UTILIZATION OF MOBILE TECHNOLOGY AND SECURITY ALOGRORITHMS TO PREVENT FORGERY OF NATIONAL IDENTITY CARDS OF THE CITIZENS OF SRI LANKA - A CONCEPT PAPER

M. Punchimudiyanse[1*]

[1]*Department of Mathematics and Computer Science, The Open University of Sri Lanka*

INTRODUCTION

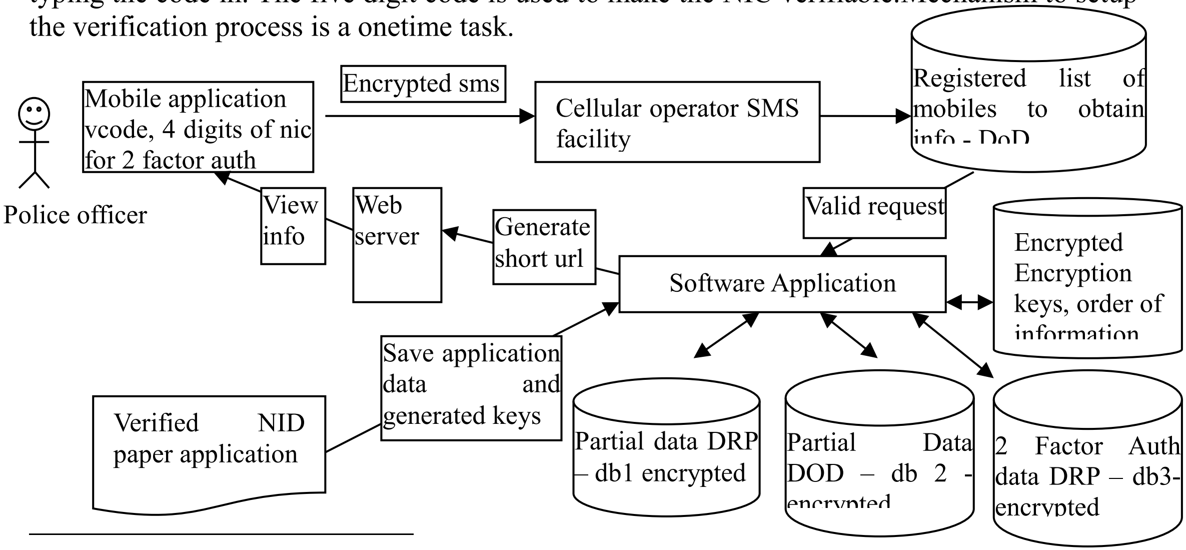
The National Identity Card (NIC) of a citizen of Sri Lanka is a handwritten paper with a lamination. The latest initiative is to issue smart ID by year 2016. Due to infrastructure and structural changes and associated cost, previous plans have still not come to fruition. Currently the same old mechanism is in use and several scams producing illegal NICs have been discovered.

A tedious document validation mechanism exists when obtaining a legal NIC, but forging it is an easy task. The photo could be swapped, and there is no quick verification mechanism for current NIC by a law enforcement authority when it is produced for verification. Any fraudulent person who is has access to printed material can produce a NIC which can go unnoticed.

The aim of this paper is to present a low cost mechanism to prevent forgery of NICs devised from existing security and mobile technologies. The proposed mechanism would make a minimum change to existing NIC and its production mechanism. It makes an NIC authenticable over a mobile phone, prevents changing of data at the Department of Registrations of Persons (DRP), Department of Defense (DoD) and prevents fraudulent persons taking advantage of the NIC verification system as well.

METHODOLOGY

The author proposes to print a code (Vcode) with five alpha numeric characters in several locations of a NIC to prevent defacing or smudges if printed in a single place. Vcode comprises a combination of a-z, A-Z, 1-9 excluding letters l,o,O (59 different characters). Approximately 714 million (59^5) different combinations exist for a five character Vcode which exceeds requirement of a little over 20 million population for Sri Lanka. A QR code (ISO/IEC 18004 June 2000) could be printed for easy reading by a mobile phone without typing the code in. The five digit code is used to make the NIC verifiable.Mechanism to setup the verification process is a onetime task.


Police officer
Mobile application vcode, 4 digits of nic for 2 factor auth
Encrypted sms
Cellular operator SMS facility
Registered list of mobiles to obtain info - DoD
View info
Web server
Generate short url
Valid request
Software Application
Encrypted Encryption keys, order of information
Save application data and generated keys
Verified NID paper application
Partial data DRP – db1 encrypted
Partial Data DOD – db 2 - encrypted
2 Factor Auth data DRP – db3-encrypted

[*] Correspondences should be addressed to Mr. M. Punchimudiyanse, Department of Mathematics and Computer Science, The Open University of Sri Lanka (email: malinda@ou.ac.lk , Tel : 0112881098)

Any information pertaining to the citizen could be kept such as finger print information, blood type and retina scan information as done in the ID card scheme in India which could be encrypted by a public key of the Department of Registration of persons then stored in database. The author proposes having two different databases, one in Dept of Registration of Persons and other in Department of Defense (DoD) to prevent IT aware people from tampering with the data.

Information fields contained in an NIC has to be ordered as a single string. Eg. Full name, other names, birthday, birth location, occupation and the address, issue date, national ID number, CRC hash code of the photo generated from a hashing algorithm CRC32 (Williams 1993) and a time stamp to prevent unauthorized updates. The entire string has to be again encrypted by an algorithm like blowfish (Schneier 1993) with appropriate key. Author recommends using blowfish / two fish algorithms because this algorithm has not broken yet and the implementation is open. Half of this encrypted personal information string (EPS) has to be stored in the Department of Registration of Persons and the other half has to be stored in a database of Department of Defense (DoD) so that either party cannot make any unauthorized alterations.

Vcode is generated using the characters generated by CRC hashing (Boyd 2012) along with digits in NIC number. If duplicate vcode is generated then padding is introduced to the original information string and regenerates EPS and Vcode. The ordering of the data fields change randomly (by a software application) from person to person but the order of which information is lined up is also kept in a separate database along with the key used for encryption. This information has to be again encrypted by blowfish algorithm with a key larger than 12 characters.

The four consecutive digits of NIC number has to be kept separately hashed by a latest SHA algorithm (for the purposes of two step verification (eg. For 885432234v hash codes of 885432234v, 8854, 8543, 5432, 4322, 3223, 2234 has to be stored with 5 character verification code). This entire process is driven by a software and it could be done only once per application. Any update should be prohibited. To remove a record proper statutory procedure involving at least two designated officers and one random officer picked by the software is proposed. To access the system access card of the employee, pin and a remote approval from Officer in charge for the day is required.

Stored in Department of registration of persons in two distinct databases

5 character vcode	1st Half of EPS	CRC of EPS	CRC of Photo	Hash of NIC

5 character vcode	Encrypted encrypt key of EPS	Encrypted order of fields	photo

Key used to encrypt the key used for EPS has to be strictly protected, possibly keys should be generated from the local language to prevent foreigners using dictionary attacks. Following fields are required for 2 step verification

5 character verification code	Hash of NIC	Hash of 1st 4 digits	Hash of 2nd 4 digits	Hash of 3rd 4 digits	Hash of 4th 4 digits	Hash of 5th 4 digits	Hash of 6th 4 digits

Stored in Department of defense (db 2)

5 character v code	2nd Half of EPS	CRC of EPS	CRC of Photo	Hash of NIC

In addition database of people who are authorized to verify the NICs has to be maintained at Department of Defense or at any other secure location.

When the person presents their NIC to a law enforcement officer, he should use a software installed in his phone to verify it by entering vcode printed in a NIC along with 4 consecutive digits of NIC number. These 4 digits were again randomly asked to prevent misusing the facility as well as typing mistakes of vcode.

Five character verification code and the 4 consecutive digits of NIC is then encrypted by blowfish with pin of requester as the key. It will be sent to a requester verification server which verifies the authenticity of the requestor from its database of registered mobile number, pin and phone IMEI number. Then the server will contact the Department of Registration of persons database via a secure link to obtain information using the 5 digit verification code and hash of 4 digits of the NIC number. It will generate a temporary url or MMS to the requester providing the verification information. The officer can verify the ID by comparing details received by him with the NIC at hand.

RESULTS AND DISCUSSION

Analyzing and choosing the right combination of strong security algorithms / technologies which are not commercially bound to any country or a company which are stated in this paper was the work carried out by the author. The idea is given as the concept paper and it is open for discussion for possible flaws. Several scenarios presented under results and discussion where this mechanism would prevent illegal activities even by parties who manage this system.

Table 1 – How this approach solves different problems associated with current NICs

Problem	**How the proposed approach address the issue**
Verification of NIC	This approach solves the problem. Any government entity or road side police officer can verify NIC using a average mobile phone No need to provide official mobile phones existing mobile of the officer would be sufficient.
Police officer enters arbitrary vcode	With 2 step authentication officer has to enter 4 digits of actual NIC number. Therefore misuses could be avoided.
Verification officer's mobile device is stolen	With officer's pin system is secured. Using the sim in different phone will not work because the system requires registered phone.
Attempts to change the photo by NIC holder or any personal detail by an employee of department of registration of persons	System sends the actual photo via MMS or accessed via short URL. User cannot affix a new photograph. Staffer cannot change the photo because CRC is generated with the timestamp of saving the entire record. Personal information string is encrypted. Changing it without using the system will be difficult without the key used for encryption. Deleting the entire record will require authorization of 3 people. 2 designated and 1 random. If it is physically deleted from database server and re entered then the time stamps will reveal the activity.
Unauthorized access to software system.	This could be prevented using two step access mechanism. That is to use the system it requires password and access card of an employee and the approval of the officer in charge for the day. So working in non office hrs could be easily prevented.
Attempts of mobile	This is prevented because of the law enforcement officer pin number

operators to obtain the information as a bulk	and the information sent via SMS is encrypted using officer pin and decrypted at department of defense.
Multilingual facility and user friendliness	Proposed mechanism is a generalized version that supports all three language NICs if hand written as per government directive recently. Only data entry required in at least 2 languages. The user application in mobile could be developed to support all 3 languages and the encryption algorithms do not distinguish between languages.
Migrate existing NIC holders to new system	That would require entering their data to the system and print the verification code and QR code into their NICs.
Cost effectiveness and ease of use	Existing application procedure will be kept intact. Only data entry fee and vcode printing fee is required to be charged. The approach does require a short toll free phone number from a mobile operator. IT infrastructure management cost and the cost for Public/Private keys. But the cost required (SMS/Internet cost) for verification is lot less compared to digital chip card readers. Fraudulent activities of coping digital cards also could be prevented as system always rely on a central database. Sri Lanka has good cellular operator coverage. Use of well established mobile operator will reduce infrastructure cost.

CONCLUSIONS/RECOMMENDATIONS

Information presented in this paper is a group of mechanisms to prevent frauds in existing NIC scheme of Sri Lankan Citizens. Implementation is completely feasible as the selected technologies / algorithms presented in this paper are regularly used in different application domains. A prototype software application to implement the concept will require 2 mobile phones (police officer / SMS gateway), Open Source SMS gateway, Tomcat/ Apache web server, Java / PHP development environment if Linux Operating system is used or Visual Studio development environment for a windows application at DRP/DoD.

REFERENCES

G. Bertoni *et al*. (29 May 2012), Keccak implemetation overview retrieved from **HTTP://KECCAK.NOEKEON.ORG/KECCAK-IMPLEMENTATION-3.2.PDF**

I. Boyd (23 April 2012), Which hashing algorithm is best for uniqueness and speed? retrieved from http://programmers.stackexchange.com/questions/49550/which-hashing-algorithm-is-best-for-uniqueness-and-speed

ISO/IEC 18004. (15-June -2000), Information technology — Automatic identification and data capture techniques — Bar code symbology — QR Code first edition Retrieved from http://raidenii.net/files/datasheets/misc/qr_code.pdf

B. Schneier. (December 1993), Fast Software Encryption, Cambridge Security Workshop Proceedings, Springer-Verlag, 1994, pp. 191-204. Retrieved from http://www.schneier.com/paper-blowfish-fse.html

R. N. Williams. (19 August 1993), a painless guide to CRC error detection algorithms version 3 retrieved from **HTTP://WWW.CSM.ORNL.GOV/~DUNIGAN/CRC.HTML**