Organizational Information Assets Classification Model and Security Architecture Methodology

Mostafa Tamtaji
PhD Candidate in IT Management; Allameh Tabatabaee University
Corresponding Author: tamtaji@atu.ac.ir

Mehdi Naghian Fesharaki
PhD in Computer; Associate Professor;
Malek Ashtar University mehfesharaki@yahoo.com

Seyed Ghaolamhasan Tabatabaee
PhD in Computer (software); Malaysia Industrial University (MIT)
sayed@cc.iut.ac.ir

Iranian Journal of Information Processing & Management

Iranian Research Institute for Information Science and Technology (IranDoc)
ISSN 2251-8223
eISSN 2251-8231
Indexed by SCOPUS, ISC, & LISTA
Vol. 31 | No. 1 | pp. 243-267
Autumn 2015
https://doi.org/10.35050/JIPM010.2015.011

Received: 2014.12.12 **Accepted: 2015.03.17**

Abstract: Organizations today are exposed to huge amount and diversity of information assets produced in different systems such as KMS, financial and accounting systems, official and industrial automation systems and so on. It is obvious that protection of information assets is necessary.

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources so that can be rapidly provisioned and released. Several benefits of this model makes organizations decide to take a strategy for implementing private cloud computing.

Management of information security is the main challenge in developing and accepting of this model. In this paper, at first, according to "design science research methodology" and compatible with "design process at information systems research", a complete categorization of information assets including 355 different types of information assets in 7 groups and 3 levels is presented to managers to be able to plan corresponding security controls according to importance of each group.

Then, in order to directing organization to architect its information security in cloud computing environment, appropriate methodology is presented.

Presented cloud computing security architecture, which resulted in the

proposed methodology, and presented classification model according to Delphi method and experts comments discussed and verified.

Keywords: Information Classification; Information Asset; Information Security; Cloud Computing; Security Architecture Methodology

الگوی طبقه‌بندی دارایی‌های اطلاعاتی سازمانی و متدولوژی معماری امنیت آن

مصطفی تمتاجی
دانشجوی دکتری مدیریت فناوری اطلاعات؛ دانشگاه علامه طباطبایی
پدیدآور رابط: tamtaji@atu.ac.ir

مهدی نقیان فشارکی
دکتری کامپیوتر (هوش مصنوعی)؛ دانشیار؛ دانشگاه صنعتی مالک اشتر
mehfesharaki@yahoo.com

سیدغلامحسن طباطبایی
دکتری کامپیوتر (نرم‌افزار)؛ دانشگاه صنعتی مالزی sayed@cc.iut.ac.ir

دانش و مدیریت اطلاعات

دریافت: ۱۳۹۳/۰۹/۲۱ | پذیرش: ۱۳۹۳/۱۲/۲۶ | مقاله برای اصلاح به مدت ۱ روز نزد پدیدآوران بوده است.

پژوهشنامهٔ پردازش و مدیریت اطلاعات
فصلنامه | علمی پژوهشی
پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)
شاپا (چاپی) ۸۲۲۳-۲۲۵۱
شاپا (الکترونیکی) ۸۲۳۱-۲۲۵۱
نمایه در LISTA، ISC، و SCOPUS
jipm.irandoc.ac.ir
دورهٔ ۳۱ | شمارهٔ ۱ | ص‌ص ۲۴۳-۲۶۷
پاییز ۱۳۹۴
https://doi.org/10.35050/JIPM010.2015.011

مقالهٔ پژوهشی

چکیده: امروزه سازمان‌ها با حجم و تنوع بسیار زیاد اطلاعات و دارایی‌های اطلاعاتی مواجه هستند که در سیستم‌های مختلف از جمله سیستم مدیریت دانش، سیستم مالی و حسابداری، سیستم اتوماسیون اداری و سیستم اتوماسیون صنعتی و ... تولید شده و حفاظت از این اطلاعات ضروری است. از طرف دیگر، رایانش ابری به‌عنوان نسل جدیدی از رایانش، مدلی برای دسترسی فراگیر و راحت ارائه می‌کند که به محض درخواست در مخزن منابع رایانشی به اشتراک گذاشته می‌شود و مزایای متعدد آن سبب گردیده که سازمان‌ها گرایش زیادی به استفاده از آن داشته باشند. چالش اصلی در توسعه و پذیرش این مدل، اطمینان از برقراری، حفظ، و مدیریت امنیت اطلاعات سازمان در محیط ابری است. در این مقاله که بر «روش‌شناسی تحقیق علم طراحی» و همسو با روال‌های «فرایند طراحی در تحقیق سیستم‌های اطلاعاتی» مبتنی است، الگوی طبقه‌بندی دارایی‌های اطلاعاتی سازمان مشتمل بر ۳۵۵ نوع مختلف در هفت گروه و سه سطح ارائه شده است تا مدیران بتوانند با توجه به اهمیت هر یک از گروه دارایی‌ها، کنترل‌های امنیتی متناظر را برای بقای سازمان طرح‌ریزی کنند. در ادامه، به‌منظور هدایت سازمان در معماری امنیت اطلاعات خود در محیط رایانش ابری، روش مناسب برای تدوین معماری امنیتی ارائه شده است. روش ارائه‌شده، به سازمان کمک می‌کند که پس از شناسایی و طبقه‌بندی دارایی‌های اطلاعاتی خود متناسب با الگوی ارائه‌شده، نسبت به معماری امنیت اطلاعات به‌صورت بهینه و کارآمد اقدام نماید. معماری امنیتی پیشنهادشده با به‌کارگیری این متدولوژی و الگوی طبقه‌بندی اطلاعات سازمانی

ارائه‌شده با روش دلفی بر اساس نظر خبرگان مدیریت سازمان و متخصصان امنیت رایانش ابری، مورد بحث و تبادل نظر، اصلاح، و نهایتاً اجماع قرار گرفته است.

کلیدواژه‌ها: طبقه‌بندی اطلاعات؛ دارایی اطلاعاتی؛ امنیت اطلاعات؛ رایانش ابری؛ روش معماری امنیت

۱. مقدمه

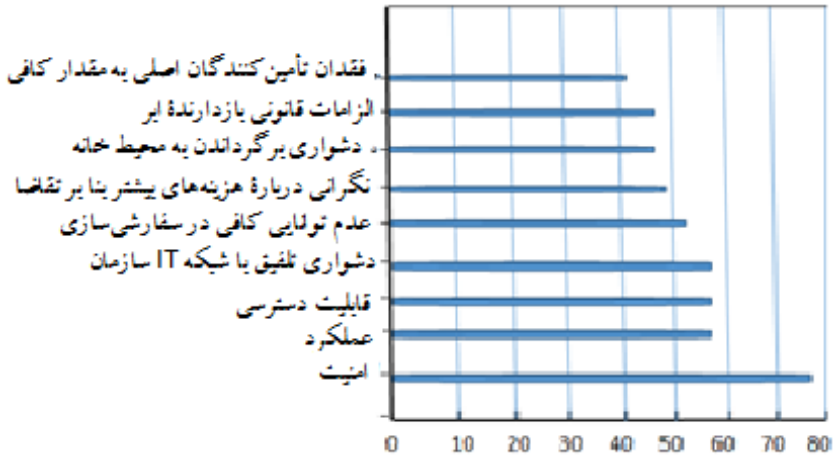
عواملی از قبیل پیچیدگی سازمان‌ها، تنوع مأموریت‌ها و اهداف، داده‌های درونی و بیرونی، فناوری‌های روبه‌رشد، کارکنان دانشی و پویا و تنوع دانش‌های موجود در سازمان باعث شده است که سازمان با انباری از اطلاعات مواجه باشد که نه قابل دور ریختن است و نه در همهٔ لحظات مورد نیاز. دسته‌بندی و برچسب‌گذاری این اطلاعات نیازمند یک سیستم کارآمد و جامع است. این معضل هنوز در سازمان‌ها حل نشده که ظهور فناوری جدیدی در رایانش، معضل دیگری را به آن می‌افزاید.

رایانش ابری مدلی برای دسترسی فراگیر و راحت است که به محض درخواست در مخزن منابع رایانشی به اشتراک گذاشته می‌شود و می‌تواند به‌سرعت و با حداقل تلاشِ مدیریتی یا تعامل با ارائه‌دهندهٔ سرویس، تأمین شده و در دسترس قرار گیرد. این مدل، امکانِ دسترسی سریع و راحت کاربر به منابع رایانشی مورد نیاز را از طریق اتصال به وب فراهم آورده و ضمن صرفه‌جویی در هزینه‌ها، دغدغه‌هایی از قبیل مقیاس‌پذیری، فراهم‌آوری منابع و انعطاف‌پذیری را کاهش می‌دهد (IBM Corporation 2012) و (Furht & Escalante 2010).

رایانش ابری مزایایی را برای سازمان‌ها فراهم می‌آورد که سبب می‌شود در آیندهٔ نزدیک رشد بسیار سریعی داشته باشد. پیش‌بینی می‌شود که در آینده، همهٔ سازمان‌ها متقاضی دریافت سرویس‌های ابری باشند، لیکن آنچه در این میان مانع گرایش برخی از آنها می‌شود، دغدغهٔ امنیت اطلاعات در محیط ابری و تضمین این امنیت است.

نتایج حاصل از نظرسنجی شرکت IDC[1] از ۲۴۴ مدیر فناوری اطلاعات نشان داد که در بین ۹ چالش اساسی مطرح در حوزهٔ رایانش ابری، امنیت، بزرگ‌ترین چالش است شکل (۱)، و با کسب ۷۴/۵ درصد، مقام نخست دغدغه‌های مدیران سازمان‌ها را به خود اختصاص داده است (Velte & Elsenpeter 2010).

1. International Data Corporation



شکل ۱. رتبه‌بندی چالش‌های اساسی رایانش ابری (Velte & Elsenpeter 2010)

از آنجا که رایانش ابری شامل بسیاری از فناوری‌ها از جمله شبکه، پایگاه‌های داده، سیستم‌های عامل، زمان‌بندی منابع، مدیریت تراکنش‌ها، کنترل هم‌زمانی و مدیریت حافظه است، تهدیدات امنیتی مختلفی با توجه به نیازمندی‌های امنیتی مختلف (محرمانگی، صحت، کنترل دسترسی، حریم خصوصی و ...) قابل تصور است. گام اول در ایجاد امنیت، پاسخ به این سؤال است که امنیت برای چه چیزی و در چه سطحی باید ایجاد شود. پاسخ به این سؤال مستلزم وجود الگویی جامع برای طبقه‌بندی دارایی‌های اطلاعاتی سازمان است.

وجود یک الگوی طبقه‌بندی دارایی‌های اطلاعاتی به سازمان این اطمینان را می‌دهد که همهٔ محل‌های تولید اطلاعات شناسایی شده و اطلاعاتِ تولیدشده در یک طبقه‌بندی مشخص در حال ذخیره‌سازی هستند. لذا، در این تحقیق تلاش شده که الگوی جامعی از طبقه‌بندی اطلاعات موجود در سازمان از دیدگاه فناوری اطلاعات ارائه شود.

همچنین در یک محیط ابری، طراحی یک معماری جامع امنیتی با استفاده از ابزارها و فناوری‌های موجود می‌تواند ضمن به حداقل‌رساندن ریسک‌های انتقال، راهنمایی برای پیاده‌سازی محیط ابری خصوصی امن برای سازمان باشد. این معماری به مدیر ارشد سازمان در ترسیم مسیر استقرار امنیت و همچنین، کنترل امنیت و تداوم آن کمک کرده و موجب حصول اطمینان در تحقق نسبی امنیت شود. بر این اساس، در ادامهٔ این مقاله برای محیط ابرخصوصی سازمان مفروض، متدولوژی مناسبی برای طراحی معماری امنیتی ارائه شده است.

۲. طرح مسئله و ضرورت تحقیق

لازمهٔ مدیریت صحیح و کارآمد اطلاعات در سازمان و برقراری امنیت آن، شناسایی و طبقه‌بندی دارایی‌های اطلاعاتی است. دارایی اطلاعاتی یعنی هر اطلاعاتی که برای سازمان مهم و باارزش بوده و قابل حفاظت است.

تنوع این دارایی‌ها و مدیریت امنیت مناسب آنها در طول چرخهٔ حیات، بدون طرح‌ریزی مناسب الگوی طبقه‌بندی امکان‌پذیر نیست. الگوی طبقه‌بندی باید دربرگیرندهٔ کلیهٔ اطلاعات مهم سازمان باشد. باید به این نکته توجه کرد که یکی از الزامات استاندارد سیستم مدیریت امنیت اطلاعات مبتنی بر استاندارد ISO/IEC 27001:2013، طبقه‌بندی و برچسب‌گذاری دارایی‌های اطلاعاتی است (سازمان ملی استاندارد ایران ۱۳۸۷).

از طرفی با توجه به مزایای متعدد رایانش ابری، در کشور ما نیز مشابه موج جهانی گسترش این مدل، سازمان‌های متعددی در صدد ایجاد ابر خصوصی برای شرکت‌های تابعهٔ خود بوده‌اند تا از مزایای محیط ابری در کاهش هزینه‌ها و افزایش دسترس‌پذیری و حتی اثرات مثبت حاکمیتیِ محیط ابری استفاده نمایند، لیکن امنیت اطلاعات ابر سبب شده که تصمیم‌گیری در این انتقالِ سخت و پیچیده باشد. ریسک‌های محیط ابری با ریسک‌های سیستم‌های سنتی متفاوت هستند و سازمان باید بتواند به نقطهٔ سربه‌سر بین ریسک‌های این تصمیم و منافع حاصله برسد. این موضوع توجه مضاعف به طبقه‌بندی اطلاعات کلیدی و طرح‌ریزی معماری جامع را ضروری ساخته است.

از طرفی پس از تعیین الگوی طبقه‌بندی دارایی‌های اطلاعاتی، بهره‌گیری از یک متدولوژی مناسب جهت طراحی معماری امنیت اطلاعات سازمانی دارای اهمیت است.

۳. سؤال و هدف تحقیق

هدف این تحقیق در گام نخست، ارائهٔ الگوی جامع و مانع طبقه‌بندی دارایی‌های اطلاعاتی سازمان است تا این اطمینان را ایجاد کند که همهٔ محل‌های تولید اطلاعات شناسایی شده و اطلاعات تولیدشده در یک طبقه‌بندی مشخص در حال ذخیره‌سازی هستند.

هدف دوم این تحقیق، ارائهٔ یک روش برای معماری امنیت دارایی‌های اطلاعاتی در محیط رایانش ابری است. سازمان با بهره‌گیری از روش ارائه‌شده می‌تواند نسبت به معماری امنیت محیط ابری خود اقدام کند.

هدف سوم این تحقیق، عملیاتی‌کردن متدولوژی مذکور و تدوین معماری مرجع امنیتی رایانش ابری است که نتیجهٔ این گام در این مقاله ارائه شده است.

در واقع، این تحقیق به‌دنبال یافتن پاسخی برای این سؤالات است:

- ◇ الگوی جامع و مانع برای شناسایی و طبقه‌بندی دارایی‌های اطلاعاتی و باارزش سازمان چیست؟
- ◇ سازمان برای دستیابی به یک معماری مرجع امنیتی باید چه مراحلی را طی کند؟
- ◇ معماری مرجع پیشنهادی محیط رایانش ابرخصوصی سازمان دارای چه اجزایی است و این اجزا چه تعاملی با هم دارند؟

این مقاله در صدد پاسخ‌دادن به دو سؤال اول بوده و نتیجهٔ به‌دست‌آمده برای سؤال سوم را نیز ارائه خواهد کرد.

٤. مبانی نظری و ادبیات و پیشینهٔ تحقیق

ظهور فناوری ابری در سال‌های اخیر تأثیر زیادی روی بسیاری از جنبه‌های کسب‌وکار داشته است. طبق پیمایش انجام‌شده بیشتر شرکت‌های کوچک و بزرگ به‌دلایل مختلف از جمله کاهش هزینهٔ زیرساخت و دسترسی سریع به برنامه‌های کاربردی از سرویس‌های رایانش ابری استفاده می‌کنند (Subashini & Kavitha 2011).

همان‌گونه که اینترنت، دسترسی به اطلاعات را متحول کرد و آن را از حالت انحصاری خارج نمود، رایانش ابری نیز کار مشابهی را برای فناوری اطلاعات انجام می‌دهد. رایانش ابری در واقع، یک تغییر الگوی تحویل و ارائهٔ منابع و سرویس‌ها را بیان می‌کند (Winkler 2011).

مفهوم رایانش ابری: رایانش ابری را می‌توان به‌عنوان سبک جدید رایانش که در آن منابع عمدتاً مجازی شده و به‌گونه‌ای مقیاس‌پذیر و دینامیکی به‌عنوان یک سرویس در بستر اینترنت ارائه شده‌اند، تعریف کرد. صرفه‌جویی در هزینه، دسترس‌پذیری بالا و مقیاس‌پذیری آسان از مزایای رایانش ابری هستند (Furht & Escalante 2010).

مؤسسهٔ ملی فناوری و استانداردها[1]، رایانش ابری را این‌گونه تعریف می‌کند: رایانش ابری مدلی برای دسترسی فراگیر و راحت است که به‌محض درخواست در مخزن منابع رایانشی قابل پیکربندی به اشتراک گذاشته شده (برای مثال شبکه‌ها، سرورها، ذخیره‌سازها، برنامه‌های کاربردی و سرویس‌ها) و می‌تواند به‌سرعت و با حداقل تلاش مدیریتی یا تعامل با ارائه‌دهندهٔ سرویس، تأمین شده و در دسترس قرار گیرد (Mell & Grance 2011).

1. National Institute of Standards and Technology - NIST

رایانش ابری یک مدل یا محیط رایانشی مرکب از اجزای فناوری اطلاعات (سخت‌افزار، نرم‌افزار، شبکه‌سازی و سرویس‌ها) و فرایندهای مرتبط با به‌کارگیری این عناصر است که در کنار یکدیگر قابلیت توسعه و تحویل سرویس‌های ابری از طریق اینترنت یا شبکهٔ خصوصی را ایجاد می‌کنند (Winkler 2011).

مفهوم امنیت اطلاعات: اصطلاح «امنیت اطلاعات»[1] حوزهٔ وسیعی از آنچه را که باید در ارتباط با حفاظت از اطلاعات و سیستم‌های اطلاعاتی انجام شود، دربرمی‌گیرد. از دید تاریخی، امنیت اطلاعات ریشه‌هایی در رمزنگاری، اختفا و سایر فعالیت‌هایی که هدفشان حفاظت از محرمانگی پیام مکتوب بوده است، دارد (von Alan et al. 2004). تعاریف متعددی برای امنیت اطلاعات ارائه شده است که در ادامه به برخی از آنها اشاره خواهد شد:

- ◇ محافظت از محرمانگی[2]، جامعیت[3] و دسترس‌پذیری[4] اطلاعات. همچنین می‌تواند خصیصه‌های دیگری مثل قابلیت اطمینان[5]، عدم انکار[6]، اصالت[7] و پاسخ‌گویی[8] را نیز شامل شود (Mell & Grance 2011) و (ISO/IEC 27000 2014).
- ◇ محافظت از اطلاعات و سیستم‌های اطلاعاتی در برابر دسترسی، استفاده، افشا[9]، اختلال[10]، تغییر[11] یا امحای[12] غیر مجاز به‌منظور تأمین محرمانگی، جامعیت و دسترس‌پذیری (Velte et al. 2010).
- ◇ اطمینان از اینکه تنها کاربران مجاز (محرمانگی)، به اطلاعات کامل و دقیق (جامعیت) در هنگام نیاز (دسترس‌پذیری) دسترسی دارند. امنیت اطلاعات عموماً دربرگیرندهٔ امنیت سیستم‌های فناوری اطلاعات و همچنین، فرایندهای غیرفناوری اطلاعات که در تعامل با سیستم‌های فناوری اطلاعات هستند، می‌باشد. هدف امنیت اطلاعات، محافظت اطلاعات و سیستم‌های اطلاعاتی از دسترسی و استفادهٔ غیرمجاز، افشا، قطع، تغییر یا خرابی است (von Alan et al. 2004).
- ◇ یک حوزهٔ مطالعاتی بین‌رشته‌ای و فعالیت حرفه‌ای است که با توسعه و پیاده‌سازی انواع مختلف مکانیزم‌های امنیتی (فنی، سازمانی، دارای منشأ انسانی و قانونی) مرتبط است و هدف آن دور نگهداشتن اطلاعات در همهٔ مکان‌ها (داخل سازمان یا بیرون آن) و حالت‌ها (هنگام ایجاد، پردازش، ذخیره‌سازی، انتقال و امحا) از تهدایدت، به‌منظور دستیابی به اهداف امنیتی

1. information security
2. confidentiality
3. integrity
4. availability
5. reliability
6. non-repudiation
7. authenticity
8. accountability
9. disclosure
10. disruption
11. modification
12. destruction

است. اهداف امنیتی می‌توانند شامل اصالت، قابلیت اعتماد[1]، حریم خصوصی[2]، دسترس‌پذیری، جامعیت، محرمانگی، پاسخ‌گویی و قابلیت ممیزی[3] باشند (Cherdantseva & Hilton 2013).

از نگاه عملیاتی و واقعی، جنبه‌های عملکردی امنیت[4] (شامل محرمانگی اطلاعات، احراز هویت، جامعیت اطلاعات، حفاظت در مقابل حملات، حریم خصوصی و دسترس‌پذیری) و جنبه‌های غیرعملکردی امنیت[5] (شامل قابلیت تعامل، قابلیت مدیریت و سادگی توسعه) باید مورد توجه قرار گیرند (Kannegati & Chodavarapu 2008).

طبقه‌بندی اطلاعات: شناسایی و طبقه‌بندی اطلاعات در واقع، هنر سازمان در تعیین منابع تولید، ذخیره‌سازی، پردازش و انتقال اطلاعات در سازمان است. به‌عبارت دیگر، سازمان‌ها باید بتوانند اطلاعات سازمانی خود را شناسایی کرده و آنها را بر اساس اهمیت در تدوام کسب‌وکار سازمان طبقه‌بندی نمایند.

در بررسی‌های انجام‌شده، الگوی جامعی که دارایی‌ها را از ابعاد مختلف شناسایی و طبقه‌بندی نماید، حاصل نشد. در سند «آیین کار مدیریت امنیت اطلاعات» انواع دارایی‌های سازمانی، به‌طور کلی، به‌صورت زیر دسته‌بندی شده است. این دسته‌بندی بسیار کلی بوده و در عمل، راهنمای مناسبی برای طبقه‌بندی اطلاعات نیست (سازمان ملی استاندارد ایران ۱۳۸۷):

الف) اطلاعات: بانک‌های اطلاعاتی و فایل‌های داده، قراردادها و توافق‌نامه‌ها، مستندات سیستم، اطلاعات تحقیق، راهنماهای کاربر، محتوای آموزشی، رویه‌های عملیاتی یا پشتیبانی، طرح‌های استمرار کسب‌وکار، تفاهم‌نامه‌های پشتیبانی، گزارش‌های ممیزی و اطلاعات کسب‌شده؛

ب) دارایی‌های نرم‌افزاری: نرم‌افزارهای کاربردی، نرم‌افزار سامانه، ابزارهای توسعه و نرم‌افزارهای کمکی؛

پ) دارایی‌های فیزیکی: تجهیزات رایانه‌ای، تجهیزات ارتباطی، رسانه‌های قابل جابه‌جایی و سایر تجهیزات؛

ت) خدمات: خدمات محاسبه‌ای و ارتباطی، تجهیزات عمومی مانند گرمایش، نور، برق و تهویه هوا؛

---

1. trustworthiness
2. privacy
3. auditability
4. functional aspects of security
5. nonfunctional aspects of security

ث) افراد و صلاحیت‌ها، مهارت‌ها و تجربه‌های آنها؛

ج) موارد ناملموس مانند اعتبار و خوشنامی سازمان.

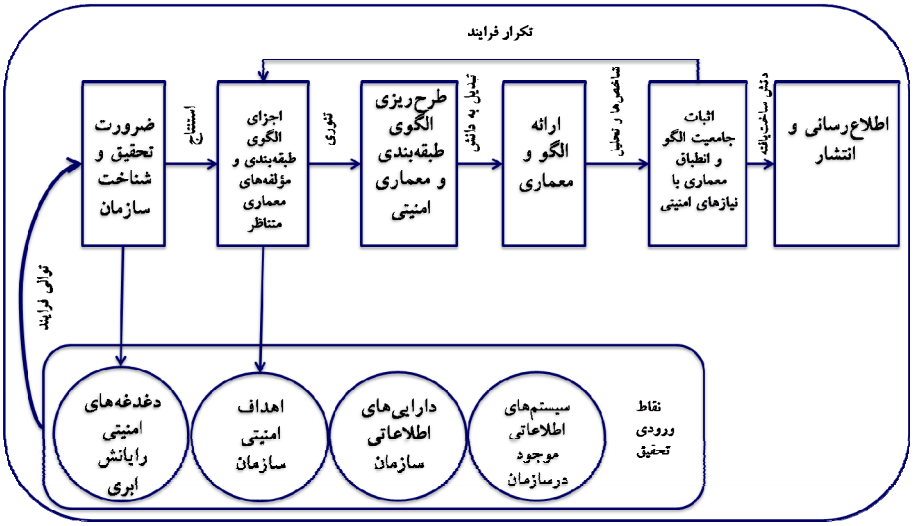
۵. روش تحقیق

روش استفاده‌شده در این تحقیق از جنبهٔ تخصصی مبتنی بر «روش تحقیق علم طراحی» است که توسط «پفرز» ارائه شده و با روال‌های «فرایند طراحی در تحقیق سیستم‌های اطلاعاتی» ارائه‌شده توسط Hevner همسوست (von Alan et al. 2004; Peffers et al. 2007).

روش تحقیق علم طراحی یک روش علمی ساخت‌یافته و پذیرفته‌شده برای پژوهش و تحقیق در حوزهٔ فناوری اطلاعات است که چارچوب فرایندی مدون و مشخص را برای طراحی کلان مدل‌ها و ایده‌های نو در شش گام ارائه می‌کند.

در تحقیق انجام‌شده از متدلوژی ارائه‌شده توسط «پفرز» استفاده شده است. لیکن با توجه به موضوع تحقیق و همچنین فرصت‌های بهبود مورد نظر، بهبودها و تغییراتی در متدولوژی لحاظ شده که در شکل (۲) قابل مشاهده است.

تحقیق انجام‌شده با این روش، در واقع، منجر به ارائهٔ یک معماری امنیتی مرجع خواهد شد و در این مقاله به دستاوردهای این تحقیق تا گام ارائهٔ الگوی طبقه‌بندی دارایی‌های اطلاعاتی و تعیین روش اشاره خواهد شد.



شکل ۲. روش اصلاح‌شده و مورد استفاده در تحقیق

به‌منظور صحه‌گذاری روند طی‌شده در تحقیق و اخذ نظرات خبرگان در خصوص جامعیت الگوی طبقه‌بندی ارائه‌شده و مناسب‌بودن روش پیشنهادی برای تدوین معماری امنیت سازمان، از روش دلفی و ابزار پرسشنامه استفاده شد. روش دلفی فرایندی ساختاریافته برای جمع‌آوری و طبقه‌بندی دانش موجود در نزد گروهی از کارشناسان و خبرگان است که از طریق توزیع پرسشنامه‌هایی در بین این افراد و بازخورد کنترل‌شدهٔ پاسخ‌ها و نظرات دریافتی صورت می‌گیرد. یکی از دلایل انتخاب این روش، وابسته‌نبودن این روش به تعداد خبرگان است. از آنجا که تعداد متخصصان و کارشناسان در دسترس در حوزهٔ مورد پژوهش زیاد نیست، لذا روش دلفی می‌تواند روش مناسبی برای اخذ نظرات باشد.

مراحل انجام‌شده برای اخذ نظرات خبرگان عبارت‌اند از:

گام اول: ابزاری که برای جمع‌آوری داده‌ها مورد استفاده قرار می‌گیرد، در مرحلهٔ نخست باید از روایی[1] برخوردار باشد. روایی بدین‌معناست که روش یا ابزار به‌کاررفته تا چه حدی قادر است خصوصیت مورد نظر را درست اندازه‌گیری کند. برای اطمینان از روایی، سؤالات پرسشنامه توسط دو نفر از خبرگان بررسی و اصلاح شد.

گام دوم: در مرحلهٔ دوم، سند الگوی طبقه‌بندی و سند تشریح روش تدوین معماری امنیتی بین خبرگان توزیع شد و نظرها به‌صورت ناشناس و بدون ارتباط با یکدیگر در قالب پرسشنامه جمع‌آوری گردید. همچنین، نظرهای آزاد اخذ شد و آنهایی که دارای تناقض بودند با تعامل به اجماع رسید و پیشنهادها در اسناد لحاظ گردید.

گام سوم: در این گام، در جلسهٔ مشترکی با حضور همهٔ خبرگان، اسناد اصلاح‌شده تبیین و نظرها در قالب پرسشنامهٔ نهایی اخذ و تحلیل گردید. ابزار مورد استفاده علاوه بر روایی، باید پایایی[2] نیز داشته باشند. پایایی، قابلیت تکرار روش یا ابزار اندازه‌گیری است و در این تحقیق برای اثبات پایایی از روش محاسبهٔ آلفای کرونباخ استفاده شد.

٦. الگوی طبقه‌بندی دارایی‌های اطلاعاتی سازمان

در گام نخست این تحقیق، از دیدگاه سیستم‌های اطلاعاتی موجود در سازمان که تولیدکننده و ذخیره‌کنندهٔ دارایی‌های اطلاعاتی سازمان محسوب می‌شوند، انواع اطلاعات موجود در سازمان که می‌توانند مهم باشند، شناسایی و طبقه‌بندی شده‌اند.

1. alidity
2. reliability

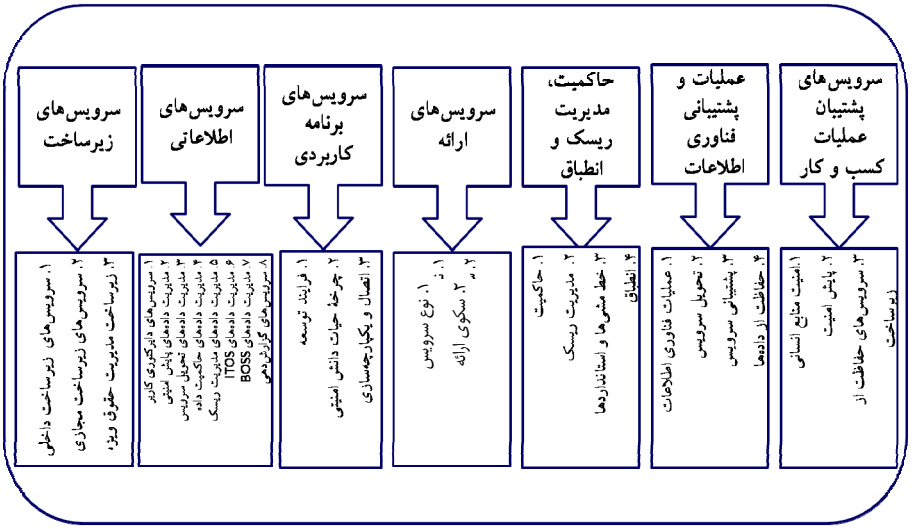
از آنجا که کاربرد عمده و مورد نظر این طبقه‌بندی، بهره‌گیری از آن در ارائهٔ یک معماری مرجع امنیتی برای حفاظت از اطلاعات است، در طبقه‌بندی ارائه‌شده نوع سیستم اطلاعاتی و اجزای تشکیل‌دهندهٔ یک سیستم اطلاعاتی (شبکه، سخت‌افزار، نرم‌افزار، رویه‌ها، پایگاه داده و کارکنان) مورد توجه قرار گرفته و اطلاعات تولیدشده توسط هر سیستم و یا جزء به‌صورت جداگانه طبقه‌بندی شده است.

در ارائهٔ این طبقه‌بندی از مجموعهٔ کاملی از مؤلفه‌های امنیتی محیط ابری که در ویرایش دوم «معماری مرجع» که توسط انجمن امنیت ابر[1] منتشر گردیده، استفاده شده است. مهم‌ترین ویژگی الگوی طبقه‌بندی اطلاعات ارائه‌شده عبارت‌اند از:

- ◇ جامع‌بودن و شمول حداکثری اطلاعات موجود در یک سازمان (مستقل از اندازهٔ سازمان و ماهیت کسب‌وکار آن)
- ◇ در نظرگرفتن حاکمیت واحد و یکپارچه برای سیستم مدیریتی سازمان و به‌تبع آن، ابر خصوصی سازمان
- ◇ جهت‌دهی طبقه‌بندی اطلاعات به مؤلفهٔ امنیتی و نگرش کل به جزء (شروع از سطح دغدغه‌ها و ادامه تا سطح راهکارها)
- ◇ ایجاد تناسب بین معماری ابر خصوصی سازمان و مؤلفه‌های امنیتی
- ◇ کاهش افزونگی‌ها و دوباره‌کاری‌ها با هدف کاهش ریسکِ وجود تناقض بین سیاست‌ها و راهکارهای پیاده‌سازی‌شده

شکل (۲) هفت حوزه و طبقه‌بندی سطح اول آنها را نشان می‌دهد. ۳۵۵ طبقهٔ اطلاعاتی استخراج‌شده، در هفت حوزه و سه سطح دسته‌بندی شده‌اند و متناظر با هر یک نیز می‌توان یک مؤلفهٔ امنیتی لحاظ کرد که برای اطمینان از حفظ امنیت آن ضروری است. در ادامه، هفت حوزه و سطح اول هر حوزه تشریح شده‌اند.

1. Cloud Security Alliance-CSA



شکل ۳. الگوی طبقه‌بندی اطلاعات سازمانی با دیدگاه امنیت اطلاعات

۶-۱. حوزهٔ سرویس‌های پشتیبان عملیات کسب‌وکار[1]: این حوزه، جنبه‌ها و موضوعاتی از قبیل منابع انسانی، پایش امنیت، اطمینان از عملکرد زیرساخت را در نظر می‌گیرد. مؤلفه‌های این حوزه عبارت‌اند از:

الف) امنیت منابع انسانی: اغلب حوادث و نقض‌های امنیتی به‌دلیل نبودِ کنترل، آگاهی و راهنما برای مهم‌ترین دارایی سازمان یعنی کارکنان رخ می‌دهد. این قابلیت، به‌منظور حصول اطمینان از وجود فرایند رسمی، روش‌های اجرایی، گزینش مناسب کارکنان و سایر موارد مرتبط با کارکنان و اشخاص ثالث همکار با سازمان ایجاد شده است.

ب) پایش امنیت: رویدادنگاری وقایع و تحلیل آنها، پایش پایگاه‌های داده و برنامه‌های کاربردی در این دسته قرار دارند.

پ) سرویس‌های حفاظت از زیرساخت: این سرویس‌ها، سرور، نقطه انتهایی[2]، شبکه و لایهٔ برنامه‌های کاربردی را امن می‌سازند.

1. Business Operation Support Services-BOSS 2. end-point

۶-۲. حوزهٔ عملیات و پشتیبانی فناوری اطلاعات[1]: این حوزه، همان واحد فناوری اطلاعات سازمان است که مسئول دریافت، ثبت و رفع مشکلات عملیات فناوری اطلاعات است. مؤلفه‌های این حوزه عبارت‌اند از:

الف) عملیات فناوری اطلاعات: عملیات فناوری اطلاعات ساختار سازمانی، الزامات مهارتی واحد فناوری اطلاعات و رویه‌های مدیریت عملیات را تعریف می‌کند تا سازمان توانایی مدیریت عملیات فناوری اطلاعات و زیرساخت مرتبط با آن را داشته باشد. این عملیات باید همسو با استراتژی سازمان باشد.

ب) تحویل سرویس: تحویل سرویس با فناوری‌های ضروری برای برقراری سرویس‌های بدون وقفه سروکار دارد. سرویس‌های این حوزه معمولاً شامل آنهایی است که برای کارکنان مناسب هستند؛ مثل: مدیریت دسترس‌پذیری، مدیریت سطح سرویس، تداوم سرویس و مدیریت ظرفیت.

پ) پشتیبانی سرویس: پشتیبانی سرویس روی دغدغهٔ اصلی کاربران یعنی اطمینان از دسترسی به‌موقع به سرویس‌های مورد نیاز تمرکز دارد. کاربران هنگام درخواست تغییر سرویس، با نیاز به به‌روزسانی و بروز مشکل در پشتیبانی سرویس مواجه می‌شوند. میز سرویس[2] تنها نقطهٔ تماس مشتری برای ثبت مشکلات است. میز سرویس تلاش می‌کند که در صورت وجود راهکار مستقیم، مشکل را حل کرده و یا یک حادثه را ثبت کند. ثبت حادثه، خود آغاز یک سری فرایندهاست که مدیریت حادثه، مدیریت مسئله، مدیریت تغییرات، مدیریت release و مدیریت پیکربندی از جملهٔ آنهاست.

ت) حفاظت از داده‌ها: در عصر اطلاعات، داده یک دارایی است. اما بیشتر داده‌ها تا زمانی که محافظت شده باشند، دارای ارزش هستند. حفاظت از داده باید شامل همهٔ مراحل چرخهٔ عمر داده، انواع داده و وضعیت‌های مختلف باشد. مراحل داده شامل ایجاد، ذخیره‌سازی، دسترسی، گردش، اشتراک و خروج از رده است. انواع داده ممکن است شامل دادهٔ ساختارنیافته مثل اسناد پردازش word، ساختاریافته مثل داده‌های موجود در پایگاه داده و نیمه‌ساختاریافته (semi) مثل ایمیل باشد. وضعیت‌های داده شامل داده در استراحت، داده در حال انتقال و داده در حال استفاده باشد.

1. Information Technology Operation & Support (ITOS)
2. service desk

۳-۶. حوزهٔ حاکمیت، مدیریت ریسک و انطباق: این حوزه شامل برنامهٔ امنیت اطلاعات سازمان به‌منظور محافظت از دارایی‌ها و کشف، ارزیابی و پایش ریسک‌های اطلاعات سازمان است. مؤلفه‌های این حوزه عبارت‌اند از :

الف) حاکمیت: فعالیت‌هایی از جمله حاکمیت سازمانی، مدیریت سطح بلوغ امنیتی سازمان و اطمینان از قابل قبول‌بودن آن، سیاست‌گذاری‌های کلان و اطمینان از یکپارچگی خط‌مشی‌ها و رویه‌های امنیتی در این حوزه قرار می‌گیرند.

همچنین، همان‌طور که سازمان، داده‌های بین برنامهٔ کاربردی و سرویس‌ها را مدیریت می‌کند، به یک مدل حاکمیت خوب تعریف‌شده برای چگونگی مدیریت، تبدیل و ذخیره‌سازی داده نیازمند است. حاکمیت داده شامل فرایندهایی از قبیل مالکیت داده، چگونگی طبقه‌بندی داده، مسئولیت‌های داده و کنترل‌های ضروری در طول چرخهٔ حیات داده است.

ب) مدیریت ریسک: مدیریت ریسک سازمان، مدیریت ریسک‌های باقیمانده و پایش وضعیت آنها و همچنین، مدیریت تهدیدات و آسیب‌پذیری‌ها که جزو مراحل ارزیابی ریسک سازمان است در این بخش قرار دارد. مدیریت آسیب‌پذیری، تلاش پیچیده‌ای است که در آن سازمان، دارایی‌ها را ردیابی کرده و در برابر آسیب‌پذیری‌های شناخته‌شده پایش نموده و از طریق اتخاذ اقداماتی مانند وصله‌زدن به نرم‌افزار، تغییر پیکربندی یا به‌کارگیری کنترل‌های دیگر در جهت کاهش اثرات مخرب به لایه‌های دیگر اقدام می‌کند. مدل‌سازی تهدیدات و آزمون نفوذ نیز بخشی از فعالیت‌های شناسایی مؤثر آسیب‌پذیری‌هاست.

مدیریت ریسک عملیاتی نیز ارزیابی ریسک را از دیدگاه کسب‌وکار مورد توجه قرار می‌دهد. با استفاده از چارچوب مدیریت ریسک، تهدیدات و آسیب‌پذیری‌های سازمان مشخص شده و ابزاری برای ارزیابی، مدیریت و کنترل ریسک‌های مختلف سازمان به‌دست می‌آید.

پ) خط‌مشی‌ها و استانداردها: خط‌مشی‌های امنیتی از الزامات مبتنی بر ریسک کسب‌وکار به‌دست آمده و در سطوح مختلف از جمله خط‌مشی امنیت اطلاعات، خط‌مشی امنیت فیزیکی، خط‌مشی تداوم کسب‌وکار، خط‌مشی‌های امنیت زیرساخت، خط‌مشی‌های امنیت برنامه‌های کاربردی و خط‌مشی مدیریت ریسک عملیاتی کسب‌وکار وجود دارند.

ت) انطباق: تمرکز این قابلیت در ردیابی و اثبات انطباق و برنامه ریزی برای رفع موارد عدم انطباق با الزامات قانونی، مقرراتی و قراردادی است.

حوزه‌های راهکارهای فناوری چهارگانه (سرویس‌های ارائه، سرویس‌های برنامهٔ کاربردی، سرویس‌های اطلاعات و سرویس‌های زیرساخت) مبتنی بر معماری چند لایهٔ استاندارد برای ساخت لایه‌های زیرساخت شبکه، داده‌ها، برنامه‌های کاربردی و تعاملات کاربر است که در ادامه تشریح خواهد شد.

۶-۴. حوزهٔ سرویس‌های ارائه: حوزهٔ سرویس‌های ارائه محلی است که کاربر نهایی با یک راهکار فناوری اطلاعات تعامل برقرار می‌کند. سرویس‌های این حوزه عبارت‌اند از:

الف) نوع سرویس: الزامات امنیتی برای حوزهٔ ارائه بر اساس نوع کاربر و نوع سرویس تغییر می‌کند. برای مثال، یک وب‌سایت تجارت الکترونیکی، چالش‌های امنیتی متفاوتی نسبت به سایت شبکهٔ اجتماعی دارد. نوع سرویس روی این قبیل چالش‌های امنیتی تمرکز دارد که بر اساس نوع کاربر و نوع سرویس متفاوت هستند.

ب) سکوی ارائه: سرویس های سکوی ارائه روی انواع مختلف نقاط انتهایی که کاربر در تعامل با راهکار استفاده می‌کند، از قبیل تجهیزات سیار، تجهیزات قابل حمل یا تجهیزات دارای کاربرد خاص تمرکز دارد. الزامات امنیتی بر حسب نوع دستگاهی که کاربر استفاده می‌کند، متفاوت است. برای مثال، یک دستگاه موبایل ریسک سرقت اطلاعات ذخیره‌شده در آن را دارد و یک ایستگاه عمومی مشترک[1]، ریسک دسترسی کاربر بعدی به اطلاعات کاربر قبلی را دارد. همچنین، این سرویس‌ها تکنولوژی‌های تعاملی مختلفی مثل تشخیص صدا یا دستخط را نیز شامل می‌شود.

۶-۵. حوزهٔ سرویس‌های برنامهٔ کاربردی: این حوزه شامل قوانین و فرایندهای پشت واسط کاربری است که داده‌ها را دستکاری می‌کند و تعاملات کاربر را انجام می‌دهد. مثلاً در یک بانک آنلاین، سرویس تراکنش پرداخت صورت‌حساب است که مقدار وجه را از حساب کاربر کسر و به حساب گیرنده اضافه می‌کند. همچنین، این سرویس‌ها فرایندهای توسعهٔ برنامهٔ کاربردی را نیز شامل می‌شود. سرویس‌های این حوزه عبارت‌اند از:

الف) فرایند توسعه: فرایند توسعه باید چالش های امنیتی را حین ساخت راهکار لحاظ نماید. این کار می‌تواند با استفاده از ابزارهایی مانند مرورگر کد منبع که درزهای امنیتی را

1. common public station

نشان می‌دهد و یا مرورگر آسیب‌پذیری برنامه‌های وب که مقاومت برنامه در برابر حملات متداول هکرها را نمایش می‌دهد، انجام شود.

ب) چرخهٔ حیات دانش امنیتی: برای ساخت برنامه‌های کاربردی امن، تیم توسعه باید به اطلاعات بروز و آخرین تهدیدات و شاخص‌های مناسب آگاهی داشته باشد.

پ) اتصال و یکپارچه‌سازی: واسط‌های برنامه‌نویسی، میان‌افزارهای یکپارچه‌ساز و مکانیزم‌ها، پروتکل‌ها و زبان مشترک برای انتقال دادهٔ معنادار بین دو برنامهٔ کاربردی در این بخش قرار دارند.

واسط‌های برنامه‌نویسی امکان تعامل و تبادل بین دو برنامه یا دو قطعه از یک برنامه را فراهم می‌آورد. برای این برنامه‌ها اعتباربخشی ورودی‌ها مهم است تا اطمینان حاصل شود که فقط ورودی‌های مورد انتظار ارائه می‌شوند. فقدان این کنترل در ورودی، آسیب‌پذیری ایجاد می‌کند و هکرها می‌توانند بدافزارهای خود را وارد برنامه کنند.

میان‌افزارهای یکپارچه‌ساز، ابزارهایی هستند که امکان تبادل اطلاعات بین برنامه‌های کاربردی بدون تعامل مستقیم با یکدیگر را فراهم می‌کنند. چالش امنیتی این سرویس‌ها حصول اطمینان از عدم خوانده‌شدن یا تغییر حین تحویل و اصالت ارسال‌کننده است.

سرویس‌های اتصال و تحویل مکانیزم‌های زیرینی هستند که از میان‌افزارهای یکپارچه‌ساز برای انتقال پیام بین برنامه‌های کاربردی استفاده می‌کنند. این سرویس‌ها باید حفاظت مورد نیاز از پیام، از جمله رمزنگاری را انجام دهند.

وقتی چندین برنامه کار مشابهی انجام می‌دهند، اغلب از مفهوم انتزاع استفاده می‌کنند و دارای زبان مشترک قابل فهم برای دیگران هستند. برای مثال، گرچه آژانس‌های هوایی پروازهای خود را متفاوت از یکدیگر مدیریت می‌کنند، ولی همهٔ آنها از یک انتزاع مشابهی استفاده می‌کنند، به‌گونه‌ای که سرویس‌های مسافرتی آن‌لاین می‌توانند پرواز مورد نظر را از بین همهٔ پروازها تشخیص دهند. این انتزاع‌ها باید مکانیزم امنیتی مناسبی داشته باشند تا در برابر دسترسی غیر مجاز محافظت شوند.

۶-۶. سرویس‌های اطلاعاتی[1]: یکی از نقاط قابل توجه در سازمان‌ها، حجم داده‌های تولیدشده در سازمان شامل داده‌های افزونه و تکراری است. همهٔ این داده‌ها باید به اطلاعات مفیدی تبدیل

1. Information Services

گردد تا مالکان دارایی‌ها بتوانند اولویت‌بندی و مدیریت ریسک‌های حوزهٔ خود را انجام دهند. این حوزه، استخراج، تبدیل و بارگذاری اطلاعات در یک مدل دادهٔ مشترک را مدیریت می کند. استخراج، تبدیل و بارگذاری، نرمال‌سازی داده، داده‌کاوی، در این حوزه است. این حوزه، کلیهٔ داده‌های عملیاتی (داده‌های مربوط به تراکنش‌های روزانه) و انبار داده‌ها (مخزن داده‌های کل سازمان) را شامل شده و دربرگیرندهٔ سرویس‌های زیر است:

الف) سرویس‌های دایرکتوری کاربر: همهٔ اطلاعات مربوط به کسب مجوز و احراز هویت در این بخش انجام می‌گیرد.

ب) مدیریت داده های پایش امنیتی: همهٔ موضوعات مرتبط با پایش امنیتی شامل پایش بیرونی (حفاظت از brand، هانی‌پات و جاسوسی سایبری)، پایش درونی (داده‌های مرتبط با روندها، الگوهای رفتاری و اطلاعات قضایی و تفحص)، گزارشات اجرایی (کارت امتیازی متوازن، داشبورد اجرایی و ثبت ریسک) و داده های مدیریت تهدیدات و آسیب‌پذیری‌ها (انطباق، وصله‌ها، وارسی سلامت پیکربندی، زیرساخت، برنامه‌های کاربردی و آسیب‌پذیری‌ها) در این گروه قرار دارند.

پ) مدیریت داده‌های تحویل سرویس: مدیریت داده‌های تحویل سرویس روی داده‌های ساختاریافته یا بدون ساختار مرتبط با مدیریت سرویس های فناوری اطلاعات در سازمان تمرکز دارد.

ت) مدیریت داده‌های حاکمیت داده: در حالی که برنامه‌های کاربردی و سرویس‌های فناوری اطلاعات در سازمان جاری شده و مدیریت می شوند، این حوزه شواهد مربوطه و داده‌های انطباق مناسب از طریق چرخهٔ حیات توسعهٔ نرم‌افزار را ذخیره می کند.

ث) مدیریت داده‌های حاکمیت، مدیریت ریسک و انطباق: همهٔ اطلاعات مرتبط با قابلیت‌های فنی امنیت اطلاعات شامل حاکمیت داده، امنیت برنامهٔ کاربردی و جلوگیری از گم‌شدن داده در بین سایر منابع اطلاعاتی در این حوزه ذخیره می‌شود.

ج) مدیریت داده‌های ITOS: این بخش داده‌های مرتبط با استراتژی و عملیات فناوری اطلاعات سازمان از قبیل مدیریت کیفیت، همراستایی فناوری اطلاعات و کسب‌وکار و ... را دربرمی‌گیرد.

چ) مدیریت داده‌های BOSS: همهٔ داده‌های مرتبط با سرویس‌های پشتیبان عملیات کسب‌وکار در این حوزه قرار می‌گیرد.

ح) سرویس‌های گزارش‌دهی: همهٔ ابزارهای تولید گزارش‌های عملیاتی، تصمیم‌سازی، کارت امتیازی متوازن، داشبورت‌ها که داده‌ها را به اطلاعات مفید کسب‌وکار تبدیل می‌کنند، در این حوزه قرار می‌گیرند.

۶-۷. حوزهٔ سرویس‌های زیرساخت: این حوزه قابلیت‌های اصلی برای پشتیبانی لایه‌های بالاتر معماری را فراهم می‌کند. این، لایه‌ای از سرویس است که از برنامه‌های کاربردی ابر را پشتیبانی کرده و بیشتر کاربران می‌توانند آن را ببینند. این سطح، از ماشین‌های مجازی، برنامه‌های کاربردی و پایگاه‌های داده تشکیل شده است. سرویس‌های زیرساخت را می‌توان به‌صورت ردیفی از رایانه‌ها، کابل‌های شبکه، منابع تغذیه، خنک‌کننده‌ها و سیستم اطفای حریق دید. همچنین، زیرساخت حقوق دسترسی نیز در این حوزه قرار می‌گیرد. سرویس‌های این حوزه عبارت‌اند از:

الف) سرویس‌های زیرساخت داخلی: سرویس‌های زیرساخت داخلی عمدتاً با دارایی‌های فیزیکی مورد استفاده توسط تأمین‌کنندهٔ سرویس ابری برای پشتیبانی سرویس‌های مجازی مرتبط است. گرچه این سرویس‌ها از دید کاربر پنهان هستند، ولی پایه و اساس عملیاتِ امن و قابل اطمینان می‌باشند؛ برای مثال، بدون وجود امنیت مناسب برای تجهیزات، یک خرابکار نیازی به واردکردن ویروس به شبکه ندارد، بلکه کافی است در بین تجهیزات قدم بزند و کابلی را از سرور جدا کند.

ب) سرویس‌های زیرساخت مجازی: زیرساخت مجازی، برخی از سرویس‌های مشابه موجود در زیرساخت فیزیکی را دارد. برای مثال، تصاویر نرم‌افزارها برای سرورهای مجازی که در سکوی مجازی‌شده روی سرور فیزیکی میزبانی می‌شوند، باید به‌صورت امن ساخته و مدیریت شوند. البته الزامات خاص زیرساخت مجازی از قبیل مجازی‌سازی ذخیره‌ساز، سرور و شبکه نیز وجود دارد.

پ) زیرساخت مدیریت حقوق ویژه: این زیرساخت تضمین می کند که کاربران دسترسی و حقوق مورد نیاز برای اجرای وظایف و مسؤلیت‌هایشان را با استفاده از مکانیزم‌های مدیریت دسترسی و هویت از قبیل مدیریت هویت، سرویس‌های احراز هویت، سرویس‌های صدور مجوز و مدیریت کاربردهای خاص دارند.

۷. روش تدوین معماری مرجع امنیتی محیط رایانش ابری

گام اول در ایجاد و برقراری امنیت شناخت چیزی است که باید مورد محافظت قرار گیرد. الگوی طبقه‌بندی ارائه‌شده در قسمت پیش، چارچوب کاملی از دارایی‌های اطلاعاتی را ارائه کرده است که سازمان را در شناسایی و طبقه‌بندی دارایی‌هایش کمک می‌کند.

برای رسیدن به یک معماری کلان امنیت، سازمان باید از یک روش استفاده نماید تا منابع محدود خود را به‌صورت هدفمند تخصیص دهد. امنیت، هزینه‌های متنوعی از قبیل هزینهٔ مادی، فضای فیزیکی، منابع انسانی و ... دارد و لازم است برای پیاده‌سازی هر کنترل امنیتی تحلیل هزینه-سود انجام گردد.

با نگاه سیستمی به موضوع برقراری امنیت در سازمان، لزوم اتخاذ یک روش مناسب‌سازی‌شده برای سازمان دو چندان خواهد شد. در ادامهٔ این تحقیق، روش تدوین معماری امنیت سازمان ارائه شده است.

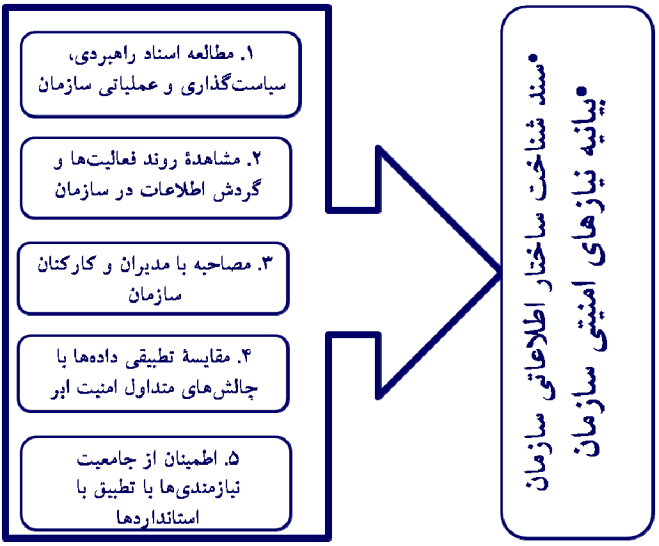
دو فرض اساسی در ارائهٔ این روش عبارت‌اند از:

- ◇ سازمان برای شناسایی و طبقه‌بندی دارایی‌های اطلاعاتی خود از الگوی طبقه‌بندی ارائه‌شده در بخش اول تحقیق استفاده کرده است.
- ◇ سازمان برای ارائهٔ خدمات فناوری اطلاعات خود از یک ابر سازمانی خصوصی استفاده می‌کند که مالکیت ابر در اختیار سازمان است.

روش پیشنهادی برای دستیابی به معماری مرجع امنیتی محیط رایانش ابرخصوصی شامل ۵ مرحله است که به اختصار در ادامهٔ مقاله تشریح شده‌اند.

۷-۱. شناخت سازمان و مهندسی نیازمندی‌های امنیتی آن: در این گام باید سازمان مورد مطالعه قرار گرفته و اهداف امنیتی و یا به‌عبارت عملیاتی‌تر، نیازهای امنیتی سازمان با استفاده از روش‌های مطالعهٔ اسناد، مشاهده، مصاحبه، مقایسهٔ تطبیقی با دغدغه‌های امنیتی سایر سازمان‌ها و نهایتاً نیازمندی‌ها با استانداردها مقایسه و هم‌ادبیات شود (شکل ۳).

همچنین، در گام اول، برای تعیین ورودی‌های معماری و شناخت سازمان توصیه می‌شود که از روش نشان‌داده‌شده در شکل (۳) استفاده شود که در واقع، جنبهٔ مبتنی بر واقعی‌بودن نیاز تحقیق را تقویت می‌کند. همچنین، روش زیر در حقیقت پاسخ به این واقعیت است که هر تحقیقی در حوزهٔ فناوری اطلاعات بدون شناخت صحیح سازمان، منجر به دستاورد قابل اجرا نخواهد بود. این گام در حقیقت، وجه تمایزی از تحقیق در سیستم‌های اطلاعاتی است که نیازمند لحاظ‌کردن سه جنبهٔ انسان، سازمان و فناوری است.



شکل ٤. فعالیت‌های گام نخست تحقیق مبتنی بر متدولوژی تلفیق علم طراحی و علم رفتاری

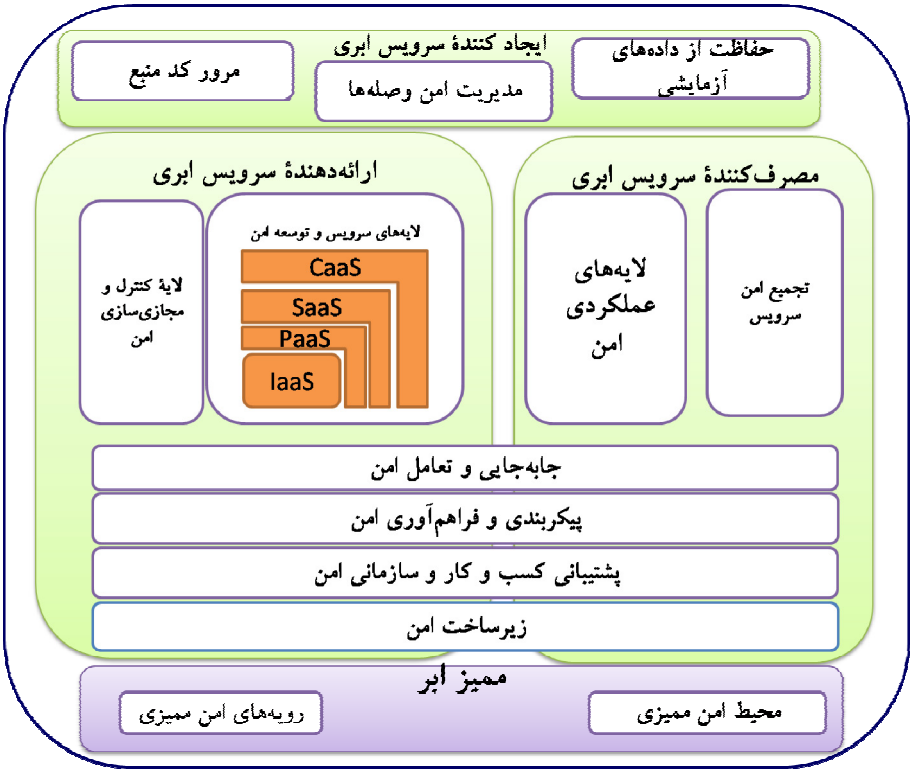
۷-۲. ترسیم معماری سطح بالای محیط ابری سازمان: ارائهٔ معماری امنیتی ابر سازمان بدون توجه به معماری محیط ابری امکان‌پذیر و واقع‌گرایانه نخواهد بود. بنابراین، در این مرحله معماری محیط رایانش ابری سازمان پیشنهاد شده است. این معماری با توجه به ساختار اطلاعاتی و عملیاتی سازمان بوده و مبنایی برای طرح‌ریزی معماری امنیتی محسوب می‌شود.

۷-۳. نگاشت مؤلفه‌های امنیتی با بازیگرهای ابری و مدل‌های پیاده‌سازی ابر: از خروجی‌های مهم معماری امنیتی، تعریف نقش‌ها و مسؤلیت‌هاست. این است که در این گام، مسؤلیت پیاده‌سازی مؤلفه‌های امنیتی به‌دست‌آمده در هر مدل ارائهٔ سرویس چهارگانه، که در گام دوم تعریف شده، باید تعیین شود. پس از تعیین الگوی طبقه‌بندی دارایی‌های اطلاعاتی و شناسایی مؤلفه‌های امنیتی متناظر با هر طبقه، لازم است مسؤلیت پیاده‌سازی هر مؤلفه تعیین شود.

۷-٤. تدوین مدل رسمی معماری مرجع امنیتی پیشنهادی: در این گام، با توجه به ماهیت هر مؤلفهٔ امنیتی و لحاظ‌کردن معماری محیط ابری سازمان، باید مدل رسمی معماری ترسیم شده و هر یک از اجزای معماری تشریح شود.

در این گام تحقیق، محیط ابری سازمان و دارایی‌های اطلاعاتی سازمان شناسایی شده است. هدف این گام ارائهٔ معماری امنیتی مرجعی است که تضمین کند کلیهٔ اطلاعات سازمان شناسایی شده و در دامنهٔ سیستم مدیریت امنیت اطلاعات سازمان قرار داده شده است. تنها در این صورت

است که می‌توان اطمینان داشت که دارایی‌های اطلاعاتی سازمان به‌گونه‌ای اثربخش محافظت می‌شوند. معماری امنیتی ارائه‌شده به‌صورت لایه‌ای در شکل (۴)، بازیگرهای ابری و اجزای معماری امنیتی تعریف‌شده برای هر بازیگر را نشان می‌دهد.



شکل ۵. معماری مرجع امنیتی پیشنهادی برای محیط رایانش ابری سازمان دارای ابر خصوصی

مصرف‌کنندهٔ ابر در معماری پیشنهادی، در واقع یک کارگزار سرویس ابر درونی[1] است که برخی از سرویس‌های مورد نیاز سازمان از جمله نرم‌افزارهای مأموریتی را از طریق ایجادکنندهٔ سرویس، تهیه و خود ارائه می‌کند و سرویس‌های عمومی را از ارائه‌دهندهٔ ابر دریافت و به کاربران نهایی ارائه می‌دهد. برای مصرف‌کنندهٔ ابری در معماری امنیتی پیشنهادی مؤلفه‌های پشتیبانی

1. Internal Cloud Service Broker- ICSB

کسب‌وکار امن، فراهم‌آوری و پیکربندی امن، جابه‌جایی و تعامل امن، پشتیبانی سازمانی امن و لایه‌های عملکردی امن و تجمیع[1] امن سرویس‌ها و لایهٔ زیرساخت امن در نظر گرفته شده است.

در معماری پیشنهادی، ارائه‌دهندهٔ ابر، یک کارگزار سرویس ابری بیرونی[2] است که سرویس‌های مشترک مورد نیاز کاربران نهایی را در اختیار آنان قرار می‌دهد. برای ارائه‌دهندهٔ سرویس‌های ابری در معماری پیشنهادی، مؤلفه‌های لایه‌های سرویس امن، لایهٔ کنترل و مجازی‌سازی منابع امن، لایهٔ زیرساخت امن، فراهم‌آوری و پیکربندی امن، جابه‌جایی و تعامل امن، پشتیبانی کسب‌وکار امن و پشتیبانی سازمانی امن در نظر گرفته شده‌اند.

ایجادکننده (یا ایجادکنندگان) سرویس‌های ابری، تیم‌های ایجاد، توسعه و پشتیبانی سرویس هستند که به‌صورت برون‌سپاری، سرویس‌های عمومی و مأموریتی مورد نیاز ابر خصوصی را برای سفارش ارائه‌دهندهٔ ابر یا مصرف‌کننده ایجاد کرده و توسعه و پشتیبانی آن را به عهده دارند. مؤلفه‌های معماری ایجادکنندهٔ سرویس ابری عبارت‌اند از: حفاظت از داده‌های آزمایشی و مرور کد منبع.

ممیز، بازیگر ابری است که ارزیابی‌های مستقل سرویس‌های ابری، عملیات سیستم‌های اطلاعاتی، عملکرد، حفظ حریم شخصی و امنیت پیاده‌سازی ابر را انجام می‌دهد. مؤلفه‌های معماری ممیز ابر عبارت‌اند از: محیط امن ممیزی و رویه‌های امن ممیزی.

۷-۵. ارزیابی الگوی طبقه‌بندی و معماری امنیتی پیشنهادی: اثبات کارآمدی دستاورد این تحقیق با روش کیفی و توصیفی انجام شده است. بدین‌منظور، ابتدا جامعیت الگوی طبقه‌بندی دارایی‌های اطلاعاتی سازمان و سپس برآورده‌شدن نیازمندی‌های امنیتی سازمان با پیاده‌سازی این معماری نشان داده شده است. همچنین، نظر خبرگان با استفاده از روش دلفی اخذ شده است.

به‌منظور اثبات کارآمدی معماری لازم است برآورده‌شدن نیازهای امنیتی سازمان توسط معماری پیشنهادی اثبات شود. لذا در این گام، مؤلفه‌های مورد نیاز امنیتی سازمان نگاشته می‌شوند تا از برآورده‌شدن نیازمندی‌های سازمان مورد نظر اطمینان حاصل گردد.

به‌منظور صحه‌گذاری روند طی‌شده در تحقیق و اخذ نظرات خبرگان در خصوص جامعیت الگوی طبقه‌بندی ارائه‌شده و معماری پیشنهادی، از روش دلفی و ابزار پرسشنامه طبق مراحل ذکرشده در روش تحقیق استفاده شد.

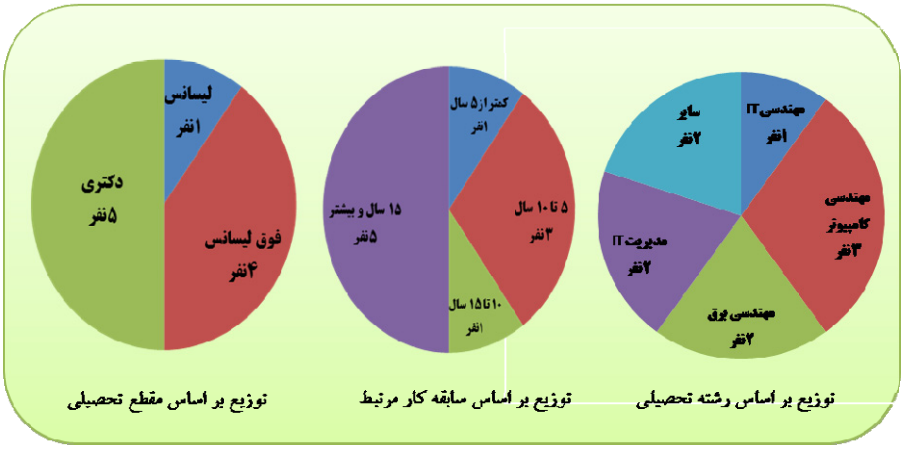
متداول‌ترین روش برای اثبات پایایی، محاسبهٔ ضریب آلفای کرونباخ است. هر قدر شاخص آلفای کرونباخ به عدد یک نزدیک‌تر باشد، همبستگی درونی بین سؤالات بیشتر و در نتیجه،

1. aggregation
2. External Cloud Service Broker- ECSB

پرسش‌ها همگن‌تر خواهد بود. کرونباخ ضریب پایایی ۴۵ درصد را کم، ۷۵ درصد را متوسط و قابل قبول، و ضریب ۹۵ درصد را زیاد پیشنهاد کرده است.

در این تحقیق برای ۱۵ سؤال نهایی پرسشنامه، ضریب آلفای کرونباخ با کمک نرم‌افزار SPSS برابر ۸۱۳/. محاسبه شد. با توجه به کم‌بودن تعداد متخصصان و کارشناسان این حوزه، نمونهٔ آماری برابر با جامعهٔ آماری در نظر گرفته شد.

جامعهٔ آماری متشکل از ۱۰ متخصص با مشخصات ذکرشده در شکل (۵) مورد استفاده قرار گرفت. در این نمونهٔ آماری، سه نفر از کارشناسان مدیریت اطلاعات فنی و امنیت سازمان نیز مشارکت داشته‌اند.



شکل ٦. جامعهٔ آماری خبرگان

نظرات ارائه‌شده در قالب پرسشنامهٔ نهایی جمع‌بندی شده است. با توجه به نتایج به‌دست‌آمده، الگوی طبقه‌بندی، متدولوژی مورد استفاده و معماری ارائه‌شده تا حد قابل قبولی به‌درستی طرح‌ریزی شده و به سازمان در دستیابی به شناسایی و طبقه‌بندی دارایی‌های اطلاعاتی و همچنین حفاظت از آنها در محیط ابر خصوصی خود و تضمین سطح امنیتی مورد نظر کمک می‌کند.

۸. جمع‌بندی، نتیجه‌گیری و پیشنهادات

افزایش روزافزون داده‌های تولیدشده در سازمان‌ها سبب شده است که سازوکارهای متنوعی برای ذخیره‌سازی داده‌ها صورت گیرد. همچنین، اطلاعات و نهایتاً دانش تولیدشده توسط انبوه

داده‌های سازمانی باید به‌گونه‌ای طبقه‌بندی و ذخیره‌سازی شود که ضمن اطمینان از ثبت کلیهٔ اطلاعات ارزشمند، قابلیت بازیابی و بهره‌گیری از آن در کمترین فرصت ممکن فراهم گردد.

از طرف دیگر، حرکت سازمان به سمت بهره‌گیری از مزایای محیط ابر خصوصی، مقولهٔ امنیت اطلاعات و جنبه‌های آن از جمله دسترس‌پذیری، صحت و جامعیت، محرمانگی، عدم انکار و ... را به یک موضوع جدی تبدیل می‌کند. بدیهی است که امنیت اطلاعات کسب‌وکار در محیط رایانش ابری قابل معامله با سایر مزایای بهره‌گیری از سرویس‌های محیط ابری نیست. لذا، برای توسعهٔ رایانش ابری، باید امنیت اطلاعات سازمان تضمین شود.

این دو دغدغهٔ اساسی باید از طریق یک راهکار جامع و مانع پاسخ داده شود تا همهٔ ذینفعان بتوانند به آن اعتماد کنند. لذا، در این تحقیق تلاش شد تا ابتدا الگوی جامعی از دارایی‌های اطلاعاتی سازمان ارائه شود. الگوی طبقه‌بندی دارایی‌های اطلاعات سازمانی ارائه‌شده در شکل (۲)، دارای مشخصه‌های زیر است:

- ◇ الگوی جامعی جهت طبقه‌بندی دارایی‌های اطلاعاتی سازمان به‌ویژه برای سازمان‌هایی که اطلاعات خود را به‌صورت دیجیتال تولید و ذخیره می‌کنند، ارائه داده است.
- ◇ تنوع داده‌های تولیدشده در سازمان و اطلاعات موجود را پوشش داده است.
- ◇ مبتنی بر پویایی و تغییر میزان اهمیت و حساسیت داده‌ها و اطلاعات سازمانی در چرخهٔ حیات آن (و گذر زمان) است.
- ◇ نمای قابل درکی از اطلاعات سازمانی ارائه کرده تا مدیران ارشد بتوانند با دید جامع، نسبت به تعیین نقاط حساس سازمانی برای توجه بیشتر در ایجاد امنیت اقدام نمایند.
- ◇ سطح‌بندی ارائه‌شده در الگو کمک می‌کند که دغدغه‌های امنیتی به راهکار امنیتی نزدیک شده و انتخاب راه‌حل‌های امنیتی برای متخصصان امنیت ساده‌تر شود.
- ◇ مبنای مناسبی برای پیاده‌سازی سیستم مدیریت امنیت اطلاعات سازمان در محیط پیچیده ابری است.

همچنین، در ادامه این تحقیق به‌منظور راهنمایی سازمان در تدوین معماری امنیتی خود، یک روش به شرح زیر ارائه شده است:

گام اول: شناخت سازمان و مهندسی نیازمندی‌های امنیتی سازمان
گام دوم: ترسیم معماری سطح بالای محیط ابری سازمان
گام سوم: نگاشت مؤلفه‌های امنیتی با بازیگرهای ابری و مدل‌های پیاده‌سازی
گام چهارم: تدوین مدل رسمی معماری مرجع امنیتی
گام پنجم: ارزیابی الگوی طبقه‌بندی و معماری امنیتی پیشنهادی

با استفاده از الگوی شناسایی و طبقه‌بندی دارایی‌های اطلاعاتی و متدولوژی ارائه‌شده، معماری مرجع امنیتی محیط رایانش ابر خصوصی یک سازمان مشخص مطابق شکل (۴) ترسیم شده و پس از اثبات برآورده‌سازی نیازمندی‌های امنیتی سازمان، کارآمدی و قابلیت پیاده‌سازی آن توسط متخصصان صحه گذاری شد.

فهرست منابع

سازمان ملی استاندارد ایران. ۱۳۸۷. *فناوری اطلاعات - فنون امنیتی- آیین کار مدیریت امنیت اطلاعات*. تهران: سازمان ملی استاندارد ایران.

ـــــ. ۱۳۸۷. *فناوری اطلاعات - فنون امنیتی - الزامات سیستم مدیریت امنیت اطلاعات*. تهران: سازمان ملی استاندارد ایران.

Cherdantseva, Y., and J. Hilton. 2013. *R*eference Model of Information Assurance & Security. 8th International Conference on Availability, Reliability and Security (ARES) 2013, University of Regensburg, Germany. IEEE Proceedings.

IBM Corporation. 2012. *IBM Cloud Computing Reference Architecture 3.0 – Security. New York: IBM publications*.

ISO/IEC 27000. 2014. *Information technology-Security techniques-Information security managementsystems-overview and vocabulary*. Switzerland: ISO publications.

Furht, B. and A. Escalante. 2010. *Handbook of cloud computing*. London: Springer Publishing Company.

Kannegati, R., and P. Chodavarapu. 2008. *SOA Secutiry, Manning*. In Proceedings of the 2001 Workshop on New Security Paradigms NSPW '01, 2001 Tokyo: Elsivier Publications.

Mell, P., and T. Grance. 2011. *The NIST definition of cloud computing.* New York: NIST Publications: National Institute of Standards and Technology.

Peffers, K. 2007. A design science research methodology for information systems research. *Journal of management information systems*. 12: 68-79.

Subashini, S, and V. Kavitha. 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications* Vol. 01. 4:33-59

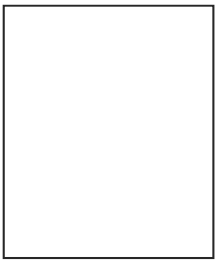
Velte, T., A. Velte, and R. Elsenpeter. 2010. *Cloud computing, a practical approach*. New York: McGraw-Hill.

Von Alan, R. H. 2004. *Design science in information systems research.* Journal of MIS quarterly.

Winkler, Vic Jr. 2011. *Securing the Cloud: Cloud computer Security techniques and tactics.* London: Elsevier publications.

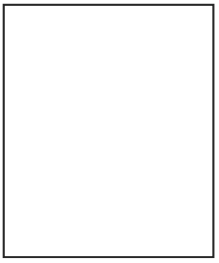
مصطفی تمتاجی

اطلاعاتی از این پدیدآور به نشریه ارائه نشد.



مهدی نقیان فشارکی

اطلاعاتی از این پدیدآور به نشریه ارائه نشد.



سیدغلامحسن طباطبایی

اطلاعاتی از این پدیدآور به نشریه ارائه نشد.