IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

An Integrative Approach for Multipurpose USID Framework Using Radio Frequency Identification: Securities and Challenges

Yogesh Pal[1], Dr. Neeraj Kumar Tiwari[2], Sujeet N. Mishra[3]

Student, Faculty of Computer Science & Engineering, SRMU, Lucknow-Deva Road, India[1,3]

Assistant Professor, Faculty of Computer Science & Engineering, SRMU, Lucknow-Deva Road, India[2]

Abstract: Every single soul in this world has its own identity, whether they are of any religion or any motherland. The Unique System ID card for humans currently revolves around textual, image and biometric information. People across globe possess multiple identification cards for their uniqueness to vote, travel, economic activity, driving vehicles etc. But there are problems such as multiple cards issued to single person for same purpose burdens government work. Our proposed model reduces all the conflict issues like Forgery, Privacy, Security, Theft, and Loss of Cards.

Keywords: National ID, Smart card, RFID Tags, Biometric, DNA, API.

I. BACK GROUND

National ID cards for Unique Identification have long been advocated as resources to enhance national security, debunk probable terrorists, and guard against illegitimate immigrants. National ID Cards are in use in many realms around the world together with supreme European countries, Hong Kong, Malaysia, Singapore and Thailand. Presently India;

The Aadhar Project was sold to the public based on the claim that enrolment was “Controlled”. This basically meant that there was no legitimate obligation to enrol. The government and the Unique Identification Authority of India, however, worked, overtime to create a practical compulsion to enrol:

National ID card was made mandatory for an ever-widening range of facilities and services. It became clear that National Id card is very important to Economic development and Security of country, without National Id Card life would soon be very difficult. Lawful or Practical, compulsion is compulsion.

II. INTRODUCTION

In this study we reduce the Aadhar coup and to create model of Secured multipurpose Unique System ID card framework with the help of technologies.Our proposed model reduces all the conflict issues of Aadhar Card like Forgery, Privacy, Security, Theft, Loss of Cards, which shrink problems such as multiple cards issued to single person for same tenacity encumbrance’s government work.

The national e-governance strategy in India, formerly known as Unique Identification Number (UID) ambitions to make our wellbeing structures more manageable and fair to every citizens of India.

TABLE:I FEATURES OF AADHAR CARD

Aadhaar work as	Aadhaar not work as
A 12-digit unique identity for every Indian individual, including children and infants	Just another card like multipurpose card
Aadhaar will provide only identity.	Aadhaar will replace all other IDs
UIDAI will give Yes/No answers to any identity endorsement queries	UIDAI information will be accessible to open and sequestered agencies
Establishes uniqueness of every individual on the basis of demographic and biometric information	Collects profiling information such as caste, religion, and language
Aadhar work as only identity record of person	It can replace other type of USID system which store all information of person with high security system.
Some biometric techniques adopt which is suffer from problem like	Every human being already carries their own personal identification in the form of DNA.
Authenticate against resident's data in UIDAI's CIDR	Authenticate against data stored on a smart card
Require Aadhaar for every authentication request reducing transaction to L:l-match	Search for Aadhaar based on details provided requiring 1:N match
Return response to requesting agencies as Yes/No	Return personal identity information of residents

The many countries have considered or are considering again their approach towards formulation of Unique System ID card (USID). But there are growing fears about the possible loss of privacy, freedom, and data security. The new technology could increase defense power more than it should be.

In this study we developed a framework for a unique identification system using integrative approaches with the help of RFID technology and biometrics. USID framework provides access of user's identity at both the local and global level along with high level security.

Both contactless smart cards and RFID use radio frequencies for communicating between the card and reader. The applications for which RF is used can be different for RFID and smartcards.

III. NATIONAL ID IN THE FORM OF SMART CARD

The National ID will be comparable to a Social Security Number in the US; at contemporaneous, multiple IDs are in use in India – voters ID card, ration card, driver's license, passport, , PAN card for taxpayers. There have been numerous illustrations of both fake ID cards being used by terrorists and criminals that have been used for gaining mobile phone connections etc. All through the contemporary wide-ranging elections in India, there were booms of Voter ID cards with mistakes as well. The Identification problem is this – no single ID is ample, and each depend on another form of authentication. There is a need for amalgamating all of these into a single ID. At the same time, the government needs to ensure that these IDs are not replicable (fortification of identity), and access to information about individuals is limited (privacy).

The Epoch of identification technology—biometrics, RFID tags, identity cards, surveillance, databases, and records—impends privacy, civil liberties, and related human interests. Since the terrorist assaults of September 11, 2001, anxieties for identification in the name of security have increased. A national ID characterizes a assignment of supremacy from individuals to establishments, and that transfer may impend our permission, subject people to unsolicited surveillance and a uniform, government-controlled identification system.

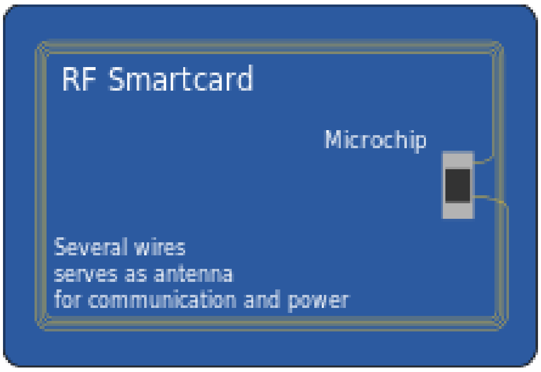

Fig. 1. Example of Smart Card

A. National Policy Of India about ID

Bestowing to Privacy International, as of 1996, custody of identity cards was unavoidable in about 100 countries, though what constitutes "compulsory" varies. It is unavoidable to have an identity card when a person ranges a recommended phase. The forfeit for non-possession is frequently a fine, but in some personal belongings it may result in incarceration until identity is established. For people doubted with crimes such as mugging or no bus ticket, non-possession might result in such imprisonment, also in countries not law fully necessitating identity cards. In drill, indiscriminate authorizations are rare, except in certain times. Companies and government constituent part may issue ID cards for security devotions or proof of a prerequisite.

India has the policy as Multi-purpose national identity cards; resonant 16 digit personal details and a unique identification number are issued to all voters since 2007. Biometric data such as fingerprints and a digital signature are delimited in a microchip implanted in the card. On it are details of the holder's date and place of birth and a unique 16-digit Countrywide Identification Number. The card has a SCOSTA QR code entrenched on the card, over and done with which all the details on the card are manageable.

B. Reimbursements Of National ID as Smart Card

Different substitute, not as much of secure ID card technologies (such as magnetic stripe, RFID), smart card technology maintenances various unique topographies that can make stronger the security and privacy of any ID system. Singlehanded essential characteristic of a secure ID system is the facility to yoke the separable owning an identity document securely to the document, in consequence providing strong authentication of the individual's uniqueness.

Smart card technology ropes PINs, biometric influences, and chromatic identity verification. Smart cards upkeep the encryption of sensitive data, both on the testimonial and all through communications with an external reader. Smart cards discourage forgers and can ensure that only the person to whom the card is allotted will be gifted to verify themselves when the card is accessible. No other technology can offer such secure, trusted, and cost-effective identification capabilities. Smart card tools can maintenance the additional applications that heighten citizen convenience besides/otherwise government service adeptness.

Smart cards can provide the unique ability to effortlessly trust identification and authentication in mutually the physical and digital worlds. This proficiency can generate major savings for country. A smart card-based ID system can be set up economically at multiple locations by using small, secure, and low-cost portable readers that take advantage of the smart card's capability to provide offline identity verification. Furthermore, the facility of smart card technology to support supplementary applications can

DOI 10.17148/IJARCCE.2016.5467

generate both cost savings and potential new profits sources. In accumulation, smart card technology is supple. Contrastingin this time printed plastic cards; smart cards can be modernized and succeeded throughout the life of the card which is very valuable to National ID card.

IV. RESEARCH APPROACH

The ultimate intention of this study is to design Unique System of Identification framework for human who is accessible as globally and local area with the help of inherits the technologies for example smart card technology, biometrics, and API and RFID tags.

A. RFID Tags And RFID

Safekeeping and Confidentiality apprehensions in Radio frequency identification (RFID) technology particularly RFID Card, is a widespread research area which have engrossed researchers for over an epoch. Verifying users at the Card end of the RFID technology establishes one of the foremost sources of attacks on the system. It does in advance the essential of augmented visibility, updated tabularization management and decreased labour levels. According to the modern information standards, Wal-Mart has been one of the privileged in the great weighbridge adoption of RFID technology [1]. According to the study work of Roy Want in [2], “Radio Frequency Identification Technology (RFID) has been technologically advanced from complexity into main stream applications that let us help to rate the manipulating of assembled figures and stocks facts”. The preliminary step for the development of RFID was during World War II, when the British operates it to identify whether planes belonged to “friend or enemy”. Some technical hitches resulted in the gunning down of connected planes and since then the use of RFID was restricted to Defence and armed forces trades due to the cost factors. New progressions in science and technology have enabled practice in profitable applications. Enormous institutions, such as the US Department of Defence, have since realized RFID which is now dispersal to other organizations and Multi-National companies [2]. Wal-Mart is the world’s second prevalent user of RFID and devoting weighty resources to develop its highly effective applications**.** RFID technology manoeuvres at multiple frequencies counting low, high and ultra-high. The frequency that is being carried out determines the distance in which RFID tags can be dignified, how many tags can be construed at one time, how fast these tags are intended, and how can application framework will impact its performance.

Radio frequency identification (RFID) tags are used in a widespread range of applications such as:, tracking goods, identifying animals through the supply chain, tracking assets such as gas bottles and beer kegs, and controlling admittance into buildings[3]. RFID tags contain a chip that stereotypically stores a static number (an ID) and an antenna that permits the chip to transmit the stockpiled number to a reader. Some RFID tags surround read/write memory to store data that can be engraved to the tag. When the tag comes within assortment of the proper RF reader, the tag is powered by the reader’s RF field and transmits its ID to the reader.

B. Biometrics Technology In Smart Card for National ID

Biometrics improvements to automatic identity authentication of a person on a basis of one’s unique biological or behavioural features [4].The Unique Identification Authority of India (UIDAI) has been produced with the mandate of providing a Unique Identity (Aadhaar) to all residents of India. Aadhaar enrolment has picked up momentum with over 27,000 enrolment stations conducting 10 Lakh enrolment severy day across the country. The CIDR processes these enrolments by de-duplicating them to guarantee uniqueness and then concerns Aadhaar numbers. One of the mandates given to UIDAI is to define usages and applicability of Aadhaar for delivery of several services. Towards Aadhaar-enabled delivery of services and applications, UIDAI provides online authentication using the resident’s demographic and biometric information [5].

C. Finger Prints Biometric

Fingerprinting is the biometric technique that is most commonly used in securing system. Fingerprinting was not a new notion as it was previous born in 14th century in China. Chinese exporters used this technique in stamping’s their children palm prints along with the footsteps for identify them contrarily. Later these from last three eras, this technique had brought rebellion in security field either it is concerning to computer system or any of the automated system where security is a for emostanxiety. Finger printing an spitting image of finger has been taken and stored in the database as a prototype.

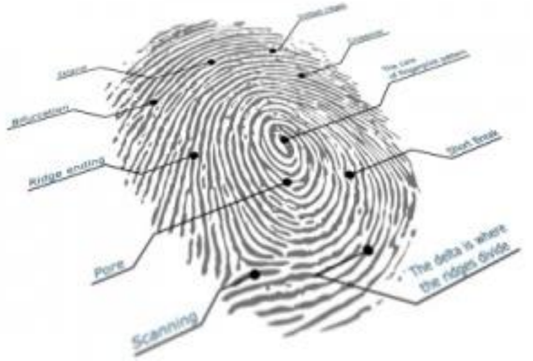

Fig.3. Finger Print

The essential challenge of this technique is to uphold and spotless the optical surface of scanner so that it would simply scan and match the pattern of any separable [6].HP (Hewlett-Packard) developed the first manufacturer to add biometric identity examination to electronic portable device, when its constructed small fingerprint scanner into its HP PDA [7, 8,].As nobody of the technique is ideal so it could be possible that somehow someone could tricks the imitation fingerprint in place of claim’s identity pattern. Recently fingerprinting introduced through memory stick fingerprint scanner commonly used in corporate sector. But there could be lot of works that has to be done apropos fingerprinting.

DOI 10.17148/IJARCCE.2016.5467

D. IRIS Recognition for Biometrics Techniques

Biometric identification clarification grounded on iris reading was combined with foreseeable authentication ways and means to accomplish more secure communications and computers better vanishing. The human iris, an annular portion between the pupil (generally, seeming black in an image) and the white sclera [9]for that reason iris is not retina.

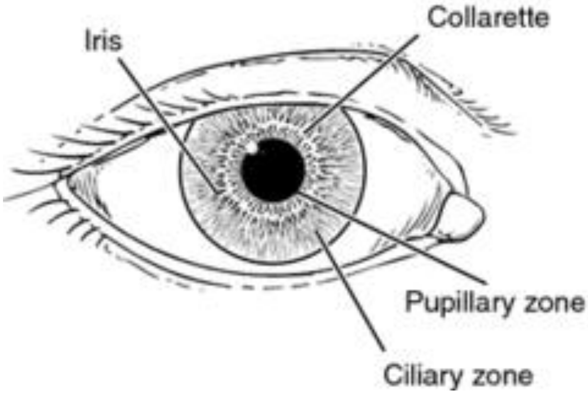

Fig.4. Iris For Biometric

The possibility of verdict two irises is neighbouring to zero. Consequently the iris appreciation system is very reliable and stable and could be used in greatest secure places. Numerous applications that require some degree of sureness concerning the personal identification of the people complicated, such as banking, computer network access, or physical access to a protected facility, are moving away from the use of paper or plastic identity cards, or alpha-numeric passwords system. These systems are too easy to downfall. In the meantime the iris is an superficially observable organ, iris based personal documentation systems can be non-invasive to their users which is of countless rank for real-world applications. Nonetheless there are three technical questions could be haggard to effort with iris recognition. The crucial issue is the IMAGE ACQUISITION. The second subject is to restrict the iris pattern from the apprehended image. Last concern is as normal just to match the recognized pattern of iris with the candidate entry of their iris configuration. In this approach Iris recognition system could be intended and affected. There is slice of things comes across the above defined technical subjects which would be fixed out while the system essentially going to be instigated and established. [10,11].

E. Retinal Recognition in Biometric

Biometrics in allusion to biological sciences is slightly simply observed as "biological statistics" [12].Retinal recognition is careful as the most dependable and effective biometric technique in the difference of others similar face recognition, fingerprint, hand geometry, keystroke dynamics and numerous. Nonetheless as we distinguish along with these techniques we have to make somatic contact on the optical scanner so that it could capture the image of humanoid feature being used and so match the pattern. So to eliminate this enslavement iris and retinal recognition has been superior. Amongst the Iris and retina, it is slight little unclear as they both are too closed tenure. So, to clear this qualm let's have a look at further down diagram.

The complete working of retinal recognition has three parts, head is Image signal acquisition and processing for capturing the image of retina and deviations it into the digital arrangement.

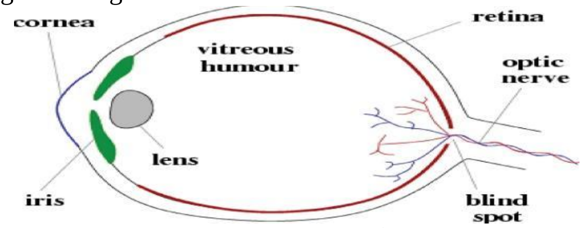

Fig.5. Retina position in eye for Biometric

Lastly signify the unique feature of retina of any distinct as and pattern. As this procedure is same as other biometrics methods but then in retinal recognition the image acquisition and processing is fairly a difficult charge. Its straightforwardness is wholly be contingent on the user constancy towards the scanner as user has to fix their position exact adjacent to lens.

F. DNA Technology

DNA technology justifies special declaration from a development viewpoint. Since DNA is the only biometric that can be reserved at birth and is stable over a lifetime, it agreements the possibility that persons can be finally linked to the crucial documentation of their survival—the birth document. The biometric pointers used by this technology purportedly deliver little or none of the individual niceties encoded in DNA, and are thus no more invasive than any other physical characteristic such as fingerprints. Though, rapid DNA assessment is still costly and not yet deployable on a physique scale.

Progressively, some view DNA as a robust applicant for the growth in biometrics because of its unique and unchangeable character, i.e., everyone's DNA is dissimilar and it cannot be alteredimpartial.DNA is the biochemical code and the heritable quantifiable initiate in the cells of the body. It is current in all the cells counting white blood cells, semen, hair roots, bone, teeth and other body nerve. DNA bits can be detected in body fluids as well, such as blood, semen, saliva, and perspiration. It is sole to each separate and because of this stuff it can be used in scientific soundings. The progression of analysing a DNA taster and procurement a profile contains of four steps: group, intensification, extraction and sequencing.

G. Cloud And API Technology with Smart Card

A cloud computing is the most important mechanism since the Internet going forward. Cloud computing environs, consumers uses an authentication system to use the cloud services through a Web-based user interface and web browser application programming interface (API). Validation on the cloud is necessary to provide secure right of entry to the cloud services by official users only.

DOI 10.17148/IJARCCE.2016.5467

At current, verification is done in different methods, such as a meek text password. Cloud computing is the greatest recent emergent for retrieving computing resources. Cloud is a throng of computer resources and provides a billion of services to its user instantaneously. A Cloud offers a friendly environment to its user and numerous services such as Software as a service (SaaS), platform as a service (PaaS), and Infrastructure as a Service (IaaS).

So this opportunity we can use for Smart Card as national ID for the purpose of online and offline services in the framework.

V. PROPOSED METHOD

The goal of proposed method is identity; to reduce the risk that a person is incorrectly denied access, is incorrectly granted access, or is not detained, depending on the particular. This Multipurpose smart cards is manageable, easy to use and offer paperless communications. Associated to other traditional ID like Aadhaar, Voter ID, Pan Card etc., they can be used to as multipurpose as single card. By this framework we implemented well National ID with the aim of improvement service delivery systems to cut out middlemen, corruption and bring services to closer to end users and legatees. This framework is capable of storing all data of user as per requirements ; range of beneficiary data such as name, address, photographs as well as biometric information, it can help in tracking, beneficiary selection, identification and targeting under anti-poverty program.

The main aim of this framework is to reduce the fault of Aadhaar Cards with the approach of smart card technology, biometric, DNA etc. for security of India National ID card.

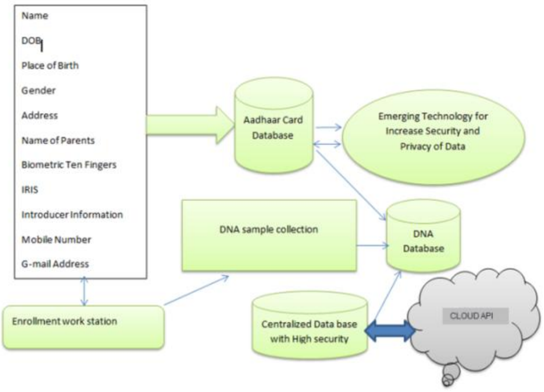

Fig.5. Proposed System Diagram For USID Framework.

VI. CONCLUSION

The modular design successfully framed to show relevance of Biometrics with DNA for more uniqueness in USID to put added layer of security. With help of advance security technologies and internet availability, the integrative approach helps to translate (with the help of API) state of botheration to government. Relying on multiple IDs will become thing of past.

ACKNOWLEDGMENT

We are thankful to all the Faculty members of Computer Science and Engineering Department, **Shri Ramswaroop** Memorial University Lucknow Uttar Pradesh for their incentive and unremitting support and our special vote of thanks to **Dr. Bineet Gupta** for their appreciated recommendations and contributions.

REFERENCES

[1]. Gowher Mushtaq , Yogesh Pal and Neeraj Kumar Tiwari, “Radio Frequency Identification Upon Near Field Communication And Far Field Communication For Next Generation Wireless Network Infrastructures,” TNC, United Kingdom, Vol. 3 Issue 3, 2015,ISSN:2054-7420

[2]. W.S. Chen, K.-H. Chih, S.W. Shih and C.M. Hsieh, “Personal Identification Techniques based Human Iris Recognition with Wavelet Transform,”IEEE, ICASSP, 2005, pp. II -949.

[3]. “Role of Biometric Technology in Aadhar Authentication”,UIDAI(2009-2012)

[4]. Akash Srivastav and Vedpal Singh, “Biometrics Based Identification Techniques,”Journal of Global Research in Computer Science, Vol. 2, No. 11, November 2011.

[5]. Anil K. Jain, Arun Ross and Salil Prabhakar, “An Introduction to Biometric Recognition,” IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image and Video Based Biometrics, Vol. 14, No. 1, January 2004.

[6]. Richard P. Wildes, Member, IEEE “Iris Recognition:An Emerging Biometric Technology,” October 31, 1996; revised February 15, 1997.

[7]. B. Sowmyaand S.L. Sreedevi “Iris Recognition System for Biometric Identification,”IJETTCS, ISSN 2278-6856.

[8]. B.H. Juang and Lawrence R. Rabiner, “Automatic SpeechRecognition - A Brief History of the Technology Development,”2011.

[9]. S. Prabhakar, S. Pankanti, and A. K. Jain, “Biometric Recognition: Security and PrivacyConcerns,” IEEE Security and Privacy Magazine, Vol. 1, No. 2, pp. 33-42, 2003.

[10]. Smart Cart Alliance Identity Council, “Identity and Smart Card Technology and Application Glossary,” 2007 (http://www.smartcardalliance.org)

[11]. M.A. Jobling and P. Gill, “Encoded evidence: DNA in forensic analysis. Nature reviews,” Vol. 5, 2004, pp. 739-751

[12]. H. Dinesha and V. Agrawal, “Multi-level authentication technique for accessing cloud services,”International Conference on Computing, Communication and Applications (ICCCA), 2012, pp. 1-4.

BIOGRAPHIES

Yogesh Pal (September 15,1994was born in Bhongoan, U.P.,India), M.Tech Student, Faculty of Computer Science and Engineering in Shri Ramswaroop Memorial (SRM) University, Lucknow Deva Road, UP, India. He has completed Dissertation in the area of Computer Science Engineering and Communication Technology. He is interested in pursuing career in government Civil services and preparing for the same apart from academic research.

Dr. Neeraj Kumar Tiwari (June 10, 1982; Unnao-INDIA) is an Assistant Professor, Department of Computer Science and Engineering in Shree Ramswaroop Memorial (SRM) University,

DOI 10.17148/IJARCCE.2016.5467

Lucknow Deva Road, UP, India. He is actively working in the area of ICT including Green Communication and E-Health. He has published more than 40 research publications and several papers were indexed in IEEE Explore, Elsevier, Springer, Science Direct, Willey Blackwell etc. He has established a correlation between the exposures of electromagnetic radiation (EMR) though wireless communicating devices or mobile phones and associated possibilities of Electromagnetic Hypersensitivity in terms of self-reported symptoms and sensations in different ethnicity.

Dr Tiwari is active member of more than 50 National and International professional bodies related to health, engineering and communications. Some of them are Health Physics Society, USA, International Society for Neurochemistry, UK, Organization for Computational Neuroscience, USA, International Brain Research Organization, USA, Society of Neuroscientists of Africa, Africa, Movement Disorders Society, USA, International Association of Engineers etc.

Sujeet N. Mishra (August 8, 1989; Jaunpur-India) is M.Tech Student, Faculty of Computer Science and Engineering in Shri Ramswaroop Memorial (SRM) University, Lucknow Deva Road, UP, India. He received his Bachelor of Engineering degree from Terna Engineering College, Mumbai University in 2012. He has completed Dissertation in the area of Human Resource Predictive Analytics. He is an active participant of research activities involving Data Science, ICT, Machine Learning, DBMS and Governance &Social Awareness.

DOI 10.17148/IJARCCE.2016.5467