Realizing Compliance Tactics to Support Authentication Bridging gap between Software Architecture and Regulatory Requirements

[1]Syeda Uzma Gardazi and [2]Shehnila Zardari

[1]Department of Computer Science, the National University of Computer and Emerging Sciences, Islamabad, Pakistan
[2]Department of Computer Science and Software Engineering, NED University of Engineering and Technology, Pakistan

Abstract
Internationally Compliance is controlled by applicable Information Security regulations e.g. HIPAA. Countries e.g. United States (US) and European Union (EU) etc. have set regulatory and standard requirements to be met for the exchange of information internally or externally. Currently, cybercrime bill has been passed by the National Assembly Standing Committee on IT which is a reactive approach rather than proactive approach in absence of Data Protection Act. This paper suggests improvement in existing Pakistani Data Protection Act 2005 draft which should be published as a proactive approach to secure data within Pakistan. Further, authors introduced a new approach to embodying e-Authentication architectural tactics at software architecture. It will result in better compliance of regulations and standards Authentication requirements for information. The first step is cross-mapping of multiple standards and rules to identify various aspects of the e-Authentication regulatory requirement compliance. Next, we have addressed how software architecture will treat Authentication Compliance Attribute (CA) and Quality Attribute (QA). In addition, CA impact over QA is also being determined and evaluated using WebEHR portal and Health Level Seven (HL7) case study.

Key words:
PCI DSS, ISO 27001:2013, ISO 9001: 2015, HIPAA, CMS, DEA, NIST, Pakistani Data Protection Act 2005 Draft, Authentication Assurance, Architectural Mechanism, and HL7.

1. Introduction

US and EU data privacy laws e.g. Health Insurance Portability and Accountability Act (HIPAA) and EU data protection law etc. limit businesses moving confidential data to countries with weak privacy compliance programs. It is essential for an organization covered under HIPAA and which outsource its business process to developing countries e.g. Pakistan –AJK (Azad Jammu Kashmir) etc. to meet the international level privacy requirements imposed to eliminate the losing potential customers due to non-compliance. An organization covered under HIPAA is required to ensure confidentiality, availability and integrity of Protected Health Information. It is essential for these organizations to adopt compliance mechanisms while outsourcing data [1].

The software being developed must ensure compliance to the applicable security regulatory requirements including e-Authentication (hereafter called Authentication) requirements. The term Authentication as defined by the Office of Management and Budget ("OMB") refers to a process that establishes assurance in electronic identities of user provided information for which Authentication is required [2]. Four types of Authentication Assurance Level are defined by the requirements for each level (as defined in OMB 04-04 and M-03-22) are described in Electronic Authentication Guideline (800-63) issued by the National Institute of Standards and Technology ("NIST") [3][4]. Controls are defined for User at each Assurance Level by proofing the identity. Assurance Level is directly affected by the use of Authentication factors [5]. Currently four Authentication factors exist namely:

- something you know (for example, a PIN) [6],
- something you have (for example, a mobile phone or a computer),
- something you are (for example, an thumb measurement), and
- somebody you know defined by RSA Laboratories [7].

Each Assurance Level as described below defines the degree of confidence based on factors referred above:

- **Level 1 Authentication** requires one-factor Authentication (e.g. User ID and Password) of the three regulatory-approved Authentication factors. Access method(s) which is (are) approved/accepted for accepted for Level two, Level three, and/or four also satisfy Level one.
- **Level 2 Authentication** also requires one-factor Authentication along with the use of cryptographic methods. It requires that the passwords used for this purpose must be strong.
- **Level 3 Authentication** requires two-factors Authentication of the three regulatory-approved Authentication factors e.g. "soft" cryptographic tokens [8].

Manuscript received May 5, 2017
Manuscript revised May 20, 2017

- **Level 4 Authentication** is quite similar to Level 3 except that it only allows “hard” cryptographic tokens using FIPS 201 compliant device.

We will like to clarify here that strong Authentication term refers to use of more than one-factor from the same set. E.g. you obtain multiple answers to challenging questions will be considered as strong Authentication instead of two-factor Authentication (or multi-factor Authentication) as it does not receive a factor from either “something you have” or “ something you are” group. However, in this paper we will refer strong Authentication as the 1.5 factor Authentication [9].

We will identify Authentication requirements description and usage in software architecture to track compliance by cross-mapping different standards and regulations in section two. In section three, Authentication Compliance Attribute (CA) and Quality Attribute (QA) will be devised and CA impact over QA is also being determined [10]. Lastly, Authentication Assurance tactics are proposed and evaluated using a case study.

2. Cross-Mapping of standards/rules

The first step of software development consists of gathering software requirements. Requirements can be either functional or non-functional in nature. Non-functional requirement e.g. performance etc. is a condition to achieve system’s functionality [11]. A functional requirement emphasizes on behavior of system. These requirements can either be collected from stakeholders or from published standards/regulations.

2.1 HIPAA Person or Entity Authentication (164.312(d))

Authentication is the confirmation process that a person is the one claimed (45 CFR § 164.304). HIPAA requires that organizations should establish and implement procedures for authorizing EPHI access to ensure HIPAA Security Rule §164.308(a)(4) and the HIPAA Privacy Rule at §164.508 compliance. It is advised to use more than one-factor authentication to protect remote access of EPHI as advised by Centers for Medicare & Medicaid Services (CMS) HIPAA Authentication guidance [12].

2.2 ISO

International Organization for Standardization does not impose any specific authentication requirement. Rather, they provide guideline which can be adopted by companies to improve their existing processes.

- ISO 27001: 2013 information security management system which can be adopted by any company to protect confidentiality, integrity and availability (CIA) of data [13].
- ISO 9001: 2015 is a quality management system standard. The ISO 9001: 2008 focuses on the processes to either produce final product or provide services [14].

2.3 PCI

Payment Card Information Data Security Standard (“PCI DSS” is an information security standard quite similar to ISO 27001. Payment Card Industry Standard Council (“Council”) set this standard to prevent/limit credit card frauds and enhance credit card information security. The current PCI DSS standard document version is 3.0 and available at PCI Security Standards Council’s website [15]. PCI DSS standard wants to secure credit card information in an effective manner by providing a comprehensive guideline for all merchants and service providers handling any type of credit card transactions. PCI standard suggest using two-factor authentication for remote-access to the network.

2.4 DEA Regulation for E-Prescription

As required by Drug Enforcement Administration (DEA) authentication regulation requirement for obtaining an authentication credential individual practitioners (21 CFR § 1311.105), an individual practitioner must obtain a two-factor authentication credential.

A two-factor authentication credential is required by the Drug Enforcement Administration (DEA) for e-prescribing controlled substances. Two-factor authentication requires that clinicians be able to present two of three verifiers: something they know (i.e., a password); something they have (i.e., hard token such as an access card); and/or something that represents who they are (i.e., a biometric, such as a thumbprint scan). These two factor authentication is required to approve access controls and sign electronic prescriptions (21 CFR § 1311.120) [16]. A two-factor authentication credential can be obtained using:

- Identity verification that comply with the assurance Level 3 or above requirements as specified in NIST SP 800-63-1 (21 CFR § 1311.08).
- Basic digital certificate assurance level achieved from a certification authority that is cross-certified with the Federal Bridge Certification Authority [17].

2.5 NIST

The National institute for Standards and Technology (NIST) issued a draft update to their special publication (SP) 800-63 [Electronic Authentication Guideline] providing technical guidance to all federal agencies implementing electronic authentication [18]. These standards are in conjunction with OMB memorandum 07-16 [19] apply to all federal information and information systems and suggest that two-factor authentication should be enabled for remote access."

2.6 ONC-ATCB 2011/2012 Test Script 170.302 (t) Authentication

The Vendor shall identify the EHR function(s) that are available to login and logout of the EHR, create a new account, establish the identification and authentication information associated with the new account, assign permissions to the new user account, and delete the account.

2.7 Integrating the Healthcare Enterprise (IHE) Access Control

IHE should define an attribute provider (semantic of a policy information point) for querying attributes about objects (i.e., subjects) for infrastructures where subject authentication is performed using multi-factor authentication.

2.8 EU Data Protection Act

The EU Data Protection Act (DPA) imposes the security requirement to all foreign and local companies processing data of EU residents. DPA does not include minimum factor limitation for authentication.

2.9 Pakistan Data Protection Act

The proposed Electronic Data Protection Act was a drafted and proposed in 2005 and so far not published. There is no law regulating the protection of data in Pakistan to date. Understanding the need of the hour, new Foreign Data Security and Protection Act 2004 draft was published by ministry to support US and EU companies outsourcing data within Pakistan. Currently, cybercrime bill has been passed by the National Assembly Standing Committee on IT which is more a reactive approach in absence of Data Protection Act.

Table 1: cross-mapping of Authentication Requirements

Authentication Requirement Analysis		
S#	***Regulation/ Standard***	***Authentication Requirement***
1	HIPAA & HITECH	Remote access to EPHI >1 factor
2	HIPAA & HITECH	Other access =>1 factor
3	FISMA-NIST 800-53 Rev	Privileged accounts, non-privileged accounts and for local access to privileged accounts access > 1 factor
4	CMS Remote Access	Remote access to EPHI >1 factor
5	CMS Security Rule	Other access to EPHI =>1 factor
6	DEA authentication regulation for e-prescriptions of controlled substances	Sign e-prescription >=2
7	Integrating the Healthcare Enterprise (IHE) Access Control	Access authentication >= 1 factor
8	EU Data Protection Act	Access authentication >= 1 factor
9	Pakistan Data Protection Act	Not applicable
10	ISO 27001	Access authentication >= 1 factor
11	ISO 9001	Not applicable
12	ONC-ATCB 2011/2012 Test Script 170.302 (t) Authentication	Access authentication >= 1 factor

3. Suggested improvement in Pakistani Data Protection Act 2005

In the absence of a Pakistan's Data Protection Law, the introduction of a cybercrime law would be overwhelming for civil rights and businesses in the country. Therefore, we suggest that Pakistani Government and AJK Government should publish Data protection Law as a proactive approach. This Act may require Covered Entities under this law to implement physical, technical and administrative level safeguards. Few improvements are suggested below:

1. Designate Compliance official who are responsible for managing Information Security Compliance program
2. Covered Entities shall implement encryption of data (at rest or in-transmission) compliant

with international standards e.g. Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2).

3. Authentication Compliance requirement at least by supporting:

- Level 3 Assurance Level or above for remote access of confidential information and
- Level 1 Assurance Level or above for other types of access.

Two-factor authentication can be used in following scenarios based on Table 1 analysis and same is suggested as an improvement for Pakistani/AJK Data Protection Act as well:

a) Remote access: Highlight all author and affiliation lines.

- If employee, staff, etc. are accessing PHI or confidential information over the Internet (via a portal or VPN, etc.), healthcare organizations should use two-factor authentication.
- Whenever helpdesk require access to customer's system, it should be used.
- All modems that are deployed in the environment should have a well-documented business justification that cannot be met in any other and should be periodically reviewed for continued applicability and need.
- Modems deployed with remote access software enabled (such as pcAnywhere or gotomypc) must be configured properly and use two-factor authentication.

b) Finance department require to gain credit card/ACH information access

c) Provider need to login at website that contains confidential information

d) Agreement execution with the client

e) PCI on cloud security & two-factor authentication

Entities should consider additional methods for securing administrative access, such as implementing two-factor authentication or establishing dual or split-control of administrative passwords between multiple administrators.

4. Conduct internal monitoring and auditing after specific intervals. International standards e.g. ISO 27001 and automated log monitoring tools e.g. Log Analyzer - Security Information Event Management (SIEM) can be used to enhance effectiveness.
5. Conduct information security trainings after specific intervals.
6. Disciplinary guidelines should be developed and enforced effectively. Employee Compliance rankings can be maintained.
7. Identify and manage risks and deducted information security offensives in timely manner.
8. Hashing should be implemented to ensure integrity of data at storage and rest. The hashing standard should be FIPs/NIST compliant.

4. specifying compliance-driven architectural Assurance mechanisms

It is a fundamental for software to achieve a desired combination of attributes (e.g., reliability, interoperability) to ensure compliance and quality [IEEE 1061]. Current QA sufficiently do not address the legal requirements. Compliance Attributes (CA) are derived from architectural regulatory requirements, QA and CA are orthogonal[24] [25]

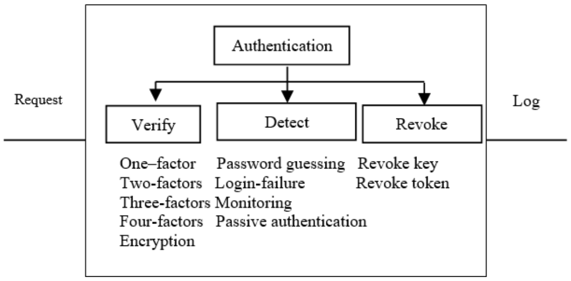

Fig. 1. Summary of access mechanism in support of Authentication

If CA and QA were not orthogonal, the choice of function would dictate the level of compliance or security. A tactic is an architecture strategy that "is concerned with the relationship between design decisions and a QA/CA response. A tactic may be either required or optional for a QA and/or CA. Within complex systems, quality attributes can never be achieved in isolation. The achievement of any one will have an effect, sometimes positive and sometimes negative, on the achievements of others. For example, authentication and reliability often exist in a state of mutual tension: the most secure system has the fewest points of failure__ typically security kernel [20][21]. There are many architectural tactics for various quality attributes such as availability, performance, security, modifiability, usability and testability [22][23].

The following are brief descriptions of tactics for Authentication:

_ Enable – An Authentication tactic for authentication factors.

_Detect–An Authentication tactic for monitoring authentication anomalies of a component by monitoring log.

_ Revoke – An Authentication tactic for revoking the access from a component.
_ Maintain User ID/Password Confidentiality by encrypting credentials.

5. Authentication Assurance tactic standardization for STB

In this section we will use a case study to incorporate Authentication tactic. Software, Transcription and Billing Corp. ("STB") US based backup office located in AJK and Poland which are using different Electronic Authentication ("Authentication") Standards for their software e.g. Electronic Health Record (EHR) and HL7 etc.

For what has been discussed hereunder, we propose that STB's software shall provide Level 3 Assurance support based on different standards, software and regulations review;

- STB is a Covered Entity under HIPAA. Person or Entity Authentication (§ 164.312 (d)) HIPAA clause requires STB to implement procedures to verify that a person or entity seeking access to EPHI is the one who claims to be so. If the rate of Authentication error rate is increased then Level of Authentication Assurance should also increase (e.g. Level 2 or higher base on CMS recommendations).

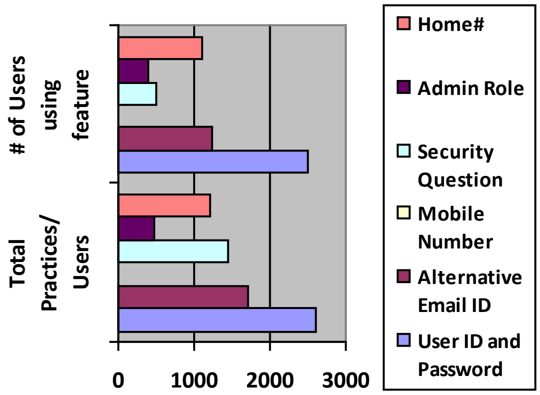

Fig. 2. STB WebEHR Authentication Analysis

- In accordance with the Center for Medicare & Medicaid Services (CMS) Authentication guideline, information systems, which support its operations and assets, should provide either Level 2 or Level 3 to protect information related to personnel, medical, and similar data.
  - **Case 1**: A User can ONLY access or update information about them.
  - **Case 2**: A User can ONLY submit, review, or update information about persons that THEY had provided DURING THE CURRENT SESSION.
  - **Case 3**: A User, not covered in Case 1 or 2, can access or update information about persons OTHER THAN themselves.

  CMS also recommends that Covered Entities under HIPAA shall implement two-factor Authentication for granting remotely accessing system that contains PHI.
- DEA Authentication regulations for e-prescriptions require that prescribers must use two-factor Authentication to sign/submit controlled substances prescriptions.
- Four Merchant Levels are defined by the Payment Card Industry Security Standards Council ("Council") in the PCI Data Security Standard (DSS) based on number of transactions per year. The transaction number i.e. 1839 determines that STB is currently at Merchant Level 5 and required to complete the Security Assessment Questionnaire (SAQ) along with Quarterly PCI Scans. The PCI DSS standard requires STB to implement two-factor Authentication for granting access (i.e. Remote) to system that contains card information.

Thus, in our view, Assurance Level 2 and Level 3 implementation requirements are binding to STB's software as it facilitates the User to handle PHI (the term defined in 45 CFR § 164.501). Currently STB software provides only Level 2 Assurance as the User is required to provide one-factor Authentication i.e. User ID and Password and this factor is provided through a secure Authentication protocol e.g. Secure Socket Layer (SSL) 128 bits etc. We understand that presently STB's Software hold capacity to Level 2 Authentication. This capacity needs to be enhanced. We recommend that STB's Software shall support Level 2 as well as Level 3 Assurance Level b providing strong (1.5) Authentication and two-factor Authentication.

6. using the architecture to reason about authentication tactic

As to next question that how STB software's login procedure can incorporate support for Level 3 Assurance that require two-factor Authentication or higher by providing standard Authentication Assurance Framework for all software; we suggest that any User accessing STB's WebEHR portal , shall be (and in some cases may be) given an option to provide an additional factor upon login from the following two options along with User ID and Password to access restricted information using STB WebEHR portal[26][27].

6.1 Recurring factors

Recurring factors are required to be given by the User upon each login, if selected.

- Image-based User Authentication [1.5 factors Authentication-Level 2] requires the User to correctly identify pictures from a dynamic grid of images presented (selected/uploaded by User during registration).
- Challenge-response Authentication [1.5 factors Authentication-Level 2] requires the User to correctly answer the security question presented (selected/devised by the User during the registration process).
- E-mail based one-time password ("OTP") [1.5 factors Authentication-Level 2]: OTP can be emailed at the User's Email ID (Email ID may be provided by the User during registration).
- SMS-based OTP or "soft" cryptographic tokens [two-factor Authentication-Level 3]: OTP can be sent at the User's mobile/cell number (which may be provided by the User during registration).

6.2 Non-recurring factors

Non-recurring factor are not required to be given by the User upon each login, if selected.

- Registered ("Trusted") Device [two-factor Authentication-Level 3]: This is a concept in which the User's system after registration ("Enrollment") is used to provide two-factor Authentication without continuous involvement of the User.

Table 2: STB's eHr and HL7 Software Function Association with Authentication

Software Key Functions for Universal Authentication		
Functions	***Equations***	***Explanations***
Login within US/EU	[Set A (R)] or [((Option A) or (Option B)) (A)]	User ID and Password is required. User can also enable Level 3 Assurance.
Login outside US/EU	[Set A (R)] and [((Option A) or (Option B)) (R)]	User ID and Password is required along with one additional factor from either Option A or Option B to access the website outside US/EU.
Forgot User ID	[Email ID (R)] and [((Option A) or (Option B)) (A)]	Email ID is required along with one additional factor from either Option A or Option B to reset password.
Forgot Password	[User ID (R) and [((Option A) or (Option B)) (A)]	User ID is required along with one additional factor from either Option A or Option B to reset password.
Account lockout	[Set A (R) and [((Option A) or (Option B)) (A)]	User ID and Password is required along with one additional factor from either Option A or Option B after 3 incorrect attempts to retrieve a credential (FIPS PUB 112). We should maintain the history of incorrect attempts. We can also enable 15 minutes account lock after 3 consecutive incorrect password attempts (optional).
Registration	[(Email-based OTP) or (SMS-based OTP) (R)]	OTP verification is required that is either Email-based or SMS-based upon registration.

Word and brackets (R) refer to mediatory or required actions, whereas word and brackets (A) refers to allowed or optional actions. In general, it is recommended that the User should use Level 3 Assurance by enabling two-factor Authentication.

7. evaluating Compliance-driven architecture

User enters their existing login password on the STB's WebEHR portal. The User is permitted to perform authorized actions after the User's login credentials are validated by the WebEHR portal. A user is created and assigned role once by providing an additional Authentication from Option A above. Technical information about the User e.g. IP address, browser, location and the operating system. User information are collected and stored in database (preferably in hash format). Following matrix represents the WebEHR key function for Authentication options. We will formulate architecture of WebEHR portal.

7.1 Style

The next step will be style selection and reference model. We will use client and server style.

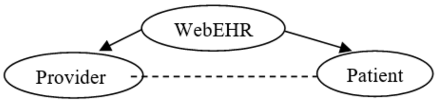

Fig. 3. STB WebEHR Portal Reference Model

7.2 Reference Model

Reference Model for WebEHR portal is shown below:

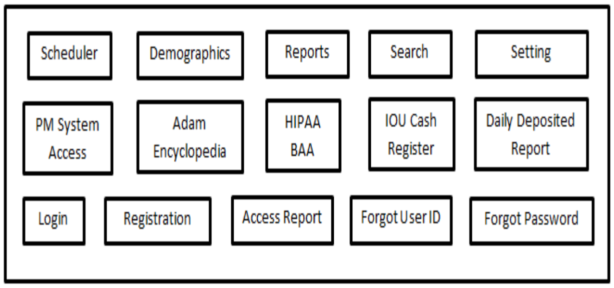

Fig. 4. STB WebEHR Portal Reference Model

7.3 Reference Architecture

At next level, we formulated Reference Architecture from Reference Architecture [28] [29].

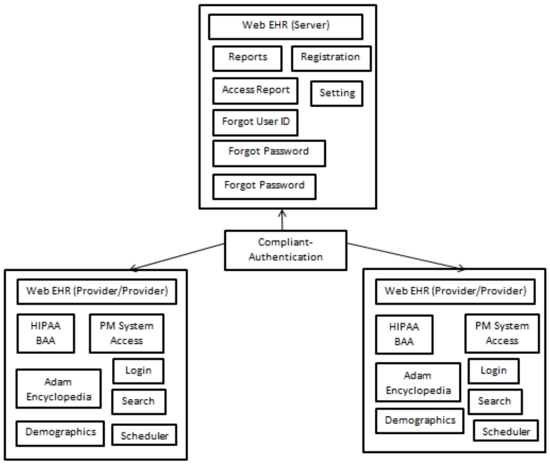

Fig. 5. STB WebEHR Portal Reference Architecture

Now we represent a segment of software architecture for WebEHR portal.

Component Provider/Patient WebEHR, Ports, out create User, submit credentials, notify_Compliant_ Authenticator in User authentication status, User_Role end Provider/Patient HER [30][31].

The figure 6 shows the expert authentication system software architecture. It also contains one log table (Rule Application Log) for storing the results of rules when applied on claims.

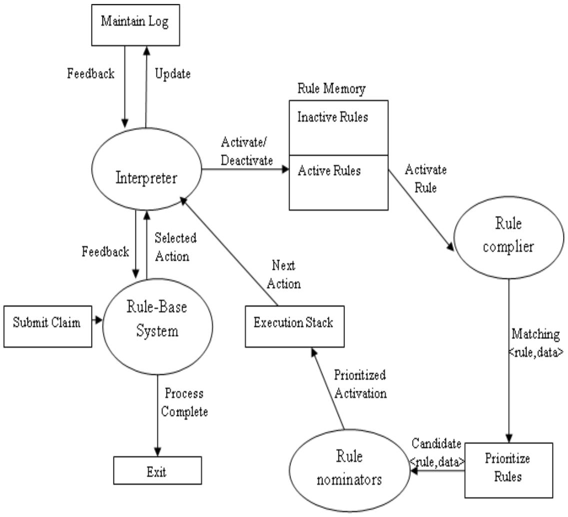

Fig. 6. EAS's Software Architecture

7.4 Evaluation

We have evaluated WebEHR portal using Architecture Tradeoff Analysis Method (ATAM) against compliance and quality attributes [25].

Compliance Sceanrio#1 (CS1) Description: Controlled substances e-perception should be digitally signed before submission.

Risk (R1): Unauthorized PHI disclosure, Non-Risk (NR1): Authorized PHI disclosure, Sensitivity (S1): Security and Tradeoff (T1): Performance

Table 3: attribute-based analysis

Attributes		***Web EHR***	***R#, S3 and T#***
QA1	Performance	-	NA
QA2	Availability	+	NA
CA1	Access Control	+	R1, S1, and T1
CA2	Encryption	+	R1, S1 and T1
CA3	Integrity	+	R4, , S1 and T1
CA4	Accounting of Disclosure	+	R1, S1, and T1

We have come to conclusion that WebEMR portal meet Authentication Compliance requirement by support Level 2 as well as Level 3 Assurance Level b providing strong (1.5) Authentication and two-factor Authentication. Statistics of testing of rule engine authentication performance on actual medical billing data have been plotted in Figure 7.

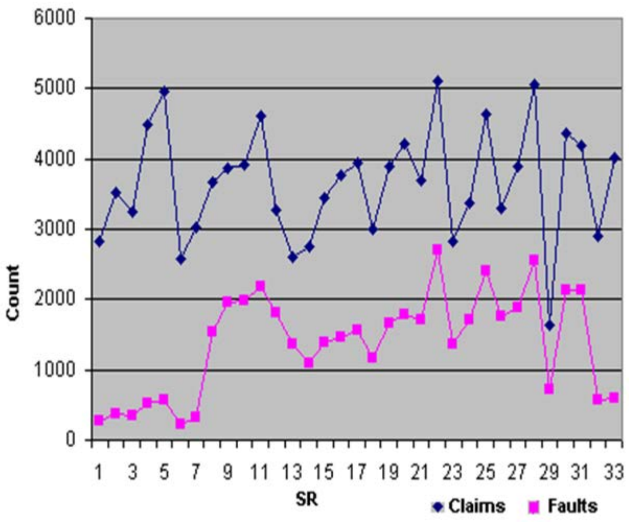

Fig. 7. Claims and authentication faults

Note that ratio of number of authentication faults to total number of claims submitted is high due to mistakes of manual data entry process. By introducing expert authentication system we do not need to apply compliance checks separately on each data source. Rather all these checks are applied after data is imported and before data is sent.

8. Conclusion & Future Work

International regulations are limiting data transfer or storage to those countries which are not imposing equivalent rules and procedures. Non-compliant aware software architecture may result into violation of regulation and penalty imposed by governing agencies. It is also essential to bridge the gap between compliance and architecture. We have refined existing security architectural mechanism approach to represent authentication regulatory requirements at software architecture and evaluated it at software architecture using a case study. Relatively a better budget has been presented as a whole this year in Pakistan, but some bitter tablets have also been wrapped under candies label. The most important aspect of budget in my view is that State Bank of Pakistan has been tasked to establish e-gateway in the country. Budget document reveals that e-gateway will streamline the mobile payments in the country. It is anticipated that e-gateway will also enable Pakistani users to be able to send and receive online payments across internet.. This step will create a lot of job opportunities for youth, specifically related to E-sector. Information security compliance requirements should be listed down and cross-mapped in to software that will deal with e-gateway within Pakistan.

Acknowledgment

The authors would like to thank HEC and FAST-NU or NUCES for their valuable contribution to the refinement or realization of compliance-driven tactic.

References

[1] The Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996) Retrieved April 14,. 2006 from http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

[2] OMB Memorandum M-04-04, Authentication Guidance for Federal agencies, December 16, 2003, available at: http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

[3] Travis D. Breaux, Annie I. Antón. 2008. Analyzing Regulatory Rules for Privacy and Security Requirements. IEEE Transactions on Software Engineering, Special Issue on Software Engineering for Secure Systems (IEEE TSE), 34(1):5-20, January/February 2008.

[4] Office of Management and Budget, Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003 available at: http://www.whitehouse.gov/omb/memoranda/m03-22.html.

[5] Nist and Emmanuel Aroms. 2012. NIST Special Publication 800-63 Electronic Authentication Guideline. CreateSpace, Paramount, CA.

[6] Federal Information Processing Standards Publication (FIPS PUB 180-4). Secure hash standard. National Institute of Standards and Technology. 2012. Retrieved from http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf October 18, 2012

[7] John Brainard, Ari Juels, Ronald L. Rivest, Michael Szydlo, and Moti Yung. 2006. Fourth-factor authentication: somebody you know. In Proceedings of the 13th ACM conference on Computer and communications security (CCS '06). ACM, New York, NY, USA, 168-178.

[8] Vipul Goyal, Yuval Ishai, Amit Sahai, Ramarathnam Venkatesan, and Akshay Wadia. 2010. Founding cryptography on tamper-proof hardware tokens. In Proceedings of the 7th international conference on Theory of Cryptography (TCC'10), Daniele Micciancio (Ed.). Springer-Verlag, Berlin, Heidelberg, 308-326.

[9] F. Bergadano, B. Crispo, and M. Lomas. 1997. Strong authentication and privacy with standard browsers. J. Comput. Secur. 5, 3 (June 1997), 191-212.

[10] Mikael Svahnberg, Claes Wohlin, Lars Lundberg, and Michael Mattsson. 2002. A method for understanding quality attributes in software architecture structures. In Proceedings of the 14th international conference on Software engineering and knowledge engineering (SEKE '02). ACM, New York, NY, USA, 819-826.

[11] Luiz Marcio Cysneiros and Julio Cesar Sampaio do Prado Leite. 2004. Nonfunctional Requirements: From Elicitation to Conceptual Models. IEEE Trans. Softw. Eng. 30, 5 (May 2004), 328-350.

[12] CMS Systems Security Manual Retrieved January 10. 2016 from https://www.cms.gov/Regulations-and-

Guidance/Guidance/Manuals/downloads/117_systems_security.pdf.

[13] "ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements". International Organization for Standardization. Retrieved 10 January 2016 from http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534.

[14] "ISO 9001:2015. ISO. Retrieved 10 January 2016 from https://www.iso.org/obp/ui/#iso:std:iso:9001:ed-5:v1:en

[15] Payment Card Industry (PCI) Data Security Standard, v3.0. PCI Security Standards Council, LLC. November 2013.

[16] Title 21 Code of Federal Regulations (CFR), Part 1311 — Requirements for Electronic orders and Prescription, 75 FR 16310, Mar. 31, 2010.

[17] Stefan A. Brands. 2000. Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. MIT Press, Cambridge, MA, USA.

[18] William E. Burr, Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk, Sarbari Gupta, Emad A. Nabbus. 2012. Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology - Special Publication 800-63-1. CreateSpace Independent Publishing Platform, USA.

[19] Office of Management and Budget, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (OMB Memorandum M-07-16)

[20] Bass, L., Clements, P., Kazman, R., 2003. Software Architecture in Practice, second ed. Addison Wesley.

[21] S.Kim, D.K. Kim, L. Lu, S. Park, Quality-driven. Architecture Development Using Architectural Mechanisms, J. Syst. Softw. 82, Aug. 2009, pp. 1211-1231.

[22] Bachmann, F., Bass, L., Llein, M., 2002. Illuminating the Fundamental Contributors to Software Architecture Quality. Technical Report CMU/SEI-2002-TR-025, Software Engineering Institute, Carnegie Mellon University.

[23] Ramachandran, J., 2002. Designing Security Architecture Solutions. John Wiley.

[24] S. U. Gardazi, A. A. Shahid, Billing Compliance Assurance Architecture for Healthcare Industry (BCAHI), Computer Science Journal, 2010.

[25] S. U. Gardazi, A. A. Shahid, Compliance-driven Software Architecture, International Journal of Advanced Computer Science and Applications (IJACSA), Volume 8 Issue 5 May 2017 [ISI Indexed].

[26] S. U. Gardazi and A. A. Shahid, Compliance Patterns and Quality Management System (QMS) Framework to ensure Medical Billing Compliance, 2nd International Conference on Health Information Science (HIS 2013), 25-27 March 2013, London, UK.(http://link.springer.com/chapter/10.1007%2F978-3-642-37899-7_7#page-1)

[27] S. U. Gardazi, C. Salimbene and A. A. Shahid, HIPAA and QMS based architectural requirements to cope with the OCR audit program, 3rd FTRA International Conference on Mobile Ubiquitous, and Intelligent Computing (MUSIC), Canada, June 2012.

[28] S. U. Gardazi, A. A. Shahid, Email System Architecture for HITECH Compliance, International Conference on Software Engineering and Data Mining (SEDM), 2010.

[29] S. U. Gardazi, A. A. Shahid, Software Architecture for Information Assurance, International Conference on Product Focused Software Development and Process Improvement (PROFES), 2010.

[30] S. U. Gardazi and A. A. Shahid, Survey of Software Architecture Description and Usage in Software Industry of Pakistan, IEEE ICET, 2009.

[31] S. U. Gardazi, S. F. Gardazi, H. Khan and A. A. Shahid, Motivation in Software Architecture and Software Project Management, IEEE ICET, 2009.