International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 12, No.1 (Nov-2022)

https://dx.doi.org/10.12785/ijcds/1201101

ADRS: Automated Details Retrieval System for victims of Incidents and Accidents using Fingerprint

Mohammed Mahmood Ali[1]

[1]*Department of Computer Science and Engineering, Osmania University, Telangana, India*
Received 1 Apr. 2021, Revised 8 Sep. 2022, Accepted 29 Nov. 2022, Published 30 Nov. 2022

Abstract: Complaints related to accidental and incident cases are not updated effectively in online databases especially by Private and Government hospitals, due to which the information details of such victims are missing. The problems faced in identifying such victims from unexpected accidents and incidents are difficult for tracing their details from existing methodology adopted. To overcome, the victim's information can be tracked with the existing available databases by building an integrated Automated Details Retrieval System (ADRS) using victims Fingerprint from which Aadhaar details and mobile numbers are extracted. Simultaneously, ADRS also searches for retrieving some additional details from repositories of Driving license, Voter-id card, Pan Card, Social Networking Sites (SNS) and Mobile Service providers. Input to ADRS is Thumb/Finger impression of victims who are partially injured or missing children's or aged persons or mentally disabled persons. Internally, ADRS detects and chooses unique Aadhaar number from the victims fingerprint. Later, ADRS starts mapping, crawling, retrieving and then gathering information through others databases (Pan, voter-id, Passport and Driving license, SNS) which makes the ADRS more precise and efficacious. This ADRS retrieves the information details by crawling through the online databases and generates the report. The generated report constitutes of Name,address, mobile, father's name, DOB and mobile number of victim along with details of six (6) nearest family members are fetched using Reinforcement machine learning technique. With this facility, unknown details can be traced and intimated to their family members regarding the condition of deceased persons or missing adults or children's. The precision rate obtained from the proposed ADRS is 96.39%. when compared to other state-of-art systems (Finger, Iris, Odor [1], FLDNet [2], Multimodal [3]).

Keywords: Accidental, Aadhaar, ADRS (Automated Details Retrieval System), Fingerimpression, Reinforcement Learning

1. Introduction

Reports of Road and safety conveys that innumerable deaths of accidents happening day-to-day life are not automated and stored in databases; due to which the information related to those victims are lacking far behind and sometimes die in the hospitals itself without recording it in the secured databases.. Even, if stored it takes lot of manual work to resolve the matter which is a time consuming process that takes minimum 1 week to 6 months as per the survey reports of Ministry of Road Transport and Highways (MoRTH) and National Crime Records Bureau (NCRB) data [**?**] [4]. Especially, in private hospitals if the victim gets admitted their information is temporarily saved in computers and later it will become obsolete. If emergency is needed by Government officials, then only the details of victim(s) will be recorded for future analysis that to in very rare cases.India in the year 2019, had recorded the deaths 1,54,732 and fatal injuries of 4,39,262as per the recent NCRB data [4].

The countries located in Africa, Latin America and Asia does not have proper information related to missing children's. But, on an average the missing children's data every year throughout the world-wide is predicted to be around 8 Lakh's exclusively from United States. Similarly, around 2.3 Lakh's and 1 Lakh are from United Kingdom and Germany countries, whereas 40K and 50K are from Brazil and Canada respectively as per the survey of 2017. United States started maintaining the updated data of missing persons for their 49 states systematically in an organized fashion with average missing persons of all ages are around 6 lakhs every year as per the NamUS database, among which 1000 deceased bodies are unidentified [5]. Since 1980's, SriLanka stands as one of the top-most country in the world for more number of cases of missing persons that ranges between 60K and 100K [6]

Usually, unknown accidental victims are admitted in the government hospital, the victim's name will be registered as "Medico Legal Case", with no name, later if the victim dies then autopsy of the body is conducted by assigning a unique number and the details are saved. In most of the cases, government follows certain guidelines like taking the body to a mortuary and keeps the body for certain period of time. After, a deadline is crossed the body is cremated, under the supervision of police officials. It is found, that the budget

E-mail address: mahmoodedu@gmail.com

expenses incurred for this whole process is barred by the government during this duration of time till the cremation of the body.

Whenever, a serious accident happens the victims will be in unconscious state, during this process the expert team under the supervision of traffic police needs to take the fingerprints and Facial(Iris) snapshots of the victim which is recorded and saved, for further analysis. Immediately, these fingerprint impressions has to be mapped with the existing databases available with the government that constitutes of information pertaining to Aadhaar card [7], driving license, registration of vehicle, voter-id, passport verification, mobile phone registration, Land registration and other relevant databases. Once, the details are retrieved, the family members of the victims need to be traced using cross-referencing technique from those databases which extracts the colleague's mobile numbers. Subsequently, this expert team will intimate to the colleagues or family members regarding the status of the victim by identifying the name, address, mobile numbers and other details which are retrieved by proposed ADRS. In one of the forensic survey conducted in the year 2016 at Oak Ridge National Laboratory proved fingerprint impressions and Iris data are active for certain period of time [8]. Most probably for Four (4) days in summer season and up to Fifty (50) days in spring and winter seasons. Recently, in 2020, deceased person's iPhone was unlocked using his fingerprint after his death within a time frame of 2 days [9].

The main objective of this research work is to effectively make use of scanned fingerprint template, and then search for a matching finger template in Aadhaar database from which the unique identity of a person is successfully identified. Henceforth, the subsequent details of a person is also retrieved from Aadhaar which can be consistently used for retrieving further more personal details (employer, job details, voter-id, current address,income, passport and close family members).Every year the government spends crores of budget for maintenance and development of mortuaries, this cost can be extensively cut-down if the victim's information is retrieved. Once, the details are extracted the victim's body would have been handed over to their family members. But, currently most of these governments are neglecting this matter. The important point is that the government has to re-think intelligently and use the advanced technological developments that aids in tracing of victim details such that it will reduce the unnecessary cost which is put-up on the government budget, due to unexpected incidents and accidents [10].

This Section, illustrates the significance and motivation of performing autopsy on Fingerprint and Faces (IRIS)of live and deceased persons, so that the identity of these victims are traced quickly by utilizing existing available technology (i.e., information stored in secured databases), maintained by government departments. This reduces cost-cutting expenditure of yearly budget allocated on mortuary development and maintenance in Government hospitals in large scale. The Section 2 explains the retrieval systems developed till date for tracing the missing children's/adults or persons mentally discarded due to aging factor, deceased persons and persons lost their memory in accidents or murdered in broad day-light in public. Further, the problems faced by the government officials (Traffic department, Police department and Hospitals)if those victims are not identified and traced in time. To overcome, an Automated Details Retrieval System is proposed in Section 3 that efficiently traces the personal history along with 6 family relatives of infected victims with the use of Machine learning, facial recognition systems, Edge computing on cloud platforms, Smart IoT technologies and Artificial Intelligence algorithms [11]. In Section 4, the developed ADRS is compared with other systems and the experimental results obtained are discussed. Finally, in Section 5, we conclude that in future, we planned to search by taking both Fingerprint and Scanned IRIS of these deceased persons in International databases if access to those databases is granted, which will retrieve further more details of those victims, resulting in enhancing the ADRS precision rate.

2. Related Work and Problem statement

In India for unique identity of an individual, we use "Aadhaar card", just like in foreign countries it is well-known as "Social Security Number". These unique identification cards stores the personal details such as Fingerprints, Iris scan, Name, mobile number, address, employment status, health condition and blood group. Those details can be effectively used for tracing of victim's who are met with incident or accident in situations where the victims are speechless due to unstable health condition. Here fingerprint of the victim plays a very crucial role for retrieving the details from various databases, especially Aadhaar database.

A. Fingerprint Scanning, Social Security Number and Its Applications

Fingerprint scanning is the method of capturing the whorls and lines from the finger tips resulting in forming a unique pattern of a person that distinguishes one's from others. Initially, around 1880's Sir Francis Galton used Fingerprint scanning for identification of individuals. Later, in 1902 US started its first usage for official purposes; slowly in 1924 the matured fingerprint system was deployed in full-fledged way by issuing cards by government authorities. In 2020, FBI and Department of Homeland Securities of US conveyed that they have 120 millions of peoples finger prints which are scanned in their various secured databases. The methodology adopted for retrieving the privy data that authorizes the unique identity of an individual in a society is considered as Social Security Number (SSN) which is linked with scanned Fingerprints and Facial Retina (IRIS). In real-time applications their usage is effectively used in most of the countries. Proposals were made by most of European nations for International sharing of fingerprint for information extraction to secure the international peace and harmony throughout the world from criminals and criminal

activities considering the restrictions of national and international privacy laws in emergency situations. Presently, India has a huge repository of fingerprint records of 1.25 billion people which is named as "AADHAAR" [12].

B. Applications of Bio-metric devices in Crime detection

Fingerprint scanning is one of the most secure and authentic method adopted for unique identification of a person throughout the world [12]. This method was initially adopted by well-developed countries like Russia, US, Japan and China for issuance of Social Security Number (SSN). Later, they have added scanning of Retina (IRIS) mandatory for unique identification of a particular person. Now-a-days, most of the countries capture the Fingerprint and Retina scanning as a mandatory parameter for unique identity of individuals. Every activity in a particular country has started linking of SSN with Property registrations, SIM card registrations, Government Jobs, Confidential security purposes, for attendance marking, ATM Bank machines, Income tax payee and many more applications. Besides the above applications, the Fingerprints are extensively used as one of the effective means of providing security to personal belongings of our day-to-day activities such as Smart Phones, Unlocking of Accessories (Fans, Lights, Home Appliances), Car unlocking and doors opening. Apart from those the Defense organizations had made it mandatory for its employees to give their Fingerprint and retina scan through automated bio-metric machines which are Wi-Fi enabled in most of the sensitive places that requires extensive security.

Veins present in Fingers are effectively used for differentiating one human from other human which is effectively used in bio-metric devices by law enforcement for authenticity purposes. Apart from that iris recognition is another strong weapon for uniquely identifying an individual which is mostly used by crime department to solve the complex cases of crimes. Similarly, a new research started for finding the unique individuals based on their odor, which is a new study of research recently born and researchers are working on this technology [1]. Among, the three (3) methods discussed above Fingerprint based on veins of human body have attracted a huge response for bio-metric devices which is currently dominant in real time applications.

To detect spoofed Fingerprints, a new Fingerprint Liveness Detection Network (FLDNet) was proposed which is built using CNN by embedding a new block structure in Attenuation layer [2]. Similarly, Multimodal Fingerprint detection algorithm was proposed to resolve human identification and authenticity problems by leveraging Genetic algorithm as well as Swarm optimization that drastically reduced the false detection rate resulting in enhancing the accuracy. In this system, they have used Fingerprint templates and Iris [3].

The precise study on types of finger-print formations (Arches, Whorls, Loops) is well-studied that proved as an effective way in forensics to investigate crime scenes [13]. The serious offences in residential areas & offices, Commercial burglary of ornaments, Murder and Vehicle theft are traced using fingerprint forensic study that solved Ninety 90% of crimes within a span of month [14]. Recently, in India, Delhi police officials initiated the process of linking the Aadhaar based system for identifying the unclaimed bodies. For this, the proposal was unofficially accepted for "Aadhar based STQC Certified finger print scanners" to solve dead bodies identification problem in hospitals and crime investigation department [10].

C. Problem statement

The conventional procedures in India earmarks many lacunae in the precautionary steps adopted for identification of dead bodies which remains unsolved, in many of cases, they persists for longer period of time, which later goes unnoticed or missing. Sometimes, the unclaimed dead bodies lead to unsolved criminals cases which need to be closed after a particular deadline. Where accused are relieved if the identity of the victim is not correctly recognized. Additionally, the expectations and grievances of relatives are further dented [10].

It is observed that, many of the people's identity is lost, due to various reasons one of them is unavailability of information in the government records. To do so, the government has set-up a plan of unique identification process of individuals by introducing "AADHAAR" card system throughout India. Many of the death certificates are given only to those persons who approach Birth & Death department by providing certain proof of death of a person from Hospital's or Grave yard in charge. Currently, the database is lacking of storing the information of Births of those persons who were born 50 years back due to lack of availability of technology especially in India. Even, if the information is available there is no proper linking of previous information with the existing information which is brought to the notice of Birth & Death department after the death of the person. The cause of these discrepancies is due to improper maintenance of databases or restriction of databases by government personal. In a study, it is revealed that some people are migrated without passport identity from other countries to our country for their livelihood, due to which their finger-print information is not traced from available database. In those unforeseen instances, some other databases needs to be searched which is not an easy task, which requires approval from international body [15].

In one of the forensic study conducted on unclaimed dead bodies at Indira Gandhi Medical college located in India quoted that dead body speaks, it's a misnomer for time being but later it is proved that it requires to employ well-equipped available resources. In another forgery case, it was found that if the clear image of Fingerprint and iris are captured and stored after the person dies. Later, those scanned data are presumably used to unlock most of the electronic systems such as Mobiles, Home accessories, online payment applications, security doors and even more.

The smart hackers and criminals have started spoofing of Finger-print and iris of victims for financial benefits and began to perform international and national online banking frauds in large scale [16].

The evidences in CCTVs footages were captured that has authentic proof of people falling due to serious infected virus named as "COVID-19". Even, Family members denied of accepting deceased bodies as people are worried about the spread of this disease. In such situations, the autopsy on finger-print needs to be taken-up for identifying those bodies so that appropriate action would be taken by concerned government authorities to handover the deceased bodies [17].

Till date, many techniques and methodologies are proposed for improving the efficiency in finger-print templates, but utilizing them by integrating with SSN and Aadhaar based system is not efficiently embedded for recognition of humans [10].

In this section, the problems faced if in-time autopsy of finger-print is not taken within the time-frame are discussed. The importance of securing Fingerprint and Iris in databases is explored. Further, how the criminals make use of spoofed finger-prints and Iris is revealed along with their adverse consequences that may give rise to various implicit crimes is discussed. To overcome all the above issues we proposed ADRS architecture that will effectively make use of scanned finger-print and Aadhaar number that successively fasten the identification process by mapping, crawling, retrieving and then gathering information through others databases (Pan, voter-id, Passport and Driving license), making the ADRS more precise and efficacious is discussed in Section 3.

3. Automated Details Retrieval System Architecture

A. Proposed ADRS Architecture

This Section illustrates the proposed Automated Details Retrieval System that aids in identifying the personal details of victims effected due in incidents and accidents as shown in figure 1.

This ADRS initially takes the finger-print as an input through a sensor-based device which successively extracts the Whorls & Ridges of finger(s) through sequence of processing steps consisting of Acquisition, pre-process, Feature Extraction, Normalization and Pattern Formation resulting in generation of pattern formation known as "template" [18]. Once the template features of a finger is extracted those are preserved and sent for storing into the assigned databases (Patterns of Whorls and Ridges). The next step is extracted template features are forwarded to Crawler and mapper component, which pursues forward for searching and mapping with template features of recorded finger-prints of people that are present in various databases [19] (Aadhaar, Voter-Id, Driving License, Pan card, Passport, SNS).

This crawler & Mapper component uses Reinforcement Machine learning technique for mapping of related information in a sequential order, initially; it searches for matching of finger-print template by crawling through the Aadhaar database and proceeds towards other databases for extraction of relevant details. Sometimes, if the Aadhaar information related to victims are missing or conflicting or insufficient or inappropriate, then the crawler and mapping component initiates steps of dual searching process in other databases otherwise it settles down with the initial search which was performed earlier.

Most of this confidential information of Authorized Unique Identification database is in encrypted format to preserve security for the data. Even, authorized personal and unknown persons could not able to browse those databases until the prior permission from government authority is not obtained. During, this retrieval process, the system is intelligently designed in such a way that it will extract details of persons up to Six (6) members of a particular family that has a relationship among them along with mobile numbers linked with the extracted information. Meanwhile, during this process, if the template of finger-print is mis-matched an alert to the Sensor capturing & filtering module (i.e., ADRS) is initiated for re-scanning or else acknowledged with a success message which has to be shown on the display. Finally, the Log file is generated that has information details of all the Six (6) persons linked to their mobile numbers. This report delivers the useful knowledge for Criminal department, Police and Hospitals departments that assists in detecting, tracing and then predicting the details of missing children(s)/Adults effected in incidents or accidents. Ultimately, the identification of victims is made easy which widely reduces the work-load and expenses of government organizations.

B. Datasets

Availability and feasibility to use those databases comprising of information related to Aadhaar, Voter-Id, Driving License, Pan Card and Passport is restricted for normal use, unless the permission access is granted from the government organization in any country of the world. The dataset for research work is taken from Kaggle.com (https://www.kaggle.com/knightking007/aadhaar) is not appropriate for doing research as per our requirement. The Names and Aadhaar number or equivalent-code is missing for accessing the information of a particular person. So, we have assigned a new employee-id named as "Attendee code" for the original "Aadhaar number" and generated new dataset as per our requirement by collecting the information from Faculty and students through Google form questionnaires to test our ADRS architecture [20].

ADRS dataset comprises of Nine (9) fields as shown in Table I, comprising of 3,020 genuine records collected from Faculties, students, non-teaching and administrative staff members of our college.

An implementation snapshot of the dataset is shown in Table II. Further the complete dataset details can be viewed

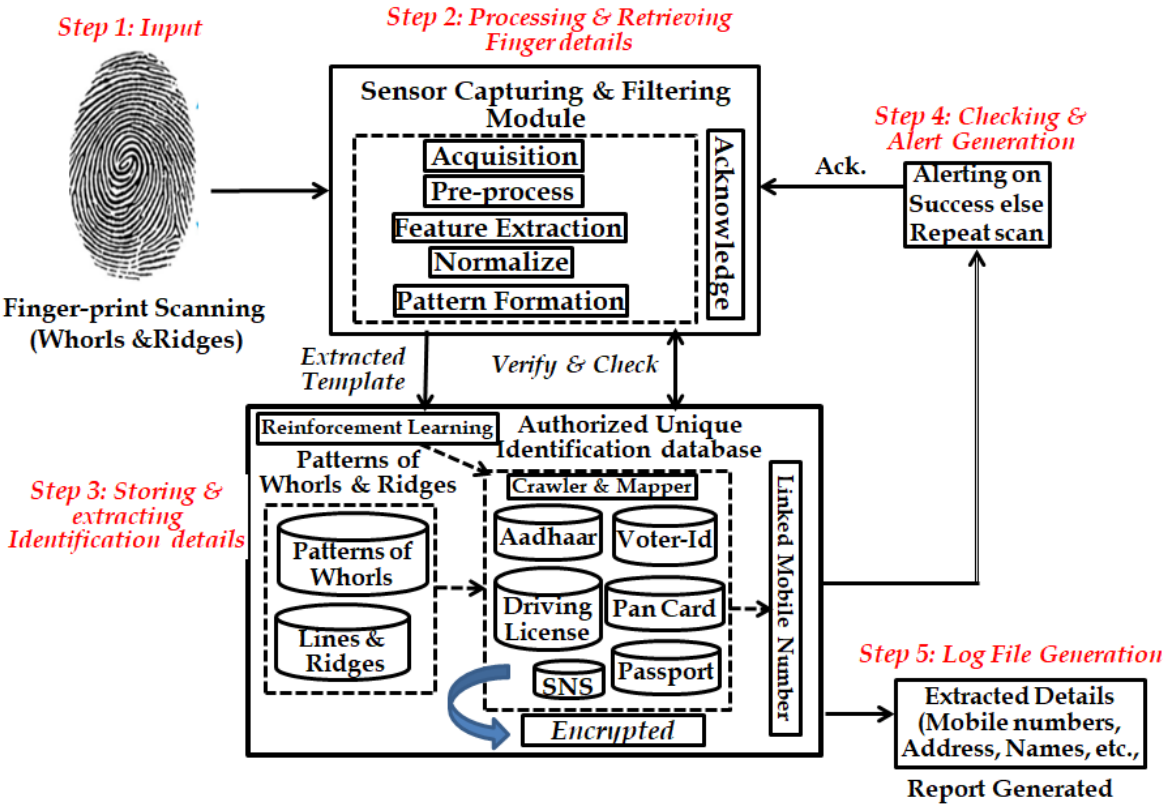

Figure 1. ADRS Architecture for Scanning of Finger-print and verifying details of victim

TABLE I. COMPRISES OF FIELDS OF AADHAAR DATASET

Sl. No.	Field Name	Data type	Size
1	Status	Varchar2	6
2	Aadhaar Number	Number	12
3	Attendee code	Varchar2	8
4	Attendee Name	Varchar2	18
5	Gender	Varchar2	1
6	Email	Varchar2	
7	Mobile number	Number	10
8	Attendeeid	Number	12
9	Category	Varchar2	8

through my personal Dropbox link, which is shared for the use of research purpose [20].

It is observed that in the given dataset, starting six (6) digits of Aadhaar are marked as "*" for security purpose, whereas the other fields are visible for analysis. In the dataset NA means (Not Allowed).

C. *Storing of Template generation and verification process of Fingerprint*

The steps involved for fingerprint storing in the database and subsequently matching with the aid of Sensor Hardware devices is illustrated in Figure 2.

Initially, the Sensors are used to capture the image with the help of Touchless 2D fingerprint standard Hardware devices, then these devices perform the pre-process task which enhances the scanned Fingerprint by improving the quality of Whorls & ridges, besides filtering out the noises[14]. Once the quality is improved then the features are extracted from that scanned improvised fingerprint image, where the template is generated for storing in the database. During the verification process the template is fed to comparison checker where the stored template from the database is cross-checked for mapping with the new fingerprint image which is captured by the hardware device [21].

TABLE II. IMAGE SNAPSHOT TAKEN FROM THE COLLECTED DATABASES OF TEACHING FACULTIES SHOWING THE FIELD NAMES AND PARTIAL RECORDS INFORMATION

Status	Aadhaar	Attendeecode	AttendeeName	Gende	Email	Mobil	Attendeeid	Category
success	72333	NCSE22	Mr. Muneeb	M	muneeb@yahoo.com	9989487863	32232	staff
success	72337	NCSE27	Mr. Kaleem	M	kaleem@yahoo.com	9889487682	32237	staff
success	72440	NCSE32	Mr. Saleem	M	saleem@gmail.com	8889487851	32245	staff
success	72551	NCSE39	Mr. Khatoon	F	khatoon23@gmail.com	8881212123	32276	staff
success	72763	NCSE46	Mr. akbar	M	akbar29@gmail.com	9392109128	32899	staff
success	72779	NCSE54	Mr. jilanibee	F	jilaniibee@gmail.com	9885782137	32282	staff

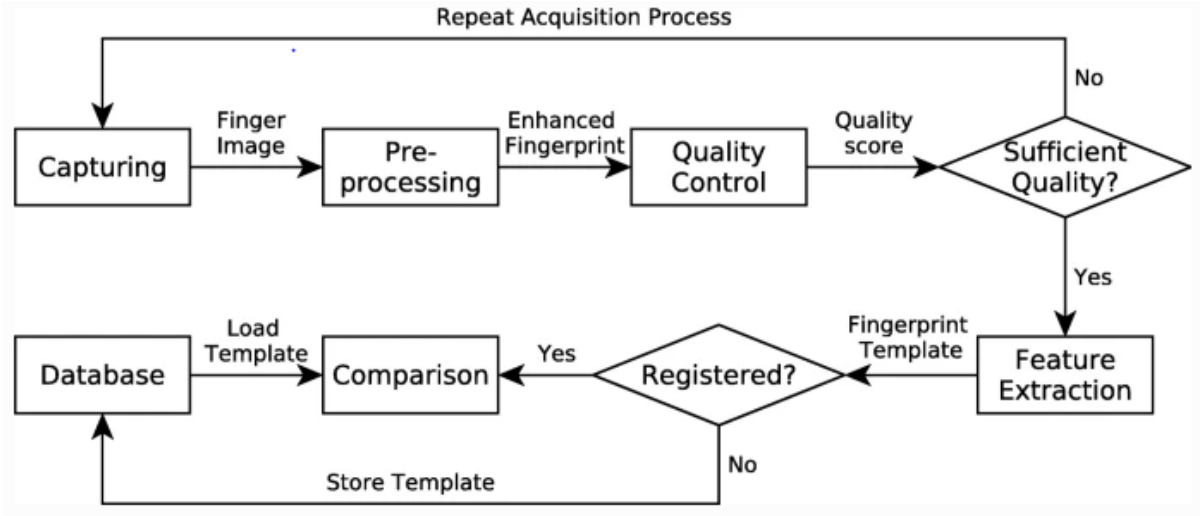

Figure 2. Steps involved in capturing & mapping of fingerprint image for extraction of template and storing database

D. Machine learning (Reinforcement Learning)

Innumerable techniques are available for analysis of data based on the requirement and necessity of their application. The techniques of Data mining and Machine learning (ensemble methods) are broadly used alternatively for prediction applications in various application-oriented domains such as Health care systems, Financial banking sector, Education institutions, Scientific & Research issues and many more. Usually, the data exists in structured, unstructured, semi-structured formats. Currently, no one technique is enough for solving a particular domain problem, we may integrate many or a particular specific technique as per the necessity for arriving to a unique solution. In our ADRS system the data is mapped from various databases using a crawler & mapping component and stored in structured organized format.

Reinforcement Learning is one of the machine learning algorithm that constitutes of multiple sub-steps to achieve a precise goal, in which each step gives either reward or penalty on an action performed by an agent where it checks for the mapping details, We have used it in crawler and mapping component for retrieving of Aadhaar details from various databases [22].

E. Working Flowchart of ADRS architecture

It is extremely important and challenging assignment to be dealt for unclaimed deaths or live bodies that are found in incidents or accidents. For this, it needs genuine and organized efforts to find those missing persons and recognize those unidentified deceased bodies. For this, the proposed ADRS architecture is illustrated using Algorithm-cum-Flowchart as shown in Figure 3.

Steps of the flowchart are elaborated as given below:

1. The fingerprint impression is received by the sensor device that captures,processes and extracts features by improving the quality of fingerprint resulting in generation of template which is stored in database as discussed in Figure 2. Subsequently, the extracted template is mapped with the Aadhaar database. If the match is found it proceeds for further analysis.

2. In this step, if the information pertaining to the template is matched with the Aadhaar database, the details of the victim are retrieved and stored temporary in the database. In case, if the mismatch occurs for the extracted template due to various reasons such as improper fingerprint impression or failure in detection process of the template from the Aadhaar database. Then, the system halts with a

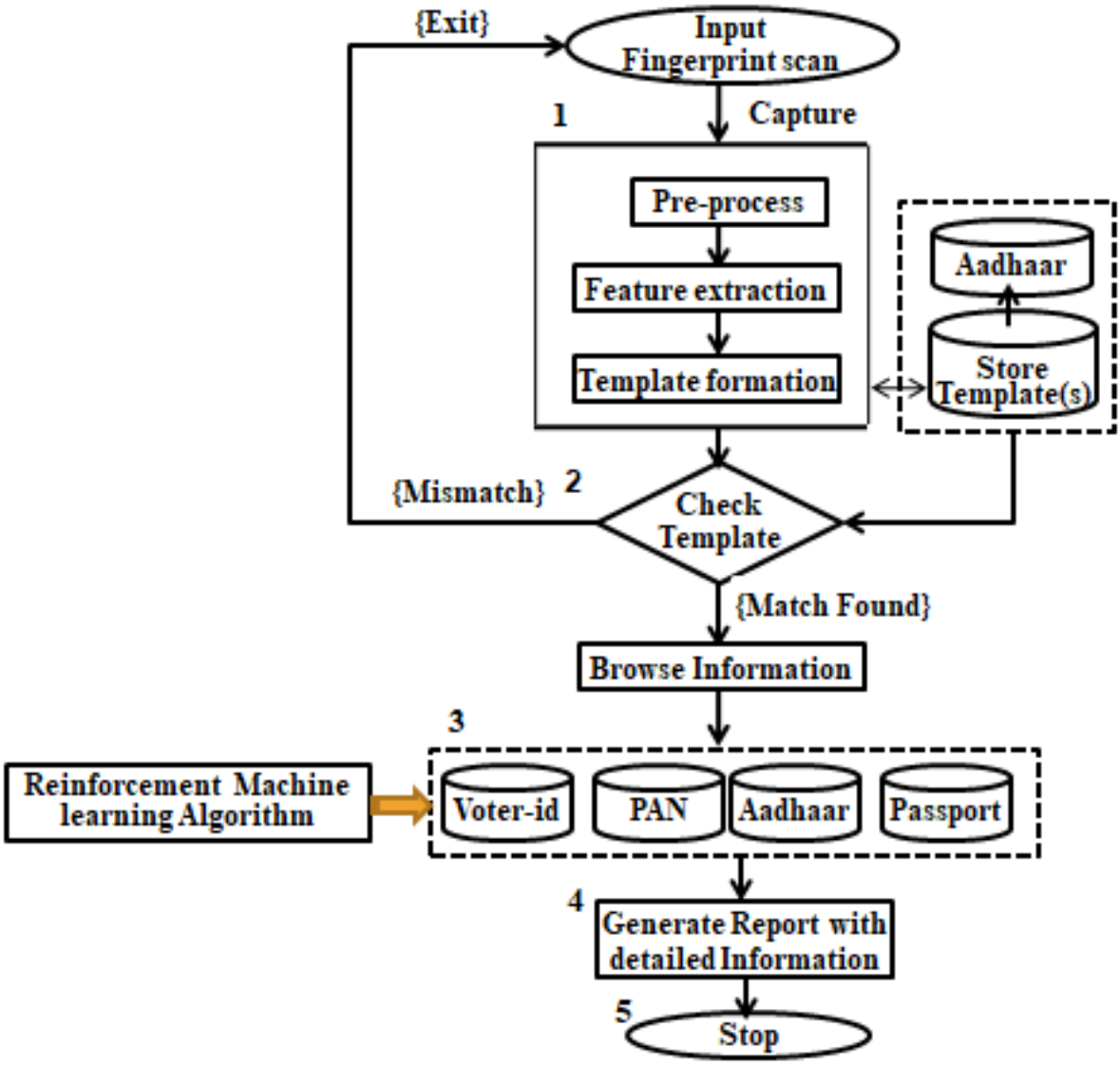

Figure 3. Extraction details of victims from various databases using ADRS architecture

request to rescan the fingerprint impression.

3. In this step, the reinforcement learning is embodied by the crawler and mapping component as discussed in Figure 3, for efficient retrieval of some more details of the victim. This step is the heart of ADRS architecture. Initially, if the complete details (Name, Aadhaar number, Address, Date of birth) are successfully retrieved it stores and initializes to search for some more details from other source of databases. During this searching process the Aadhaar details are chosen by the reinforcement learning and tries to Cross-verify the details from other databases (voter-id, passport, driving license, SNS) if everything is mapped the system proceeds for further process. In case, if conflict arises in any one of the fields namely in Name, DoB, Address it retrieves those information as miscellaneous details and records the conflicting details in the database. Immediately, the mapped retrieved details are further processed for analysis where Two (2) or more fields (i.e., Father's name or Address) are picked and mapped to retrieve the details of family members up to Six (6) members (based on address or father name) [23].

4. Once the information retrieval and mapping process is completed the report is generated and saved for tracing the victim details who are met with incident or accident.

5. Finally, the generated report is cross-checked using Mobile number, Address, Name, or other details which are retrieved by the ADRS using Reinforcement machine learning technique. So, that the information of victim is given to their family members.

Interesting fact is that once the Aadhaar details are successfully, retrieved on matching of Fingerprint template from Aadhaar database. Subsequently, the Crawler and Component picks the Aadhaar details and tries to search (i.e. maps) in PAN database. From the PAN database, unique PAN number along with the employment details, Income, Bank details and other necessary information is also retrieved. Apart from that, the SNS database is also checked which detects the email-ids.

4. Proposed Methodology

The ADRS is developed using PHP language as Fingerprint packages are readily available online that can be deployed and configured into our system. We used XAMPP server as it proved a cross-platform for Fingerprint Stack packages, Apache server connectivity, MariaDB database- and Scripts are well-written and supported by the use of PHP in a friendly manner without any configuration and connectivity problems [24]. The mapping details are retrieved using the fingerprint impression captured by Sensor and submitted for retrieving the Aadhaar details by ADRS model. The accuracy of ADRS is evaluated using the precision metric, for which the formulae is shown in Equation (1). The overall working of ADRS architecture Figure 1 is explained using a flowchart-cum-algorithm in Figure 3.

Precision=(Number of Accurately retrieved Aadhaar Numbers from Dataset)/(Total number of Aadhaar Numbers available) X 100 ..... (1)

Precision=(2911)/(3020) X 100=96.39%

The precision rate obtained is 96.39%, the reason behind the decrease in precision rateisbecause of 2.51% of fingerprint impression were not taken properly, 1.10% of fingerprint impressions are not correctly mapped from Aadhaar database showing a response of “mismatch” for few of them and a response of “invalid fingerprint” is shown after processing by our ADRS system.The complete working of ADRS architecture is explained using an algorithm shown in Figure 4.

After retrieving of Aadhaar numbers the ADRS is tested for checking of authorized mobile numbers which was assigned during the registration of Aadhaar. The system has successfully retrieved all the Names, Mobile numbers and Date of Birth; Apart from that for some of the persons only year of birth was retrieved. Taking those retrieved Aadhaar details, we have cross-verified the information from the other databases (Pan, Voter-id, Passport, driving license, SNS) to retrieve further more information that has resulted in retrieving of some more additional information such as Multiple names, Income details, Working company, email-ids and Bank details. To maintain security concerns we did not disclose their personal details due to privacy restrictions. A separate script is executed again that performs a dual search process to the retrieve the details of other persons by checking/mapping of Address details and Father name. We have assigned a threshold of up to six(6) nearby related relatives information of that particular person needs to be extracted by ADRS. Thus, we have successfully executed our ADRS system with good results as discussed above.

The proposed ADRS model is compared with the existing Data retrieval models [19] [21] [23] by choosing the available features in each of these systems without considering the bias towards any of the system which is shown in Table III. No doubt, our proposed ADRS lack in few features, but in view of tracings the victims it performs well as shown in Table IV.

The chosen features are shown in Table III, are only for knowing the parameters that are supported by earlier developed systems. The objective of ADRS is to retrieve the details of victims using fingerprint is successfully attained by crawling through various databases and retrieving the necessary in-formation based on which decision of identifying the persons who are met with unforeseen incidents such as missing of children’s, adults, aged people, mentally retarded persons and accidental victims are traced. We have configured the above models using our existing dataset [20] and the results obtained by each of these systems are depicted in Table IV. The fingerprint matching of FLDNET model is 97.21% which is better than ADRS Model which has 96.39% accuracy. The comparative analysis is depicted using histogram in Figure 5.

During the report generation process from distributed sources of databases resulted in multi-classification problem for few of the victims resulting it difficult to properly differentiate/mapping among the victims due to improper naming convention in various databases. To overcome, a plan for embedding of Block-chain technology is devised, apart from Reinforcement Learning methods.

5. Conclusion and Future work

ADRS (Automated Details Retrieval System) works on the principle that the information pertaining to Authorized Unique identification details of persons are provided from authentic databases of Aadhaar, Pan card, voter-id, driving license, SNS and Passport. Initially, the ADRS, starts browsing Aadhaar details, and successively proceeds further. For Comparison of ADRS with state-of-art systems, we have collected the information from College faculties and Students through a questionnaire’s through Google form to test our system and generated our own Aadhaar datasets. The snapshot of the dataset is shown in Table II, for the proof. We also tried to extract employment details using PAN card and SNS, but we could not able to succeed up to the expectations.

The earlier systems developed were totally different as such we could not able to make appropriate comparative analysis. Henceforth, this ADRS system is uniquely developed by choosing and configuring as per our pre-defined dataset comprises of (Aadhaar, PAN, Voter-id, Passport) collected from various sources. The precision rate obtained

```
Input: Scan Fingerprint Impression
Output: Retrieve individual details (Report Generation)
Read Fingerprint_Impression //Scans the Fingerprint
Check (Finger_Template, Aadhaar)
   // Processes and Filters Scanned Finger and maps with Aadhaar
{
 Process Ridges and Lines
    //Checks and improves Quality of Ridges and Lines of Scanned finger
 Map (Finger_template, Aadhaar) //Starts checking Fingerprint template in Aadhaar
 Compare (Finger_template, Aadhaar)
    //Checks the percentage of  mapped Fingerprint with Fingerprints  of Aadhaar
 if (Finger_template fails)
 Rescan&ProcessFinger_template
    //Improper fingprint or mismatch found repeat the scanning of Finger
 else
 Crawl (mapped Finger_template, Aadhaar)
    //on succsessful mapping of Fingerprint in Aadhaar
 Retrieve Aadhaar details
    //Extract Aadhaar number, DOB, Name, Mobile number, Address, Photo
 Apply Reinforcement Learning (Aadhaar, PAN, Voter-id, Passport)
 {
 Check (Voter-id, PAN, Aadhaar, Passport)
  //Pick extracted Aadhaar  details &start searching for matching details in other Databases
 {
 Collect and Map retrieved details sequentially
  // Sequentially extract and assign the matched details to Aadhaar number
 if (Finger_template matched, Aadhaar)
 {
 Update and re-allocate(Finger_template, Aadhaar, PAN, Voter-id, Passport)
  // Repeatedly check and re-assign the appropriate retrieved information and remove
  // discrepancies
 }
 Generate Report
  // Log file generated with complete details mapped to Aadhaar number
 }
 }
 }
```

Figure 4. Complete Working Algorithm of ADRS architecture

is based on Fingers template mapped with Aadhaar database that achieved 96.39% accuracy.

It is observed that in few of the deceased cases of serious accidents the body parts (hands), especially fingers are found totally damaged. In those cases, it becomes very difficult to take the fingerprints of such deceased persons. To overcome, those problems in future, we planned to integrate the datasets of Facial and Retina (IRIS) (i.e., Face & Eyes) scan of the victims to further improvise the system [1]. Besides, this we also planned for tracing and tracking the mobile phone call history of the victims by contacting with the authorized Service providers of various Cellular networks; so that it boost-up the task faster in identifying their close family members and friends. Another, important future work is our ADRS architecture needs to be enhanced by embedded with the features that support bio-metric fingerprint searching process from International databases for unique identification of a victim in case if the victim details are not retrieved properly from the existing repositories.

6. Acknowledgement

I would like to thank Director Dr. Baser Ahmad, Head CSED Dr. Abdul A. Moeiz Qyser and all the students and staff of MJCET for providing their Fingerprint details for

TABLE III. DEPICTS THE ADRS FEATURES CHOSEN FOR COMPARISON WITH OTHER DEVELOPED SYSTEMS

Features	Proposed ADRS	Finger, Iris, Odor systems [19]	FLDNet [21]	Multimodal [23]
Aadhaar	Yes	Yes	Yes	Yes
Passport number	Yes	No	No	No
PAN	Yes	No	No	No
Fingerprint	Yes	Yes	Yes	Yes
Iris	No	Yes	No	Yes
Human body Odor	No	Yes	No	No
Performance	Good	Good	Average	Good
Spoof	No	No	Yes	Yes
Face	No	Yes	No	Yes
Accuracy	Medium	Average	Medium	Medium
Cost	Low	High	High	High

TABLE IV. PERCENTAGE OF PRECISION ACCURACIES OBTAINED BY DIFFERENT MODELS

Features	Proposed ADRS	Finger, Iris, Odor systems [19]	FLDNet [21]	Multimodal [23]
Aadhaar	94.39	92.31	85.32	87.77
Passport number	90.39	67	76.32	89.11
PAN	85.32	79.32	57.21	45.32
Fingerprint	96.39	90.12	97.21	94.23

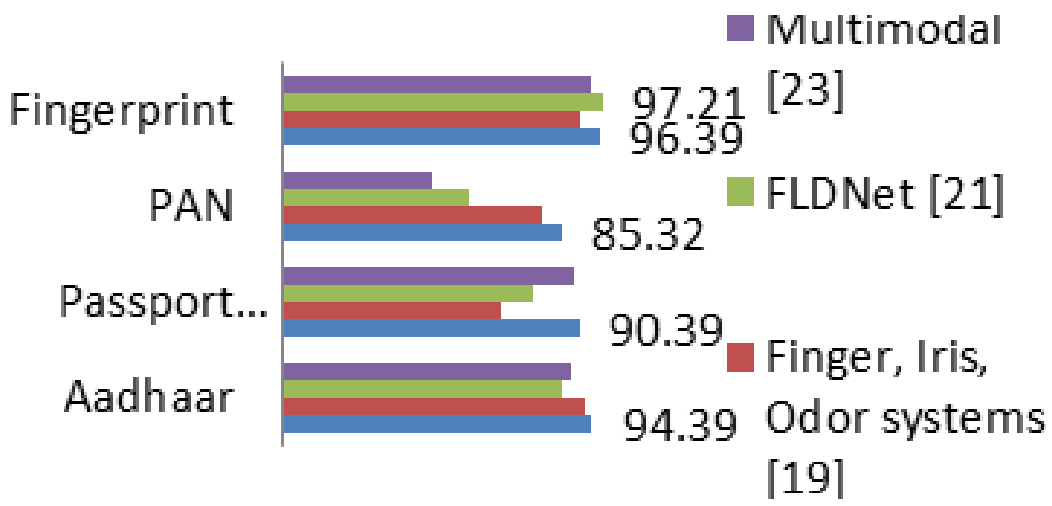

Figure 5. Histogram comparison of ADRS model with other models

unique identification that helped us in forming of ADRS datasets of Students, Teaching and non-Teaching Faculty members that helped us to test the proposed ADRS system [20].

References

[1] S. A. Khan and S. Naaz, "Road safety in india: Status report 2020, transportation research and injury prevention programme," in *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, ser. ICIMIA '20. Morroco: IEEE, 2020, pp. 525–530.

[2] Y. Zhang, S. Pan, X. Zhan, Z. Li, M. Gao, and C. Gao, "Fldnet: Light dense cnn for fingerprint liveness detection," *IEEE Acess*, vol. 8, pp. 84 141–84 152, Apr. 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9079882

[3] E. Sujatha, J. S. Sathiya, P. Deivendran, and G. Indumathi, *Multimodal Biometric Algorithm Using IRIS, Finger Vein, Finger Print with Hybrid GA, PSO for Authentication*, ser. Lecture Notes on Data Engineering and Communications Technologies, A. Khanna, D. Gupta, Z. Pólkowski, S. Bhattacharyya, and O. Castillo, Eds. Berlin Heidelberg: Springer Singapore, Jan. 2021, vol. 54.

[4] R. H. Sir Edward, B. A. H. Khan, and B. H. B. Rai, "Accidental deaths suicides in india," 2020. [Online]. Available: https://ncrb.gov.in

[5] N. F. S. T. C. (NFSTC) and O. Occupational, Research Assessment,

"National missing and unidentified persons (namus)," 2022. [Online]. Available: https://www.namus.gov/dashboard?nocache=

[6] "Missing persons by state," 2022. [Online]. Available: https://worldpopulationreview.com/state-rankings/missing-persons-by-state

[7] UIDAI, "Aadhaar registered device specifications – rule book," 2021. [Online]. Available: https://uidai.gov.in/images/resource/Aadhaar_Registered_Devices_2_0_4.pdf

[8] k. Sauerwein, B. S. Tiffany, W. S. Dawnie, and B. B. Chris, "The effect of decomposition on the efficacy of biometrics for positive identification," *IEEE Acess*, vol. 62, pp. 1599–1602, Feb. 2017. [Online]. Available: https://pubmed.ncbi.nlm.nih.gov/28240354/

[9] W. Elizabeth, "Unlock of iphone after a person dies," 2017. [Online]. Available: https://www.wtsp.com/article/news/nation-world/yes-a-dead-person-can-unlock-an-iphone-if-detectives-act-fast/507-490873582

[10] K. Arvind, K. Mahesh, and K. S. Rishabh, "Identification of unclaimed dead bodies- a possible aadhar based solution," *IP International Journal of Forensic Medicine and Toxicological Sciences*, vol. 3, pp. 74–76, 2018.

[11] M. A. Mahmood, K. Moizuddin, and R. Lakshmi, "Framework for surveillance of instant messages in instant messengers and social neworking sites using data mining and ontology," *IEEE-Student's Technology Symposium*, pp. 297–302, 2014.

[12] "The history of fingerprints," 2022. [Online]. Available: https://onin.com/fp/fphistory.html

[13] K. N. Win, K. Li, J. Chen, P. F. Viger, and K. Li, "Fingerprint classification and identification algorithms for criminal investigation: A survey," *Future Generation Computer Systems*, vol. 110, pp. 758–771, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X19315109

[14] P. Woodman, R. Julian, C. Spiranovic, and K. Ballantyne, "To trace or not to trace: A survey of how police use and perceive chemical trace evidence," *Forensic Science Journal*, vol. 309, pp. 1–12, 2020.

[15] P. Prabhakar, "Tracing biometric assemblages in india's surveillance state: Reproducing colonial logics, reifying caste purity, and quelling dissent through aadhaar," *Scripps Senior Theses*, vol. 1533, pp. 758–771, 2020. [Online]. Available: https://scholarship.claremont.edu/scripps_theses/1533/

[16] N. Evans, "Handbook of biometric anti-spoofing: Presentation attack detection," *Springer*, vol. 1533, p. 519, 2019. [Online]. Available: https://www.springer.com/gp/book/9783319926261

[17] W. l. Sera, A. M. Mamas, and a. et, "Applications of digital technology in covid-19 pandemic planning and response," *Elsevier*, vol. 2, pp. 435–440, 2020. [Online]. Available: https://www.thelancet.com/journals/landig/article/PIIS2589-7500(20)30142-4/fulltext

[18] K. Kenneth and J. S. Wayne, "Nist biometric image software(nbis)," 2015. [Online]. Available: https://www.nist.gov/services-resources/software/nist-biometric-image-software-nbis

[19] J. Priesnitz, C. Rathgeb, N. Buchmann, and et al., "An overview of touchless 2d fingerprint recognition," *Journal of Image Video Processing*, vol. 8, 2021. [Online]. Available: https://doi.org/10.1186/s13640-021-00548-4

[20] M. A. Mahmood, "Datasets of aadhaar details," 2022. [Online]. Available: https://www.dropbox.com/s/fc304xcktg44yzo/MJ%20College%20student%20and%20staff%20biometric%20IDs%20%20March%202021.zip?dl=0

[21] P. Birajadar, M. Haria, P. Kulkarni, S. Gupta, P. Joshi, B. Singh, and V. Gadre, "Towards smartphone-based touchless fingerprint recognition," *Sadhana*, vol. 44, p. 161, 2019. [Online]. Available: https://doi.org/10.1007/s12046-019-1138-5

[22] D. Durga Bhavani, K. Rajeswari, and N. Srinivas Naik, "Big data analytics on aadhaar card dataset in hadoop ecosystem," in *First International Conference on Artificial Intelligence and Cognitive Computing*, R. S. Bapi, K. S. Rao, and M. V. N. K. Prasad, Eds. Singapore: Springer Singapore, 2019, pp. 459–466.

[23] T. Lillicrap, J. Hunt, A. Pritzel, N. Heess, T. Erez, Y. Tassa, D. Silver, and D. Wierstra, "Continuous control with deep reinforcement learning," 2015. [Online]. Available: https://doi.org/10.48550/arXiv.1509.02971

[24] "Fingerprint biometric scanner using php," 2015. [Online]. Available: https://github.com/AyushKaul/Biometric-Fingerprint-Integration/blob/master/Biometric_match.php

Mohammed Mahmood Ali Mohammed Mahmood Ali received Doctor of Philosophy, Ph.D.(cse) from University college of Engineering, Osmania University in 2017. He had completed his M.Tech in Software Engineering from J.N.T.U(H) in 2008 and A.M.I.E., Engineering from Institution of Engineer (India) in 2004. He is an active researcher. He has been guiding Ph.D, M.Tech and B.E students and has more than 26 publications to his credit in International Journals and Conferences of IEEE, Springer & Inderscience. Presently,serving as reviewer for reputed journals like IEEE Transactions Systems, Man, Cybernetics (Part-C), Springer Nature Journal (Institution of Engineers), IJCDS, IJECE and IJEECS. I am one of the Journal editors of ICCCT conference proceedings. His areas of research include Social Network Analysis, Surveillance of Social media, Data Science and Machine Learning.