIS) will replace HANIS, but they also felt that this plan to replace HANIS will never happen since years has gone by talking about ABIS. HANIS is said to be linked to the banks, South African Revenue Service (SARS) and other institutions that require ID verification from the safe and secured DHA registry.

10.1.1 Challenges with the DHA ICT systems

The HANIS system is said to be slow most of the time and very sluggish to capture data at the frontline offices which experience these problems daily. Human errors always occur when capturing data and some are deliberate due to fraud and corruption committed by officials. It is easy for officials to steal a person's identity and sell it to another person (especially foreign nationals) which makes the work of other CJS agencies difficult when trying to trace offenders. Respondents also mentioned that the NIIS cannot block a person who has flouted the visa or immigration policy. For example, if a person has stayed in the country for more than the permitted days, the system simply declares the person “undesirable”. The NIIS cannot block such a person from entering or applying for entry into the country again.

In regard to the ECMS of the DHA which is enabled to capture the biometric data (fingerprints and facial) of all travellers who entered or exited South Africa legally through ports of entry is not fully operational. Other Immigration District officers still drive to border posts or ports of entry to verify the legitimacy of documents - this is costly and a waste of resources. The systems in district offices are not linked electronically with border posts, refugee camps and the NIIS. This exercise is undertaken regularly and nothing is being done to mitigate this serious challenge. Most of these centres, border posts and camps still use manual or paper-based systems.

10.2 The South African Police Service (SAPS)

The respondents from the SAPS indicated that the old Case Administration System (CAS) was replaced by the new electronic Integrated Case Docket Management System (ICDMS). Some stations, if not all still utilise the old CAS as a backup. The respondents have indicated how the process of scanning and registering case information through the ICDMS is similar to what the literature has indicated. Furthermore, respondents alluded that the ICDMS is used to share docket information with the courts and is called e-docket. However, some stations like Akasia and Loate still rely on the CAS because of the challenges with ICDMS.

The ICDMS can upload and capture pictures of suspects (ID Photo) with a webcam and fingerprints through the Person Identification and Verification Application (PIVA). The SAPS stations can receive forensic results and fingerprint verification from the Local Criminal Record Centre (LCRC) through the ICDMS. The information captured on the ICDMS is secure and cannot be tampered with. Access to the ICDMS data requires registration and whoever worked on the information from the system can be traced because access codes are used.

10.2.1 Challenges around the ICDMS and other systems

All the stations have indicated that the systems are always very slow and always off-line, sometimes the server is down for days. Sundays and Fridays the server is down the entire day while on Saturdays it is half a day. When the ICDMS is overworked, it freezes and no case number will be generated, it cannot charge or produce a charge sheet and in that case, no docket will be registered. These challenges impact negatively on the courts as there are late appearances of suspects, no case docket information is sent to ECMS (charge sheet) and this delays court proceedings and trials. The officers indicated that even when the network is on or online, the systems can be offline. Due to the flaws of the ICDMS, the IOs are unable to populate the e-docket with sufficient and complete case docket information. Sometimes both case docket scanners and ICDMS are not working and this causes delays, creates workload and backlogs. According to the IOs, the SAPS still use hard copies of dockets at court. The signing of dockets cannot be done electronically on the ICDMS, it is done manually on the actual docket.

The respondents indicated that the new or current scanners are of poor quality and are always faulty, while the old scanners are functioning well; some stations still prefer to use old scanners. Most of the stations do not have data capturers, therefore, the IOs will personally take dockets to court and not utilise ICDMS. Case dockets are reported 24/7 and one data capturer cannot attend to all cases and furthermore, the data capturer cannot close the dockets on the system – only an IO can.

According to the Detective Commanders, the ICDMS is under-utilised by most of the IOs because they are computer illiterate, old and reluctant to learn the system. The commanders also alluded that the new young members are willing to use the system when it is online. Some of the stations like Bronkhorstspruit police station had no laptops and IOs at Ekangala police station indicated that members do not have computers. All the respondents indicated that the IOs need laptops, cellular phones and 3G devices to enable them to work in the field or away from the office. In Akasia, the laptops at the stations are not linked to the mainframe or server. As a result, the IOs cannot monitor what is happening to the CSC ICDMS or what other IOs had populated on the system. When IOs are not in the office, they cannot access the ICDMS data.

The police stations cannot access death certificates from the DHA systems, an application is done manually which takes weeks and causes delays in court proceedings. The two links, NETFAS and Global Access Control System (GACS), sometimes do not function on the ICDMS while information is being populated on it. The information takes too long to appear and is very slow during the capturing of data. The system identifies mistakes and requests the operator to fix them, while there is nothing wrong with the information. To fix these messages (GACS & NETFAS) can take up to a week to allow that function to operate. This means the information will then take a week to appear on the system.

The respondents were asked to mention other technologies that are used to fight crime. These technologies may be at the station or mobile ones. Furthermore, it was crucial to know which units within the station assist IOs in gathering information and capturing suspect information. Some of these systems are linked to the ICDMS, Forensic Services and LCRC. The Crime Information Analysis Centre (CIAC) and Crime

Information Management and Analysis Centre (CIMAC) units situated at the stations are responsible for profiling suspects' information (ID, colour photos, fingerprints and criminal records) crime registering and crime analysis. The information captured by the CIAC and CIMAC is sent through to ICDMS. At some stations like Ekangala, the CIAC and CIMAC struggles with these systems and their suspects' profiles are captured on CAS not ICDMS and sent to IOs through e-mail. The electronic **Persons Identification Verification Application (PIVA)** is used to scan suspect fingerprints and this is linked with the ID number of the suspect. PIVA is also used to verify suspect information on the criminal records database. PIVA at all police stations is linked to systems at the LCRC but not with HANIS, AFIS and NIIS. Since the SAPS police stations do not have a direct link to DHA, they send fingerprints manually on paper which takes weeks. PIVA was down for weeks at Ekangala and Loate SAPS during the time of the study.

The Automated Fingerprint Identification System (AFIS) is used by the Criminal Record Centre (CRIM) to verify suspect information with DHA. **The Morpho Touch** is a system used to verify the ID of a suspect when appearing in court. At some police stations like Loate, there is no verification of the suspect's ID to determine if the person is the correct one appearing in court **-** everything is done manually. The **Global Access Control System (GACS)** is a system that is used to locate a suspect or verify information of a suspect through a South African ID number. The GACS will then give the details of a person such as a residential address, name of relatives, employment status and previous employment, assets, properties, banking details amongst other information. Some police stations like Loate indicated the challenge they have with access to GACS. The **Circulation** is a system used to circulate reported stolen vehicles, livestock, persons or any reported missing or stolen items. Some not all police stations can access this information as long as the circulation system is fed with details of the missing item.

10.3 The National Prosecuting Authority (NPA)

After the South African Police Services (SAPS) has processed all necessary case docket information into the ICDMS, the information is electronically transferred to the Electronic Case Management System (ECMS) of the NPA. The NPA prosecutors alluded that the ECMS system is used to capture information of a suspect due to appear in court. The charge sheet (J15) emanates from the e-docket pushed through to ECMS by the ICDMS, then the ECMS generates a charge sheet with a URL number. The URL is a unique number allocated to each charge sheet, while the SAPS system has allocated a docket number to the charge sheet or the case docket. According to respondents, the URL and the case number are two different things. The clerks of the court are the ones that receive charge sheets from ICDMS and capture data to the ECMS and ICMS. The data capturers or the clerks print the electronic charge sheet which is then taken to court. The ECMS can access all SAPS ICDMS dockets nationwide.

The study has found out that the NPA prosecutors do not utilise the ECMS at all, only the senior prosecutors have full access to the system. The NPA relies on the data capturers and clerks of the court who are employed by the Department of Justice. Apart from generating charge sheets, the NPA could not assist the study with the benefits and capabilities of the ECMS. According to the clerks or data capturers, the IOs do not capture all the dockets on the ICDMS – the dockets are not loaded electronically on the e-docket. Some prosecutors are reluctant even to use their laptops or even to learn other systems like ECMS. Most of the NPA offices do not have network points. To utilise the ECMS successfully, it requires three prosecutors to populate various information onto the system (ECMS), therefore, utilising ECMS according to some prosecutors is time-consuming.

10.3.1 Challenges with ECMS and other systems

The respondents (clerks, data capturers, prosecutors and court managers) indicated various challenges associated with the ECMS. The most common problem with the ECMS is that it is always down, slow, always freezes, off-line and sometimes there is no network. The NPA does not have clerks to capture docket information on the ECMS, they rely on the DoJ & CD clerks and this creates extra work for them.

According to the NPA, the case rejects or the delays by the SAPS ICDMS cause delays to process charge sheets and to create the URL and this leads to manual processing of case dockets information. The SAPS case dockets are full of errors and poor handwriting, wrong age and names of suspects, dates (e.g: s will look like z), the information on the ICDMS about a case docket does not always tally with the physical docket – this causes discrepancies in court as well as when the docket information is captured on the ECMS. Handwritten charge sheets get lost and most contain errors such as spelling errors and wrong information. The IOs also take long to respond to these errors identified by the NPA.

The court proceedings are recorded on the Court Recording and Transcription (CRT) solution system. There are deliberate errors done by court officials who fail to record the court proceedings. It becomes a challenge when the court decides to re-open a case because some of the recordings are not available. Normally when the recording system stops functioning, the court should adjourn until the system can record. Prosecutors and staff of the justice department do not utilise the e-library function. They prefer to use books and documents for reference.

10.4 The Department of Justice and Constitutional Development (DoJ&CD)

Officials from the Department of Justice indicated that they do not handle case dockets. They only deal with charge sheets from the prosecutors. Unlike the prosecutors, the magistrates and the judges do not work closely with the police. The charge sheets are supposed to be processed through the electronic Integrated Case Management System (ICMS). However, the DoJ&CD still uses paper to process the judgements and rulings. According to respondents, the main functions of courts is "case flow management" through the ICMS. Since the implementation of IT systems, the DoJ&CD is responsible for the two systems (ECMS & ICMS). Some of the officials from the DOJ, especially Court Managers were part of the team that designed or selected specifications for the systems. Their role was to select functions that are essential for their services. Case docket information is kept on the ECMS system and after a court appearance, the clerks will populate the charge sheet and add information received from the court. The clerk imports the data from ECMS to the ICDMS. The clerks will then verify information on the physical docket against the e-docket/ICDMS, due to the discrepancies the court has discovered.

According to the respondents, the ICMS can capture all relevant case docket information electronically. It captures information from the date of the trial until the verdict is passed. The system also closes a case when the court has made a declaration or decision. The ICMS calculates statistics on the number of cases registered and enables the Department of Justice to monitor the cases that appear in court in respect of the dates, postponements and the finalisation of cases. The information from the ICMS is published on the court doors, to inform officials and the public which cases were heard in the courts for example, Court A, B, C or 1,2,3 and the date of the court case. People attending court and officials can see which cases are in progress.

The respondents from the DoJ alluded that the ICMS also keeps track of the docket from day one in court until the final day. The verdict of each case is kept on the ICMS system. The systems can also capture information from the old or closed cases that is, cases finalised before the implementation of the ICMS. The ICMS can re-open old cases that were closed because of a lack of evidence (before the implementation of the ICMS) and re-register them when new evidence surfaces and produce a new charge sheet with the URL number as an existing case. This can only happen when the old case has been captured with the ECMS before re-opening on the ICMS. Before the ICMS was implemented, recordings from the audio machine were burned onto a disc and archived. Today the ICMS can save court recordings that can be retrieved at a later stage. The NPA's ECMS and the Department of Justice ICMS are linked, so is the ECMS linked to the ICDMS of the SAPS. The ICMS is linked with the console or CRT machines in court. Recordings and transcripts can be saved on the ICMS.

10.4.1 The challenges with the ICMS and other related matters

Most of the complaints were centered around police incompetence and mistakes on the case dockets, rather than the system itself. These errors make it difficult to populate information on the ECMS and discharge a charge sheet to ICMS. Since the DoJ clerks handle both the ECMS and the ICMS, the workload is overwhelming. The ICMS is said to be slow, always off-line and sometimes it shuts down on its own for days. The system sometimes fails to complete the charges and therefore the case cannot be captured or closed and this causes delays and piles of work but also creates room for errors. Charges that are linked to the suspect, are sometimes not found on the system or the system uses different charge names. One example is that there is no charge such as intimidation, malicious damage to property and others on the system, so the clerks will capture what is closest to the charge not the real charge.

Challenges with the J175 function: when case dockets are closed by the station as undetected, the ICMS fails to re-open such cases, cannot get direct access to the case docket information. The console or Court Recording and Transcription (CRT) machines sometimes are not working. These failures to record the court proceedings are sometimes associated with corruption which is done deliberately. The SAPS, NPA and the DOJ work with the same case dockets, however, on most occasions the case statistics do not tally. The data captured by DOJ clerks sometimes is inaccurate, there is no data integrity and nobody does quality assurance. The courts including the presiding officer, still use both paper-based and electronic information.

10.5 The Department of Correctional Services (DCS)

In 2019 the DCS was still utilising the old system called Admission and Release (A & R), Community Corrections and manual paperwork. Offenders sent from courts to correctional facilities are still accompanied by paper documents or forms during the receipt and release of offenders. For example, the J15 (Charge sheet), J1, J7 (for further detain) and J3 (for sentencing from the Department of Justice) from the Courts are received on paper. All the CJS agencies and other government departments still send all their written correspondence on paper. In 2017 the DCS piloted the new electronic Integrated Inmate Management System (IIMS) to replace A&R at two facilities in Gauteng: Kgosi Mampuru in Pretoria and Johannesburg Correctional Services (Sun City). The other two IIMS were piloted in Middleburg and Carolina. In 2019 the DCS was still in the process of developing the system and adding functions to the IIMS, the piloting was still ongoing especially in Kgosi Manpuru. According to respondents, various units of the DCS were participating to ensure that their services are incorporated within the build-up functions.

The IIMS is a single point (centralised place) of contact for inmates, parolees, probationers and offender registration. The information registered on the IIMS can be accessed by all DCS centres and is linked to DHA and all CJS agencies. Documents from the court like J7 will be sent electronically to correctional facilities. The information on the system is secured and whoever changes the information must have a password and can be easily traced. The IIMS can notify the DCS when the court decides to grant bail to the inmate – this minimised the risk. The IIMS will provide the DCS with information that is crucial about the inmate. For example, the IIMS can provide the DCS with inmate previous criminal records information and it captures processes of the trial to recommend a suitable rehabilitation progamme for the inmate. Work will be done accordingly and on time as there will not be delays in information and paperwork from other agencies. One responded also alluded that "*It will be easy to do our day to day duties with IIMS*". The IIMS will save time, filing space (e-filing) and movement of documents from, section to section and from agencies. The DCS data will be saved in one central place, easy to access and shared with other CJS agencies. The IIMS will be able to use biometrics, scan fingerprints and faces of inmates. The IIMS in Kgosi Mampuru uses what is called a "microscope" to check the authenticity of the fingerprints. The IIMS wherever it is piloted was not yet linked or integrated with other systems used by various sister agencies (CJS).

10.7 The effectiveness and the efficiencies of the CJS Information and Communication Technologies

From the stated functions of the main ICT systems and the challenges mentioned in the literature as well as the respondents, a conclusion is drawn from a list of these shortcomings. Only the department of correctional services is excluded from this discussion since their system is not fully functional. Common negative features were discovered that made the CJS IT system ineffective and efficient. They are slow, freeze most of the time, off-line even when the network is up and operating these systems is time-consuming. The system failed to entice users to rely on it. Most of the users (IOs, prosecutors and magistrates) still prefer to use paper. The e-filing is not even utilised, which defeats the purpose of migrating to technology and saving time and space. The court function of Case Flow management is still done manually and the advanced functions of the ICMS are not being utilised.

10. 8 Integration of the criminal justice ICT systems

The South African CJS is still battling to interchange the data as described by figure 1 of the literature review. The current situation is that there is no integration between the CJS, and the rollout takes long to implement. The respondents indicated that working in silos and procurement is done in isolation which also contributes to the gaps that affect the integration of these systems. A key aspect of the ICT philosophy is the ability to integrate with other systems and provide a comprehensive solution with features and advantages that will allow the CJS IT users to obtain the greatest benefits from it. These systems must be encrypted[2] to avoid theft of information and corrupt activities by users.

XI. CONCLUSION

The study has followed all the prescripts of the preferred methodology by successfully collating and analysing data as described. It identified the existing challenges within the ICT of the South African justice system. The CJS has identified its determination to modernise the agencies by implementing electronic systems aimed at exchanging information amongst the agencies. A conclusion was drawn that there are more challenges and gaps like underutilisation, poor quality of the systems that need to be addressed before thinking of integrating these systems. The integration of the CJS ICT is going to be a long process that requires effective and efficient ICT systems and the will to embrace technology by the intended users.

XII. RECOMMENDATIONS

For the Criminal Justice System agencies (CJS) and the Department of Home Affairs (DHA) to address the challenges as well as to keep the ICT systems effective and efficient to enhance productivity, this article has made the following suggestions:

[2] convert (information or data) into a code, especially to prevent unauthorized access.

12.1 Change Management process and principles: To ensure that the systems are fully utilised, the CJS agencies should implement proper change management processes and principles. This must include critical elements that are essential to facilitate successful change management outcomes. For example, the CJS agencies should identify what will be improved and communicate the change to members, plan for the change, monitor and manage resistance, dependencies, and risks; and review, revise and continuously improve among other processes (smartsheet. 2020).

12.2 Capacity building: Capacity building has typically been defined as the development and strengthening of human and institutional resources. The study has discovered that most of the officials in the CJS are computer illiterate, especially older members. Computer training should be a prerequisite to new members so that they are able to use IT systems. The ECMS and ICMS have modules or e-learning functions to assist users to learn how the system functions, therefore, being computer literate will assist members to get acquainted with the systems before and after formal training of these systems.

12.3 Piloting of the ICT systems: Most of the Criminal Justice Systems have proven to be inadequate because they are slow, freeze and are sometimes offline. The system must be tested before introducing it more widely. For example, the ICDMS was said to be fully implemented by the 2019/20 financial year but the study has found that the system has more challenges. The CJS should test the systems with a small group of people or areas for a longer period to ascertain if it would be successful before the full roll-out.

12.4 Monitoring the ICT systems: Shortcomings of the ICT systems have given rise to critical situations in most of the CJS agencies. Good Information Technology infrastructure is important to all CJS agencies to control operations and eliminate possible errors that will affect services given to the users. To detect and prevent failures of the systems, the CJS agencies should have a good monitoring tool/system and Network Performance Monitor (NPM). Monitoring systems are responsible for controlling the hardware, networks and communications, operating systems, or applications, among others, in order to analyse their operation and performance, and to detect and alert about possible errors (Pandorafms, 2020). A good monitoring system improves the use of the hardware of the organisation (Pandorafms, 2020).

REFERENCES

[1]. Africa Portal. (2006). Irregular Migration to South Africa During the First Ten Years of Democracy: https://www.africaportal.org/publications/irregular-migration-to-south-africa-during-the-first-ten-years-of-democracy/ [accessed 10/10/2019].

[2]. Creswell & Clark. (2011). Designing and conducting mixed method research. Thousand Oaks. SAGE Avalos, G. (2016). Police Use New Technologies to Fight Crime : https://www.govtech.com/dc/articles/Police-Use-New-Technologies-to-Fight-Crime.html

[3]. Department of Correctional Service. 2018. Department of Correctional Services Annual Report 2018/2019: https://www.gov.za/documents/department-correctional-services-annual-report-200182019-23-sep-2019-0000 [accessed 14/005/2019]

[4]. Department of Home Affairs (2018). EMCS with biometrix. Pretoria, South Africa http://www.dha.gov.za/files/KPIS_2018_2019/SOs_KPI_Sheets%202018/EMCS%20with%20biometrics.pdf

[5]. Department of Home Affairs (2019a) What is ABIS: http://www.dha.gov.za/index.php/civic-services/abis [accessed 04 May 2019]

[6]. Department of Home Affairs (2019b). Strategic Plans, Annual Performance Plans & KPI Sheets: Pretoria, South Africa http://www.dha.gov.za/index.php/about-us/plans [accessed 11 October 2019]

[7]. Department of Home Affairs (2019c). Home Affairs White Paper. Pretoria, South Africa https://www.gov.za/xh/node/785967

[8]. Department of Home Affairs (DHA) (2019b). White Paper on Home Affairs: Pretoria, South Africa http://www.dha.gov.za/files/dhawhitepaper.pdf [accessed 29 January 2020]

[9]. Department of Justice & Constitutional Development (DoJ& CD). 2017. Progress report: Integrated Justice System (IJS) programme: http://pmg-assets.s3-website-eu-west-1.amazonaws.com/170531IJSReport.pdf [accessed 22 May 2019]

[10]. Department of Justice & Constitutional Development. (2018). The Department of Justice & Constitutional Development Annual Report 2018/2019: www.justice.gov.za [accessed 22 May 2019)

[11]. Dlamini. (2017). State agencies lament lack of integration of criminal justice systems. Johannesburg, South Africa: Sunday Times. Retrieved 05 08, 2019, from https://www.timeslive.co.za/news/south-africa/2017-11-09-state-agencies-lament-lack-of-integration-of-criminal-justice-systems/

[12]. Gauteng Department of Community Safety. (2016). Implementation of Smart Policing Initiatives in the Gauteng province [13] Government of South Africa. (2020). Justice and Correctional Services: www.gov.za

[13]. International Association of Chiefs of Police (IACP) (2014). Data, privacy and public safety. A law enforcement perspective on the challenges of gathering electronic evidence: https://www.theiacp.org/sites/default/files/2019-05/IACPSummitReportGoingDark_0.pdf [accessed 11 December 2019]

[14]. Miles& Huberman. (1994). Analysing qualitative data: https://www.nsf.gov/pubs-pub-chap-4 [accessed 20 May 2019]

[15]. National Prosecution Authority (NPA). (2008). NPA Annual Report 2008-2009: Governance and Resourcing: http://pmg-assets.s3-website-eu-west-1.amazonaws.com/docs/091119npaannreport5.pdf [accessed 24 January 2020]

[16]. National Prosecution Authority (NPA) (2017). Annual Report: the National Director of Public 2017/2018: https://www.npa.gov.za/sites/default/files/annual-reports/NDPP%20Annual%20Report-%202017-18.pdf [accessed 20 December 2019]

[17]. OSCE. 2009. Guidelines on Population Registration. Published by the OSCE's Office for Democratic Institutions and Human Rights (ODIHR) Aleje Ujazdowskie -WarsawPoland:: https://www.infosys.am/upload/DocFlow/Publications/t635234418136129516_39496.pdf [accessed 17 August 2021]

[18]. Pandorafms. (2020). The importance of having a good monitoring system: https://pandorafms.com/blog/why-you-need-a-monitoring-system/ [accessed 04 March 2020]

[19]. Parliamentary Monitoring Group (PMG). (2009). Department of Justice and Constitutional Development Annual Report 2008/09: https://webcache.googleusercontent.com/search?q=cache:ODEDRvSreLkJ:https://pmg.org.za/committee-meeting/11124/+&cd=2&hl=en&ct=clnk&gl=za. [accessed 31 January 2020].

[20]. Parliamentary Monitoring Group (PMG) (2010). SAPS Information Technology requirements and concerns about State Information Technology Agency (SITA):https://pmg.org.za/committee-meeting/12245/ [accessed 20 November 2019]

[21]. Parliamentary Monitoring Group (PMG) (2012). Security Improvements, fraud detection and prevention and online verification of identity: Home Affairs briefing: https://pmg.org.za/committee-meeting/14883/ [accessed 15 May 2019]

[22]. Parliamentary Monitoring Group (PMG) (2016). Governance and Resourcing: http://pmg-assets.s3-website-eu-west-1.amazonaws.com/docs/091119npaannreport5.pdf [accessed 27 November 2019]

[23]. SABRIC Bank (2020). Department of Home Affairs (DHA) Online Services: https://www.sabric.co.za/media-and-news/press-releases/department-of-home-affairs-dha-online-services/ [accessed 29 January 2020]

[24]. Saldana, J. (2009). The coding manual of qualitative research. Thousand Oaks. SAGE

[25]. Smartsheet. (2020). 8 Elements of an Effective Change Management Process: https://www.smartsheet.com/8-elements-effective-change-management-process [02 March 2020].

[26]. South African Police Service (SAPS). (2013). SAPS TMS - ICDM Project Status: pmg-assets.s3-website-eu-west-1.amazonaws.com › 130419saps [accessed 31 January 2020].

[27]. South African Police Service (SAPS). (2015). Progress with the new Investigation Case Docket Management System (ICDMS) project for the SAPS. 2015: https://www.saps.gov.za/resource_centre/publications/police_mag/police_jan_2015.pdf [accessed 14 October 2019].

[28]. South African Police Service. (2016). Annual report 2016/2017:https://www.saps.gov.za/about/stratframework/annual_report/2016_2017/part_a_2017.pdf [accessed 17 December 2019]

[29]. South African Police Service (SAPS). (2017). SAPS annual performance plan 2018/2019: https://www.saps.gov.za/about/stratframework/strategic_plan/2018_2019/annual_performance_plan_2018_2019_updated.pdf [accessed 04/11/2019].

[30]. South Africa Yearbook. (2017). Correctional service: https://www.gov.za/about-government/correctional-services [accessed 10 January 2020]

Solani Mthombothi. “The South African Criminal Justice System: Identifying the challenges of the Information and Communication Technologies.” *International Journal of Humanities and Social Science Invention (IJHSSI),* vol. 10(12), 2021, pp 17-28. Journal DOI- 10.35629/7722