Architecture and Insecurity Issues of a Handheld Device

Mohamed Hamdi[1)]

Abstract

Diseases can be prevented by proper immunization procedures, however, with most parents working in this generation and not most clinics pay much attention on the individual planning and notifications of their patients, this research will show a solution to such crucial issue. The research depicts an architectural structure using mobile computing which will plot a chart of vaccination planner synchronous with the parent's personal planner so as to set a schedule amenable to both the parties and a notification through will be generated. This will be a tool for parents and assistance to clinics and hospitals catering vaccinations shots for children.

Keywords: Vaccination, Planner, Handheld Device, Security Threats, Vulnerability

1. Introduction

Mobile technology applications have the capability and potential to improve healthcare service quality as they instantaneously provide critical patient test data, enabling medical staff to render treatment immediately[1[[2][3][4]. Mobile services emphasize full-time information accessibility, real time and service-quality. Thus, mobile healthcare applications are recognized as emerging and enabling services in most countries [5][6][7]

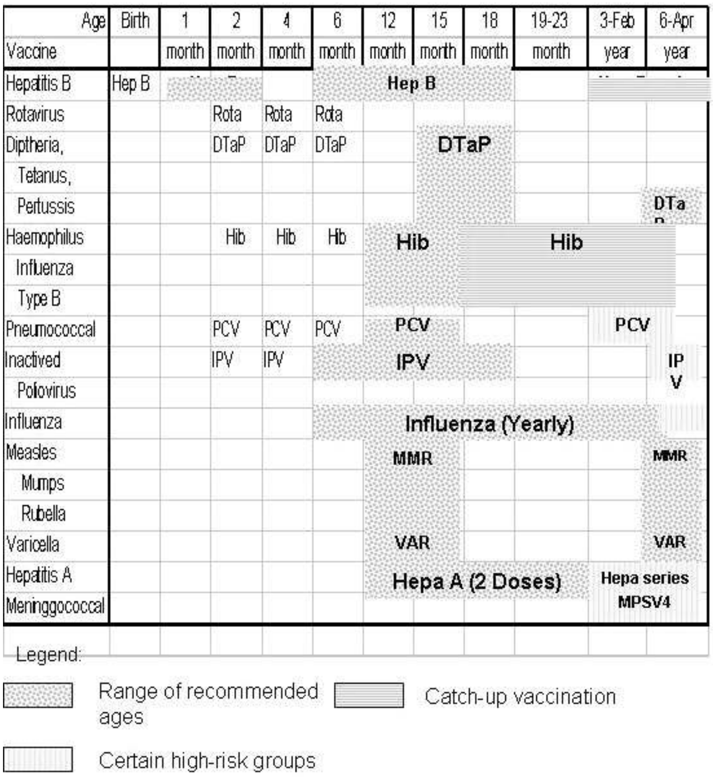
Vaccination is the administration of a vaccine to stimulate a proactive immune response that will prevent disease in the vaccinated person it contact with the corresponding infectious agent occurs subsequently [1]. Thus vaccination, if successful, results in immunization: Vaccination is a highly effective method of preventing certain infectious diseases. For the individual, and for society in terms of public health, prevention is better and more cost-effective than cure. Vaccines are generally very safe and adverse reactions are uncommon. Routine immunization programs protect most of the world's children from a number of infectious diseases that previously claimed millions of lives each year.

Using this vaccination as an issue in healthcare and implementing in a mobile device makes the authors confident enough that this research will be a milestone to a more sophisticated and useful application in the area of ubiquitous healthcare.

Received(September 20, 2010), Review request(September 21, 2010), Review Result(1st:October 03, 2010, 2nd:October 18, 2010)
Accepted(December 31, 2010)

[1]Communication Networks and Security Research Lab. University of November 7th at Carthage, Tunisia
email: mmh@supcom.rnu.tn

[Table 1] Recommended Vaccination Schedule for children 0-6 years



Age	Birth	1	2	4	6	12	15	18	19-23	3-Feb	6-Apr
Vaccine		month	month	month	month	month	month	month	month	year	year
Hepatitis B	Hep B				Hep B						
Rotavirus			Rota	Rota	Rota						
Diptheria,			DTaP	DTaP	DTaP		DTaP				
Tetanus,											
Pertussis											DTa
Haemophilus			Hib	Hib	Hib	Hib		Hib			
Influenza											
Type B											
Pneumococcal			PCV	PCV	PCV	PCV				PCV	
Inactived			IPV	IPV	IPV						IP V
Poliovirus											
Influenza					Influenza (Yearly)						
Measles						MMR					MMR
Mumps											
Rubella											
Varicella						VAR					VAR
Hepatitis A						Hepa A (2 Doses)				Hepa series	
Meninggococcal										MPSV4	

Legend:

▨	Range of recommended ages
▤	Catch-up vaccination
▥	Certain high-risk groups

Most parents have realized the need of administering vaccinations to children. Vaccinations come in different stages and in different age levels. Despite there are catch-up vaccination schedules at different age levels worst is high risk is around the corner. Thus it is just convenient and practical for parents to have a digital aid that will do the appointments with their children's physician instantaneously because parents have tons and tons of work loads and have become preoccupied these in their work these days.

2. Related Studies

Our research are based on the following: Childhood Immunization Schedule, This immunization schedule is based on the 2008 Childhood and Adolescent Immunization Schedule recommended by the Advisory Committee on Immunization Practices (ACIP), the American Academy of Pediatrics (AAP), and the AmericanAcademy of Family Physicians (AAFP). This schedule provides generally recommended dates for immunization based on your child's birth dates. Some diseases or treatments for disease affect the immune system. For children with these diseases or for children receiving these treatments, the recommended immunization schedule may need to be modified. If you have questions or concerns, consult your child's physician or other healthcare professional for advice about your child's immunization schedule.[12]

Another related study to vaccination planner is the eMedCheck; it is an electronic medication screening form that can be run on a PDA. Using this software, POD staff record basic information about family member. The software uses decision rules to determine which medication each person should receive. It also records the results for later analysis.

The objective of such research was to create a mathematical and simulation of mass dispensing and vaccination clinics (also known as points of dispensing or PODs) and to develop decision support tools to help emergency preparedness planners plan clinics that have enough capacity to serve residents quickly while avoiding unnecessary congestion. A poor clinic design will have insufficient capacity and long lines of patients waiting for vaccinations. More patients require more space as they wait to receive treatment. I too many patients are in the clinic, they cause congestion, crowding and confusion.[10]

Vaccine Check Immunization Program is another related study to the one being proposed by the authors. This application is a data unit corporation’s vaccine check interactive immunization program. This unique and important program will create an instant immunization schedule based upon the individual’s age and immunizations history.The displayed schedule may be viewed by vaccine date, including vaccine required today. The schedule may then be saved for future reference.

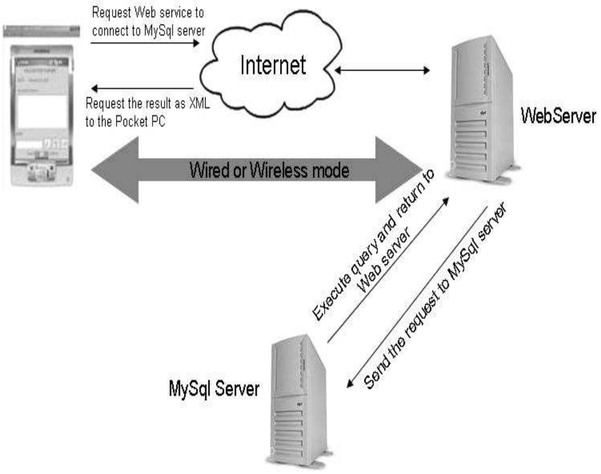
Because of the increasing complexity of childhood and adolescent immunization schedule, including the use of new combination vaccines, health care professionals are faced with a most difficult task to create immunization schedules for children with complex vaccine records, especially for children who have fallen behind.The program makes this process easier and more exact. The Vaccine Check program is an essential resource for all health care professionals involved in vaccine administration.[13]

3. Vaccination Planner Architecture

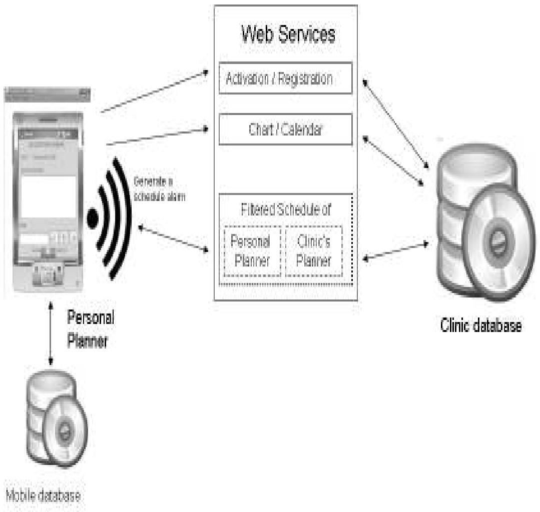
The general architecture of vaccination planner is depicted on Fig.1. The objective of this research is to develop a decision support tool that will help parents to automatically received vaccination shots appointment for their children ages 0-6 years old initially from their Pediatricians. However, it will not only be a conventional type of vaccination schedule from the Pediatrician becauseas an additional feature it will be able to filter the personal planner of the parent using the mobile device as shown in the Software Representation Diagram of Fig.2 and be able to displayed as a blocked calendar in the end of the Web Server. This blocked calendar will be the basis of filtering an amenable schedule both for the parents to bring their children in the clinic for vaccination shots and the child’s schedule base on the its vaccination planner schedule in the Pediatricians portal.

We are exploring applications of personal digital assistant technology to a range of medical applications.

In this research the researchers used a Connected Device Configuration (CDC) since this is for devices with much greater memory, processing power and network connectivity such as smart phones, set-top boxes, internet, and embedded servers. CDC is defined as a specification that has passed through Java Community Process (JCP). The CDC is known as Java Specification Request (JSR) 36. The CDC specification is much smaller document than the CLDC specification because the CDC is much closer to a Java 2 Standard Edition (J2SE) runtime environment than the CLDC.


Request Web service to connect to MySql server
Internet
Request the result as XML to the Pocket PC
WebServer
Wired or Wireless mode
Execute query and return to Web server
Send the request to MySql server
MySql Server

[Fig. 1] Vaccination Planner Architecture



[Fig. 2] Software Representation Diagram

The specification defines four things in particular: [14]

·The capabilities of the Java virtual machine (VM). Unlike the CLDC, the CDC VM is a full-featured VM

·A subset, much larger than the CLDC's, of the J2SE 1.3 classes.

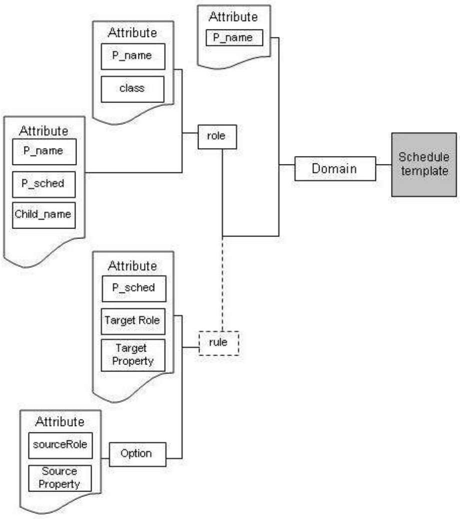
·The same API's (application programming interfaces) that are new to the CLCD

·Support for file-and datagram-based input/output using both the GCF and the familiar java.io and java.net classes

A. Filtering

This paper introduces an innovative approach to match suitable schedule to process context. Fig.3 shows the XML Schema of schedule template. Schedule template defines one domain, contains one or more roles and zero or more rules.

Each role has one or more properties. Each property can be defined as a triple <parent_name, personal_schedule_date, child_name>. The parent_name and child_name are used to identify and describe the property, personal_schedule indicates whether this property is amenable or not. A rule indicates thatsome property of a role is dependent on some property of another role. Different types of rules can be defined according to different types of dependencies. Currently only one type of rule is defined, namely the "setVAlue" type. A rule of "setValue" type indicates that the value of the specified property can be one of a series of options. The following Fig.depicts an example of schedule template.



[Fig. 3] Structure of schedule template

B. Process context

In our approach, the core concept is the process context. Process context can help filter the amenable schedule suitable both to the parents and the clinic. Process context can be automatically created by scheduling process when role need to assign a schedule for vaccination.

Formula 1: Process context = (Criteria, Weight Vector)

Criteria are used to filter out unqualified schedule. Criteria are determined by property dependencies on schedule level, e.g., If a dependency is defined as "the clinic be flexible to provide schedule that the parent wants", and it is known that the parent requires a specific date then the criteria can help improve the precision and narrow down the result set when finding services in a service repository.

Formula 2: Criteria = {property dependencies}

Weight vector: Weight vector is used to rank all the qualified schedule so that the user can select the best one among them. Weight vector contains the merits and their weight used in ranking. When finding schedule for different roles, the weight vectors are also different from each other.

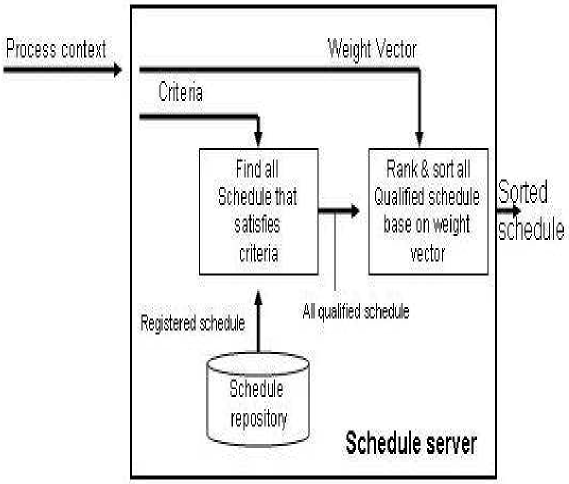
C. Priority Set

Priority set is a asset of domains under which services should be given a higher rank. It can further be divided into two subsets: static priority set and dynamic priority set.

Static priority set: is one schedule process, the static priority sets for finding services for different roles are the same.

Dynamic priority set: in one business process, the dynamic priority sets for finding services for different roles may be different.

The internal process of Auto Vaccination planner finds schedule interface can be demonstrated and shown in Fig.4. When Schedule server receives the process context in a service-finding request, it first extracts the criteria from the processcontext and uses the criteria from the schedule repository, and then extracts the weight vector from the process context and uses the weight vector to rank the entire qualified schedule.



[Fig. 4] Internal process of schedule interface

4. Web Services Security Issues

Web services and service-oriented architecture (SOA) is an important trend, but it prompt serious concerns about security. As web services technologies and specifications continue to evolve, developed have focused on the need for industrial-strength, secure services. There are middleware technologies that support custom built systems and integrate applications to produce operational and management efficiency

Mobile powered devices and software offer a potential benefit, including lower operating costs and greater productivity.[15][16] However, organization that deploy mobile solutions need to make security a priority. Illustrated in the Fig.5 is the possible security threats to auto vaccination planner implemented in a handheld device.

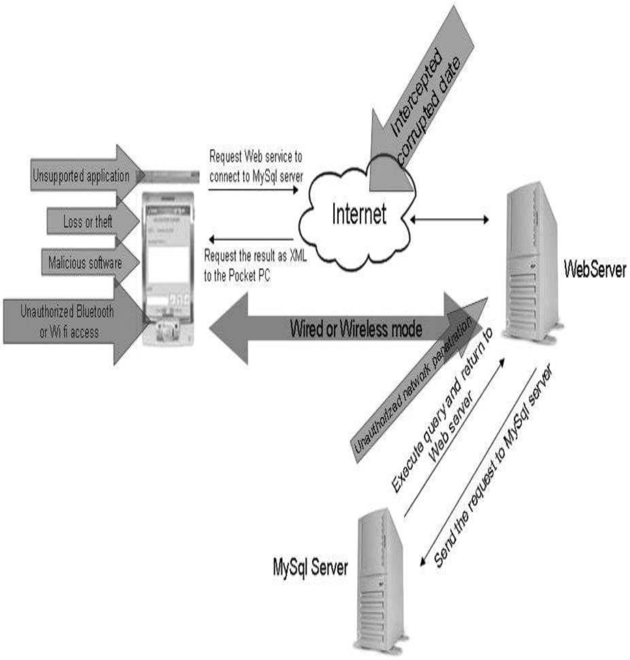
Malicious software: Viruses, Trojan horses and worms are familiar threats to traditional workstations and laptops. While mobile devices have not yet become a significant target, there is a growing consensus among security experts that mobile devices will be a targeted. Even malicious software not designed to deliberately inflict damage may have unintended consequences such as data disclosure or corruption

Loss of sensitive data: Some organizations consider mobile devices a security risk only if they have a business application installed. Other organizations consider the loss of calendar and contact information a security risk. Consider the potential consequences if an executive's e-mail inbox or calendar, full of meetings and briefings, were retrieved by a competitor. Contact information can also cause problems if it falls into the wrong hands, as recent high-profile incidents have demonstrated. Organizations need to protect the data on their employees' mobile devices.

Device loss or theft: Losing a device to mishap or theft can cause lost productivity, data loss, and potential liability under data-protection laws. Thousands of mobile phones and networked handheld devices are lost or stolen every year. As sales of mobile devices increase, the negative effects of device loss and theft are sure to increase accordingly.

Unauthorized device connectivity: An employee device connecting to a personal device to exchange Active Sync may bypass security settings and applications required on a corporate device

Unsupported or unsigned applications: Older applications that are no longer supported, while they may still work, are dangerous because they may be vulnerable to attack by new viruses. If an unsigned application is installed on a device it could make changes to device that would jeopardize it security.


Intercepted
corrupted date
Unsupported application
Loss or theft
Malicious software
Unauthorized Bluetooth or Wi fi access
Request Web service to connect to MySql server
Request the result as XML to the Pocket PC
Internet
WebServer
Wired or Wireless mode
Unauthorized network penetration
Execute query and return to Web server
Send the request to MySql server
MySql Server

[Fig. 5] Security threats to a network that supports mobile devices

Intercepted or Corrupted data: With so many business transactions taking place over mobile devices, there is always concern that critical data could be intercepted along the path through the Internet cloud, via tapped phone lines or intercepted microwave transmissions

Unauthorized Bluetooth or Wi-Fi access: Many mobile phone users employ hands-free Bluetooth headsets, potentially leaving hackers a hole for BlueSnarfing data on the device or BlueBugging to gain control of the device. Ad hoc wireless network connection can also lead to unauthorized device access.

Unauthorized device connectivity: An employee connecting a personal device to the Exchange Active Sync may bypass security settings and applications required on a corporate device.

Unauthorized network penetration: Because many mobile devices provide a variety of network connectivity options, they could potentially be used to attack protected corporate systems. Attackers who gain access to a mobile device may be able to impersonate a legitimate user and gain access to the corporate network.

5. The Crossed Crypto-scheme as solution

The most recent physical security protocol, Wi-Fi Protected Access (WPA) and the emerging 802.11i standard, both specify 802.1 x securities as a framework for strong wireless security. 802.1x use authentication, it requires user to provide credentials to security server before getting access to the network. The credentials can be in the form of user name and password, certificate, token or biometric. The security server authenticates the user's credentials to verify that the user is who he or she claims to be and is authorized to access the network. The security server also verifies that the access point isa valid part of the network. This is done to protect the user from connecting to an authorized access point that may have been set ups to fraudulently capture network data.

A. Asymmetric Encryption

This method employs a pair of keys, consisting of a public key and a private key. The algorithm used in asymmetric encryption, such as RSA are usually based on solving number-theoretical problems. The security of these algorithms is assured by the inherent difficulty of solving such problem. Example is decomposing large amount into their prime factors. Asymmetric is more acceptable solution for e-commerce, the world is currently promoting encryption as the transaction without the prior requirement to exchange key or secrets. The e-commerce world is currently promoting asymmetric encryption as the solution to all the security need. The advantage of asymmetric is in its functionality. It provides security in a wide range of applications that cannot be solved using only symmetric techniques. [3] [4] However, we pay a price for this in a computational efficiency and increased cost.

1. RSA (Rivest, Shamir and Adleman) is widely used public key stream. It is an asymmetric key system, which uses variable key sizes. 512-bit, 1024-bit and 2048-bit RSA are the mostcommon. Its security lies in the difficulty of factoring large composite integers. Although RSA is the most popular Asymmetric cryptography, ECC offers a smaller key sizes, faster computation, as well as memory, energy and bandwidth savings and is thusbetter suited for small devices.

The difficulty of the encryption process lies in the size of the integers involved in the modular exponentiation. In 512-bit RSA, M, e and n are potentially 512-bit number, which cannot be represented in standard integer's formats

$C = M \ e \bmod n$

2. ECC as asymmetric, Elliptic Curve Cryptosystem. This requires much less processing while at the same time being much harder to crack. For instance, a 256-bit ECC key is a secure as a 3,072-bit RSA key. An elliptic curve E over a field F is defined by the Weierstrass equation: [5[

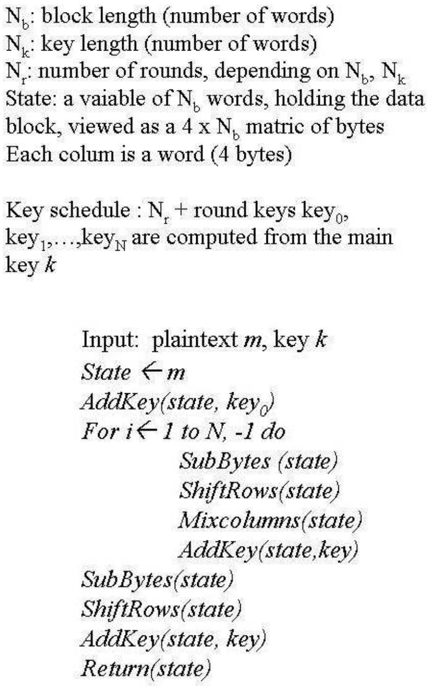
$$E/F\!:y^2 + a_1xy + a_3y = x^3 + a2x^2 + a_4x + a_6 \text{ with } a_1, a_2, a_3, a_4, a_6 \in F.$$

An important characteristic of elliptic curves is that the points on the elliptic curves form a group. Details of this elliptic curve you may refer to [6]. Various researchers have proved that ECC requires more time to break as compared to RSA and DSE Certicom [27], In Certicom the result of their study had been summarized: ECC provides greater efficiency than either integer factorization systems or discrete logarithm systems, in terms of computational overheads, key size and bandwidth. In implementation, these savings mean higher speeds, lower power consumption, and code size reductions. ECC has been accepted as a standard by various bodies.

B. Symmetric Encryption

Symmetric cryptography involved two parties who share a joint secret or key. This exclusive knowledge of the key enables private and secure communications between the two parties. Without the threat of a third party eavesdropping or otherwise tampering with messages in transit. In this instance, the same key is used for encryption and decryption.

1. AES in Pre-shared Key mode Pre-shared key mode is one of the operation modes of WPA it is also known as Personal mode. It is designed for home and small office networks that don't require complexity of 802.11i authentication server. Each wireless network device encrypts the network traffic using a 256 bit key. This key may be entered either as a string of 64 hexadecimal digits, or as a passphrases of 8 to 63 printable ASCII characters. Shared-key WPA is vulnerable to password cracking attacks if a weak passphrase is used. To protect against brute force attack, a 13 character truly random passphrase is sufficient.[2] The structure and algorithm of AES is as follows:



N_b: block length (number of words)
N_k: key length (number of words)
N_r: number of rounds, depending on N_b, N_k
State: a vaiable of N_b words, holding the data block, viewed as a 4 x N_b matric of bytes
Each colum is a word (4 bytes)

Key schedule : N_r + round keys key_0, key_1,…,key_N are computed from the main key *k*

```
Input:  plaintext m, key k
State ← m
AddKey(state, key_0)
For i ← 1 to N, -1 do
        SubBytes (state)
        ShiftRows(state)
        Mixcolumns(state)
        AddKey(state,key)
SubBytes(state)
ShiftRows(state)
AddKey(state, key)
Return(state)
```

This cipher is an iterative clock cipher. It therefore consists of a sequence of transformation to encipher or decipher the data. The encryption and decryption begin at the end with the step to mix sub keys with the data block. To decipher a block data, one must perform an Add Round key step (XORing a subkeys with the block) by itself, then the regular transformation rounds, and then a final round with the Mix column step omitted.. The cipher itself is defined by the following steps:

- · An initial Round Key addition
- · Nr-1 Rounds
- · A final round

C. Crossed Crypto-scheme

From the two major types of encryptions we can conclude that Asymmetric encryption provides more functionality than symmetric encryption, at the expense of speed and hardware cost. On the other hand symmetric encryption provides cost-effective and efficient methods of securing data without compromising security and should be considered as the correct and most appropriate security solution for many applications. In some instances, the best possible solution may be the complementary use of both symmetric and asymmetric encryption.

The algorithm presented here combines the best features of both the symmetric and asymmetric encryption techniques. The plain text data is to be transmitted in encrypted using the AES algorithm. Further details on AES can be taken from [8]. The AES key which is used to encrypt the data is encrypted using ECC. The cipher text of the message and the cipher text of the key are then sent to the receiver. The message digestby this process would also be encrypted using ECC techniques. The cipher text of the message digest is decrypted using ECC technique to obtain the message digest sent by the sender. This value is compared with the computed message digest. If both of them are equal, the message is accepted otherwise it is rejected. [17]

6. Conclusion

The expected technological advances indicate the tremendous potential of Vaccination Planner technology. Several emerging technologies, promise further performance improvements. However, a number of challenging tasks should be further addressed in an effort to make this technology affordable, robust, secure, and easy to use. Further challenges include:

Standards for wireless communication, messaging, and system support.

Planner, and automatic upload to support intermittent upload links to the medical server.

Given the increasing number of user's familiar with the use of cell phones and PDAs, we expect wider user acceptance

The catering of not just children vaccination in the system but as well as the vaccination for all ages.

Outlining the features of security-enhanced mobile network and protocol for data encryption and device authentication.

References

[1] E.A. Mendonc¸a, E.S. Chen, P.D. Stetson, L.K. McKnight, Approach to mobile information and communication for healthcare, Int. J. Med. Inform. 73 (2004) 631–638.

[2] Y.C. Lu, Y. Xiao, A. Sears, J.A. Jacko, A review and a framework of handheld computer adoption in healthcare, Int. J. Med. Inform. 74 (2005) 409–422.

[3] A. Krause, D. Hartl, F. Theis, M. Stangl, K.E. Gerauer, A.T. Mehlhorn, Mobile decision support for transplantation patient data, Int. J. Med. Inform. 73 (2004) 461–464.

[4] J.R. Barrett, S.M. Strayer, J.R. Schubart, Assessing medical residents' usage and perceived needs for personal digital assistants, Int. J. Med. Inform. 73 (2004) 25–34.

[5] H.J. Ten Duis, C. Van der Werken, Trauma care systems in the Netherlands, Injury 34 (9) (2003) 722–727.

[6] E. Ammenwerth, S. Graber, G. Herrman, T. Burkle, J. Konig, Evaluation of health information systems-problems and challenges, Int. J. Med. Inform. 71 (2/3) (2003) 125–135.

[7] R. Haux, Health information systems—past, present, future, Int. J. Med. Inform. 75 (3–4) (2006) 268–281.

[8] Vaccination Schedule, http://www.wikipedia.org

[9] Children’s Health, http://www.children.webmd.com

[10] The Children and Adolescent Immunization Schedule 2008, http://www.aap.org.

[11] http://www.cdc.gov/vaccines

[12] http://www2a.cdc.gov/nip/kidstuff/newscheduler_le/

[13] Improving mass vaccination Clinic Operation, http://www.isr.umd.edu/Labs/CIM/projects/clinic/emedcheck.html

[14] http://www.healing- arts.org/children/vaccines/ vaccines-database.htm

[15] http://www.developer.com/java/j2me/article.php

[16] http://technet.microsoft.com/enus/library/default.aspx

[17] "802.11mb Issues List v12" (excel). 20-Jan-2009.CID98. https://mentor.ieee.org/802.11/file/08/11-08-1127-12-000m-tgmb-issues-list.xls. "The use of TKIP is deprecated. The TKIP algorithm is unsuitable for the purposes of this standard"

[18] Weakness in Passphrase Choice in WPA Interface, by Robert Moskowitz. Retrieved March 2, 2004

[19] Cohen H , Gerhard Frey, Handbook of Elliptic and Hyper-elliptic curve Cryptography, Chapman & Hall /CRC, NW, FL, 2006

[20] Blake I, G. Seroussi and N. Smart (eds). Advances in Elliptic Curve Cryptography , Cambridge University Press, 2005

[21] http://csrc.nist.gov/publications/fips/fips197/fips -197.pdf

[22] L NGALAMOU, L MYERS, Petri Nets and Fuzzy Sets in Hybrid Controllers Synthesis: The Discrete-Event Aspect, WSEAS TRANSACTIONS on SYSTEMS and CONTROL Volume 4, 2009 p 98 – 118

[23] D. R. Lopez, S.;Sanchez-Solano, and A. Barriga, Xfuzzy: A Design Environment for Fuzzy Systems, Seventh, IEEE International Conference on Fuzzy Systems, (FUZZ-IEEE 98), pp. 1060-1065, Anchorage - Alaska, May 4-9, 1998.

[24] X. Li, W. Yu, and F. Lara-Rosano, Dynamic Knowledge, Inference and Learning under Adaptive Fuzzy, Petri Net Framework, IEEE Trans. On Systems, Man and Cybernetica, Vol.30, No.4, November 2000, 442-450. TEH All, Development of a Data warehouse for Lymphoma Cancer, Diagnosis and Treatment Decision Support. Proceedings of the 10th WSEAS International Conference on MATHEMATICS and COMPUTERS in BIOLOGY and CHEMISTRY, Pp. 15 _24. ISSN: 1790-5125, ISBN: 978-960-474-062-8. 2009.

[25] Abonnenc, E., Les phlébotomes de la région éthiopienne (Diptera: Phlebotomidae). Mémoire de l’ORSTOM. 55, pp. 1–289. 1972.

[26] Bacaer, N., Guernaoui, S., The epidemic threshold of a simple seasonal model of cutaneous leishmaniasis. J. Math. Biol. 53, pp. 421–436, 2006.

[27] Boussaa, S., Boumezzough, A., Remy, P. E., Glasser, N., Pesson, B., Morphological and isoenzymatic differentiation of Phlebotomus perniciosus and Phlebotomus longicuspis (Diptera: Psychodidae) in Southern Morocco. Acta Trop. 106, pp. 184–189. 2008.

[28] Boussaa, S., Pesson, B., Boumezzough, A., Faunistic study of the sandflies (Diptera: Psychodidae) in an emerging focus of cutaneous leishmaniasis in Al Haouz province, Morocco. Ann. Trop. Med. Parasitol. 103, pp. 73-83. 2009

[29] Chaves, L.F., Hernandez, M.J., Mathematical modelling of American Cutaneous Leishmaniasis: incidental hosts and threshold conditions for infection persistence. Acta Trop. 92, pp. 245–25. 2004.

[30] Guernaoui, S., Boumezzough, A., Pesson, B., Pichon, G., Entomological investigations in Chichaoua: an emerging epidemic focus of cutaneous leishmaniasis in Morocco. J. Med. Entomol. 42, pp. 697– 701. 2005.

[31] Guessous-Idrissi, N., Chiheb, S., Hamdani, A., Riyad, M., Bichichi, M., Hamdani, S., Krimech, A., Cutaneous leishmaniasis: an emerging epidemic focus of Leishmania tropica in north Morocco. Trans. R. Soc. Trop. Med. Hyg. 91, pp. 660–663. 1997.

[32] Kermack, W.O., McKendrick, A.G., A Contribution to the Mathematical Theory of Epidemics. Proc. Roy. Soc. Lond. 115, pp. 700-721, 1972.

[33] Hang Xaio, Xiubin Zhang, Comparison Studies on Classification for Remote Sensing Image Based on Data Mining Method, WSEAS TRANSACTIONS on COMPUTERS. Volume 7, ISSN: 1109- 2750, pp. 552 558, 2008.

[34] Silvia Martorano Raimundo, Drug Resistants Impact on Tuberculosis Transmission, Proceedings of the 9th WSEAS International Conference on Mathematics & Computers In Biology & Chemistry, Bucharest, Romania , ISBN ~ ISSN:1790-5125 , 978-960-6766-75-6, Pages 176-181, 2008.

Authors

Mohamed Hamdi

Dr. Mohamed Hamdi received his PhD in telecommunications from the Engineering School of Communications (Sup'Com, Tunisia) on 2005. From 2001 to 2005 he has worked for the National Digital Certification Agency (NDCA, Tunisia) where he was head of the Risk Analysis Team. Dr. Hamdi was in charge to build the security strategy for the Tunisian root Certification Authority and to continuously assess the security of the NDCA's networked infrastructure. He has also served in various national technical committees for securing e-government services. He co-authored more than 50 papers that have been published in international journals and conferences. Currently, Dr. Hamdi is serving as an assistant professor for the Engineering School of Communications at Tunis. He is also member of the Communication Networks and Security Lab (Coordinator of the Formal Aspects of Network Security Research Team), where Dr. Hamdi is conducting research activities in the areas of risk management, algebraic modeling, intrusion detection, network forensics, and wireless sensor networks.