Volume 4, Issue 3, March 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Secure Monitoring Of 46 Habit Drugs Using Abe in Cloud

Prof.Shantala C.P, Mr. Asif Ulla Khan
C.I.T Engineering College/VTU University
India

Abstract*—Antibiotics, also known as antibacterial, are types of medications that destroy or slow down the growth of bacteria. The problem statement is that there is no proper regulation about the usage of habit forming antibiotics. The government has come across such 46 habit forming drugs that should not be available freely form 1st march 2014[1]. They will be no longer counter drugs and will be sold only through a doctor's prescription. According to the government notifications chemist should maintain the information such as patient name, prescribed doctor name and amount of 46 habit drugs sold. Such information should be maintained for three years, later the Drug and Control General of India, and zonal authorities will appear for inspection. To make this problem simpler we bring our concept where each and every chemist is provided with service software to update all the necessary information (patient name, prescribed doctor name, antibiotic name, quantity sold, and opening stock, closing stock) to the centralized cloud by using the mobile or computer weekly/daily. As we use cloud for storing drugs details, the data will be secure and it is not going to be tampered. The sub zonal officer can sit in a sub zonal office and can see the information all through the year. They can set the limit on drugs and can check for any deviations, if any the corrective measures can be taken zonal wise, state wise, district wise and even individual chemist details can be tracked by drug control authority without any hassle.

***Keywords*—- DCGI, cloud computing, Attribute based encryption, SMTP Protocol.**

I. Introduction

Antibiotics are powerful medicines that fight bacterial infections. Used properly, antibiotics can save lives. They either kill bacteria or keep them from reproducing. Your body's natural defenses can usually take it from there [2]. The side-effects include: soft stools, diarrhoea, or mild stomach upset such as nausea. Less commonly, some people have an allergic reaction to an antibiotic, and some have died from a severe allergic reaction - this is very rare. Drug resistance, mainly antibiotics, has been one of the most serious public health problems of today in the world with some of the infectious diseases becoming untreatable with the existing drugs. Resistance to drug occurs due to both improper and excessive use of drugs by patients. The emergence of multi drug resistant TB in India and several other Asian and African countries is due to improper use of TB drug by poor patients. And today, no drug is available to treat such deadly form of TB spreading in these countries. The government has prepared a list of such 46 antibiotics (tablets) drugs such as alprazolam, codein, isonaizid…etc those 46 drugs will only be available on prescription from doctor from March 1st 2014. These 46 antibiotics will be no longer the counter drugs and will be sold only through a doctor's prescription. Chemist has to record the information about these drugs in a separate format such that it should include the patient details, prescribed doctor details, and quantity sold for three years. After three years the drug control authority will set up for open inspection for each and every chemist shop to go through the details.

The main reason for this trend is the tendency of the physicians to prescribe this class of drug as an easy option even for a minor infection. For ex: - prescribing of codeine containing cough syrups to patients having even mild cough is a very common practice amongst general practitioners. This needs to be checked as uncontrolled consumption of cough syrups containing codeine and sugar by diabetic patients can push up their sugar level.

There are 6 lakh pharmacies across the country, monitoring these pharmacies antibiotics details and set for inspection is a difficult task for the government and has set the period of three years for inspection keeping this into consideration we would like to bring the idea of implementation of the ACT through this paper.

II. Proposed Design

A. Explanation

Any medicine manufactured by the company will bring into the notice of central government further it is transferred for the approval to the central drug laboratory. Which will check the composition, DTAB and DCHS transport all the drugs to the sub zonal office from there the medicines will reach to each and

every wholesaler and medical representatives further they are provided to each and every chemist shop. The chemist will maintain the opening and closing stock of each and every antibiotic. According to our proposed system the chemist should update the information regarding 46 antibiotics to the sub zonal cloud.

Cloud Computing

Cloud computing is the next stage in the Internet's evolution, providing the means through which everything from computing power to computing infrastructure, applications, business processes to personal collaboration can be delivered to you as a service wherever and whenever you need[4],[5],[6].

Cloud computing is offered in different forms: - public clouds, private clouds, and hybrid clouds, which combine both public and private.

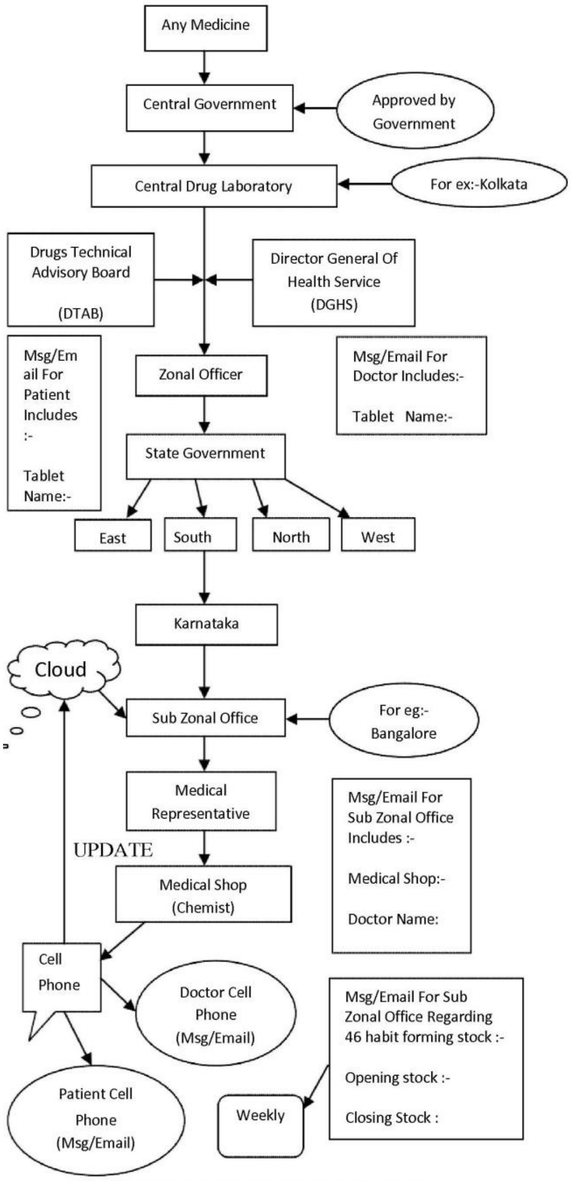
Any Medicine
Central Government
Approved by Government
Central Drug Laboratory
For ex:-Kolkata
Drugs Technical Advisory Board (DTAB)
Director General Of Health Service (DGHS)
Msg/Email For Patient Includes :- Tablet Name:-
Zonal Officer
Msg/Email For Doctor Includes:- Tablet Name:-
State Government
East
South
North
West
Karnataka
Cloud
Sub Zonal Office
For eg:- Bangalore
Medical Representative
Msg/Email For Sub Zonal Office Includes :- Medical Shop:- Doctor Name:
UPDATE
Medical Shop (Chemist)
Cell Phone
Doctor Cell Phone (Msg/Email)
Msg/Email For Sub Zonal Office Regarding 46 habit forming stock :- Opening stock :- Closing Stock :
Patient Cell Phone (Msg/Email)
Weekly

FIG 1:-ARCHITECTURE OF PROPOSED SYSTEM

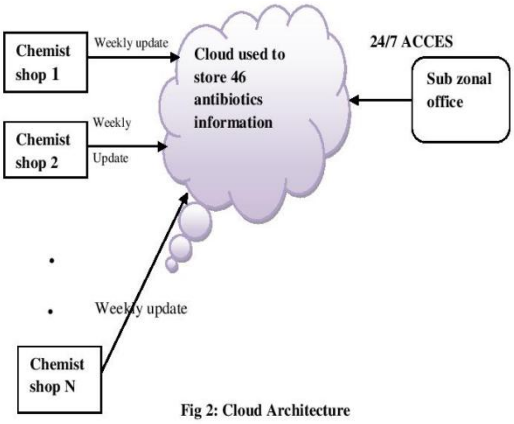

Fig 2: Cloud Architecture

B. *Private Cloud*

Private cloud is the phrase used to describe a cloud computing platform that is implemented within the corporate firewall, under the control of the IT department.

C. *Public Cloud*

A public cloud is one based on the standard cloud computing model, in which as service provider makes resources, such as applications and storage, available to the general public over the Internet.

D. *Hybrid Cloud*

A hybrid cloud is an integrated cloud service utilizing both private and public clouds to perform distinct functions within the same organization.

E. *Attribute Based Encryption to store data in cloud*

Attribute-based encryption (ABE) is a public-key-based one-to-many encryption that allows users to encrypt and decrypt data based on user attributes. A promising application of ABE is flexible access control of encrypted data stored in the cloud, using access polices and ascribed attributes associated with private keys and cipher texts [7], [8], [9].

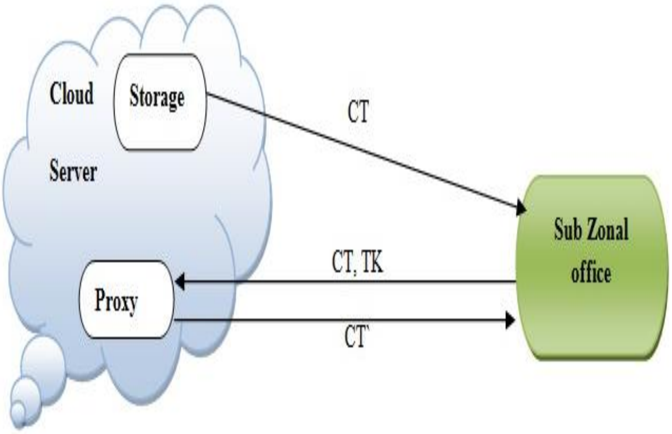

Fig 3:-ABE system with outsourced decryption.

A. Algorithm Implementation

Setup(λ, U) The set up algorithm takes as a input a security parameter λ and a small universe description U={1,2,….l}. It runs G (λ) to obtain (p, G, Gt, e), Where G and Gt are cyclic groups of prime order p. It then chooses g, u, v, d Є G, and α,a Є z*p uniformly at random. For each attribute i Є U, it choose a random value si Є Z*p. Finally, It chooses a collision- resistant hash function H: G ➔ Z*p. The public parameters are published as PK {G,Gt,e,g,u,v,d,gα,e(g,g)α,Ti=g si Ʉ I, H). The master secret key is MSK=α.

Keygen (PK, MSK, S) the key generation algorithm randomly picks t Є z*p. The secret key SKs =(S, K, Ko, Ki) is computed as K= gαgαt, Ko= gt, Ki = Ti^t Ʉi Є S.

Encrypt(PK,M,A) The encryption algorithm takes as input the public parameters PK, a message M Є Gt to encrypt and an LSSS access structure A=(A,ρ) ,Where A is an l*n matrix and ρ is a map from each row Ai of A to an attribute ρ(i). It chooses two random vectors v , v ` Є Zp*^n, denoted v=(s,v2,….,vn) and v`=(s`,v2`,…,vn`). For each row Ai of A, it chooses r1,i,r2,i Є Zp* uniformly at random .Finally it chooses a random messages Ṁ Є Gt . The cipher text is CT =((A ,ρ), C^,C1,Ć1,C1,i,D1,i,,Ć2,C2,i,D2,i),Where,

$$\begin{aligned}
&\hat{C} = u^{H(M)} v^{H(\dot{M})},\\
&C1 = M.e(g,g)^{\alpha s}, \dot{C}1 = g^{s},\\
&C1,i = g^{\alpha Aiv}\, T^{-r1} i\rho(i), D1,i = g^{r1}, i\ Ʉi \in \{1,2,\ldots\ldots,l\},\\
&C2 = \dot{M}.e(g,g)^{\alpha s`}, \dot{C}2 = g^{s`}\\
&C2,i = g^{\alpha Aiv`} T^{-r2} i\rho(i), D2,i = g^{r2}, iɄi \in \{1,2,\ldots\ldots,l\}.
\end{aligned}$$

Decrypt (PK,SKs.CT) The decryption algorithm takes as a input the public parameters PK , a private key SKs =(S, K,Ko, Ki) for a set of attributes S and a cipher text CT==((A,ρ), C^,C1,Ć1,C1,i,D1,i,,Ć2,C2,i,D2,i) for an access structure A=(A,ρ). If S does not satisfy the access structure A its output┴. Let I c{1,2,….,l} be defined such as I={i:ρ(i) Є S}. It computes constant ωi Є Z*p such that ∑iЄIωiAi=(1,0,…,0). The decryption algorithm then computes:

$$C1.\frac{\square i \in I\left(e(C1,i,K0).e(K\square(i),D1,i)\right)^{\square i}}{e(\acute{C}1,k)}$$

$$= M.e(g,g)^{\square s}.\frac{\square i \in I e(g,g)^{\square tAi}.v.wi)}{(e(g,g)^{\alpha s} e(g,g)^{\alpha ts}} = M$$

$$C2.\frac{\square i \in I\left(e(C2,i,KO).e(K\square(i),D2,i)\right)^{\square i})}{e(\acute{C}2,K)}$$

$$= \dot{M}.e(g,g)^{\square s`}.\frac{\square i \in I e(g,g)^{\square tAi}.v`.w`}{(e(g,g)^{\alpha s`} e(g,g)^{\alpha ts`})} = \dot{M}.$$

B. SMTP Protocol

SMTP stands for Simple Mail Transfer Protocol. It's a set of communication guidelines that allow software to transmit email over the Internet,[10][11]. Most email software is designed to use SMTP for communication purposes when sending email and it only works for outgoing messages. When people set up their email programs, they will typically have to give the address of their Internet service provider's SMTP server for outgoing mail. There are two other protocols - POP3 and IMAP - that are used for retrieving and storing email.

SMTP provides a set of codes that simplify the communication of email messages between servers. It's a kind of shorthand that allows a server to break up different parts of a message into categories the other server can understand. Any email message has a sender, a recipient or sometimes multiple recipients a message body, and usually a title heading. From the perspective of users, when they write an email message, they see the slick interface of their email software, but once that message goes out on the Internet, everything is turned into strings of text.

III. Technology

As we use cloud for storing drugs details, the data should be secured and should not to tamper as the details are critical to regularize the ACT. The chemist can update these details in to the centralized cloud (drug authority can only view this) with his authentication details on daily basis or once a week. The information he stores in to the cloud will be encrypted and no one else can view the files unless he has the key to decrypt it. Hence the information in the cloud will be tampered proof. The proposed system provides chemists to update details either using his mobile or a computer, this portable system will save time as well the data can be transferred at any instance of time. The drug control authority can inspect any time as the information will be available to them 24/7. They can set the limit on drugs and can check for any deviations, if any the corrective measures can be taken zonal wise, state wise, district wise and even individual chemist details can be tracked by drug control authority without any hassle. As we can see the fig there will be N number of the chemist present in all over the country, each chemist will be provided with a GUI. Through which each and every chemist get register with the ACT and later he will get his username and password. The chemist can log in into the site and add details such as patient details, doctor details, opening stock, closing stock, of 46 habit forming drugs. Whenever a patient buy the medicine, chemist will update patient details, doctor details amount of antibiotics. Chemist will generate the report weekly once and send that to the subzonal cloud.

The drug control authority can check for any details regarding 46 habit antibiotics any time 24/7 through the cloud and can see if any misleading use of drugs is taking place. In such cases drug control authority can easily identify the improper usage of drugs in particular region and can stop such practice by taking necessary action as per the law.

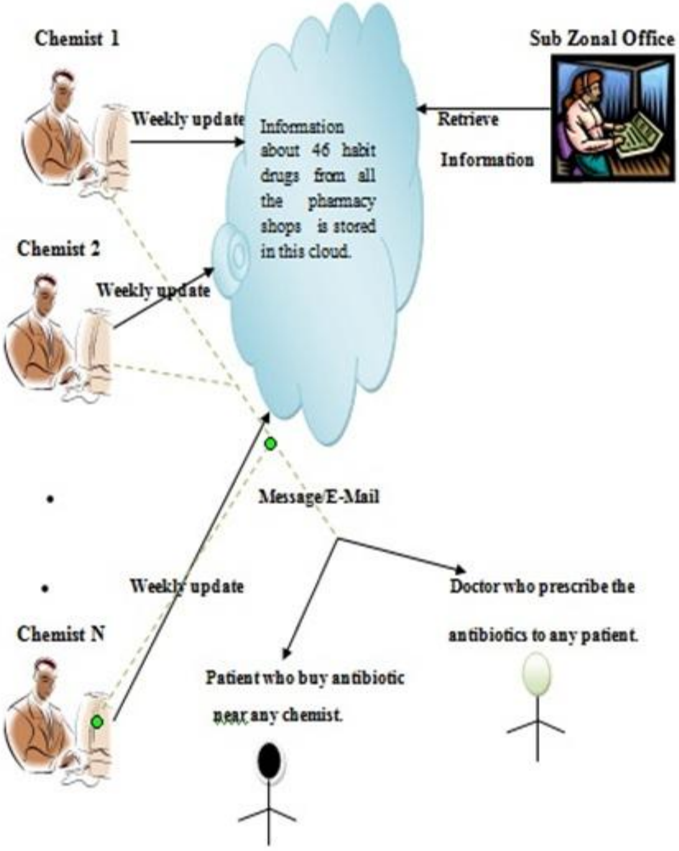
Chemist 1
Weekly update
Information about 46 habit drugs from all the pharmacy shops is stored in this cloud.
Sub Zonal Office
Retrieve
Information
Chemist 2
Weekly update
Message/E-Mail
Weekly update
Chemist N
Doctor who prescribe the antibiotics to any patient.
Patient who buy antibiotic near any chemist.

Fig4 :-Tehonlogy Implemented

IV. Conclusion

We are going to use attribute based encryption because, it is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes (e.g. the country he lives, or the kind of subscription he has). In such a system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes. An adversary that holds multiple keys should only be able to access data if at least one individual key grants access. So that the key can be hold by the subzonal office and can done encryption easily. Since there is no dynamic information regarding the any antibiotics, this will be the first concept. In which the information about 46 antibiotics will be uploaded dynamically, to the drug control authority.

Acknowledgment

I express my sincere gratitude to Dr. D. S.Suresh Kumar, Director, CIT, I also thanks to HOD Prof. C. P. Shantala for continuous guidance without which I would not come up with this paper, I also thanks to all teaching, non teaching staff of CIT College.

References

[1]. http://articles.economictimes.indiatimes.com/2013-09-17/news/42148783_1_drugs-notification-prescription.

[2]. http://www.nlm.nih.gov/medlineplus/antibiotics.html.

[3]. http://www.businessstandard.com/article/currentaffairs/46-habit-forming-drugs-to-be-sold-only-on-doc-sprescription-113091700919_1.html.

[4]. http://www.webopedia.com/TERM/C/cloud_computing.html.

[5]. http://www.dummies.com/how/to/content/comparing-public-private-and-hybrid-cloud-computin.html.

[6]. http://steadfast.net/blog/index.php/customers/public-private- or-hybrid-decoding.

[7]. A. Lewko and B. Waters, “Decentralizing Attribute-Based Encryption,”EUROCRYPT: Proc. 30th Ann. Int' Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology,pp. 568-588, 2011

[8]. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, “Security in Mobile Ad Hoc Networks: Challenges an Solutions,”IEEE Wireless Comm.,vol. 11, no. 1, pp. 38-47, Feb. 2004.

[9]. S. Muller, S. Katzenbeisser, and C. Eckert, “Distributed Attribute-Based Encryption,”Proc. 11th Int’l Conf Information Security and Cryptology (ICISC 08),pp. 20-36, 2009.

[10]. http://whatismyipaddress.com/smtp.

[11]. http://www.networkworld.com/details/636.html.

[12]. S. Chow, “New Privacy-Preserving Architectures for Identity-/Attribute-Based Encryption,” PhD thesis, NYU 2010.

[13]. Y. Zheng, “Key-Policy Attribute-Based Encryptio SchemeImplementation,”http://www.cnsr.ictas.vt.edu/resources.html,2012.

[14]. Y. Zheng, “Privacy-Preserving Personal Health Record System Using Attribute-Based Encryption,” master’ thesis, Worcester Polytechnic Inst., 2011.

[15]. M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, “Secure Attribute-Based Systems,”J. Computer Security vol. 18, no. 5,pp. 799-837, 2010.

[16]. A. Lewko and B. Waters, “Decentralizing Attribute-Based encryption,”EUROCRYPT: Proc. 30th Ann. Int’l Conf Theory and Applications of Cryptographic Techniques: Advances in Cryptology, pp. 568-588, 2011.

[17]. J. Hur and D.K. Noh, “Attribute-Based Access Control with Efficient Revocation in Data Outsourcin Systems,”IEEE Trans.Parallel and Distributed Systems,vol. 22, no. 7, pp. 1214-1221, July2011.

[18]. B. Lynn, The Stanford Pairing Based Crypto Library.

[19]. N. P. Smart and F. Vercauteren, “On computable isomorphism in ef-ficient asymmetric pairing-base systems,”Discrete Appl. Math., vol.155, no. 4, pp. 538–547, 2007.

[20]. R. Canetti, H. Krawczyk, and J. B. Nielsen, “Relaxing chosen-cipher-text security,” inProc. CRYPTO, 2003, pp 565–582.

About Author (s):

Prof.Shantala C.P. received the BE and M.Tech degrees both in computer science and engineering. She is working toward the PhD from Visvesvaraya Technological University She is also serving as Vice principal & Head of the Department Chanabasaveshwara Institute of Technology. NH 206,BH road ,Gubbi,Tumkur,karnataka,India-572216.

Mr.Asif Ulla Khan received the BE degree in Computer science and engineering. Worked in shridevi polytechnic for two and half years as a HOD in computer science department. At present, Pursuing M.Tech in software enginnering at Chanabasaveshwara Institute of Technology. NH 206,BH road,Gubbi,Tumkur,karnataka,India-572216.