IEEE SA
STANDARDS ASSOCIATION

IEEE Standard for Big Data Business Security Risk Assessment

IEEE Consumer Technology Society

Developed by the
Standards Committee

IEEE [illegible]d 2[illegible]13™-2020

IEEE

STANDARDS

IEEE Standard for Big Data Business Security Risk Assessment

Developed by the

Standards Committee
of the
IEEE Consumer Technology Society

Approved 24 September 2020

IEEE SA Standards Board

Abstract: The purpose of this standard is to standardize the reference framework and technical measures of Internet business security risk assessment based on big data technology, summarize and abstract internet business event data, and determine and quantify Internet business security risk through rule model and artificial intelligence model, covering the fields of text recognition, video recognition, voice recognition, picture recognition, URL identification, behavior identification and other aspects, including service provider's organization and personnel management, system and process development, data protection and other strategies, provide reference guide and technical support for security planning, security construction and security operation of big data business security risk assessment.

Keywords: artificial intelligence model, big data business security risk, IEEE 2813™, rule model

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

PDF: ISBN 978-1-5044-7084-1 STD24422
Print: ISBN 978-1-5044-7085-8 STDPD24422

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (https://standards.ieee.org/ipr/disclaimers.html), appear in all standards and may be found under the heading "Important Notices and Disclaimers Concerning IEEE Standards Documents."

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA, and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE standards documents are supplied "AS IS" and "WITH ALL FAULTS."

Use of an IEEE standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON, ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE is the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents**.

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and Standards Coordinating Committees are not able to provide an instant response to comments, or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile and Interests area of the IEEE SA myProject system. An IEEE Account is needed to access the application.

Comments on standards should be submitted using the Contact Us form.

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; https://www.copyright.com/. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit IEEE Xplore or contact IEEE. For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE SA Website. Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in IEEE Xplore. Users are encouraged to periodically check for errata.

Patents

IEEE Standards are developed in compliance with the IEEE SA Patent Policy.

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at https://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. IEEE Standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

Participants

At the time this standard was completed, the BDBSRA Working Group had the following entity membership:

Yongxia Wang, *Chair*
Baiqing Sun, *Vice Chair*
Daozhuang Lin, *Secretary*

Organization Represented	*Name of Representative*
0xSenses Corporation	Daozhuang Lin
Anhubao Corporation	Huafeng Li
Chaincomp Technologies Co., Ltd.	Yuxi Dong
China Academy of Information and Communications Technology	Song Kong
DNV GL Business Assurance (China) Co. Ltd.	Han Fang
Harbin Institute of Technology	Baiqing Sun
Hangzhou Hikvision Digital Technology Co., Ltd.	Bin Wang
JD.com, Inc.	Wendi Song
Shanghai Di'an Technology Inc.	Chucheng Yuan
Tencent	Yongxia Wang
The Third Research Institute of The Ministry of Public Security	Yan Chen

The Working Group gratefully acknowledges the contributions of the following participants. Without their assistance and dedication, this standard would not have been completed.

Xiang Wang, *Technical Specialist*

Wei Dai Cai Xin Juan Bin Zhou

The following members of the entity Standards Association balloting group voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Anhubao Corporation
China Academy of Information and Communications Technology (China Academy of TeleCommunication Research, MIIT)
CAICT (CATR)
DNV GL Business Assurance (China) Co., Ltd.
Harbin Institute of Technology
Hesai Technology
JD.com, Inc.
Panasonic Corporation of North America
Shanghai Di'an Technology Inc.
Tencent
The Third Research Institute of The Ministry of Public Security

When the IEEE SA Standards Board approved this standard on 24 September 2020, it had the following membership:

Gary Hoffman, *Chair*
Jon Walter Rosdahl, *Vice Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Ted Burse
Doug Edwards
J. Travis Griffith
Grace Gu
Guido R. Hiertz
Joseph L. Koepfinger*
David J. Law
Howard Li
Dong Liu
Kevin Lu
Paul Nikolich
Damir Novosel
Dorothy Stanley
Mehmet Ulema
Lei Wang
Sha Wei
Philip B. Winston
Daidi Zhong
Jingyi Zhou

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 2813, IEEE Standard for Big Data Business Security Risk Assessment.

Internet technology began to show a rapid development trend in the 1990s, and business risks began to emerge in the early 2000s, such as a large number of traffic risks in social products, content violations, credit fraud, false registrations, and so on. These Internet business security risks endanger Cyberspace Security.

In the industrial Internet era, business security has become a potential limit on enterprise development. With business cloud solutions becoming the norm of enterprise information construction, industrial security should be embedded in the whole process of sales, operation, production, management, etc. More and more cloud companies are improving their own security capabilities by establishing security risk control teams, purchasing third-party big data risk control services, and the service mode of business security is gradually evolving toward the cloud service mode of free configuration and high stickiness continuous transaction. At the same time, at present, intelligent risk control is in a high-speed development stage. Mature big data business security risk control services usually use a number of AI technologies to build core risk control capabilities.

At the beginning of 2020, the new coronavirus disease (COVID-19) pandemic had a profound impact on almost all types of organizations and people in the world. During the pandemic, programs that provide the public with many convenient functions such as epidemic inquiry, epidemic prevention and control, mask purchase, material donation, online shopping, online education, cloud conferencing, etc., launched one after another, and generally needed to be completed within a limited time (e.g., of one to three days), which requires fast iteration and upgrading of service functions. At the same time, the programs also faced complex cross network exchange issues, operational pressures several times higher than usual, and-potential illegal hacker attack threats, in which the security risk control service of big data business plays a great role.

With the rapid development of technology, however, it is urgent to establish corresponding standards to guide the application of the industry and standardize technical capabilities. BSI issued pas201:2018 “Guide to supporting the cooperation between fintech companies and financial institutions” in 2018, which provides fintech companies with a full process guide from proposing the concept of fintech solutions, improving business models, clarifying the technology development roadmap, and signing cooperation legal agreements to final deployment and implementation.

The purpose of this standard is to standardize the reference framework and technical measures of Internet business security risk assessment based on big data, summarize and abstract internet business event data, and determine and quantify Internet business security risk through rule model and artificial intelligence model. It covers the fields of text recognition, video recognition, voice recognition, picture recognition, URL Identification, behavior identification and other aspects, including service provider’s organization and personnel construction, system and process development, data protection and other strategies, provide reference guide and technical support for security planning, security construction, and security operation of big data business security risk assessment.

Contents

IEEE Standard for Big Data Business Security Risk Assessment

1. Overview

This standard can be applied to internet-based business scenarios, and can also be served serve as a practical guide to achieve help assess business security risk control through the big data technology.

This standard can be applied in other types of organization, including public or privately-owned or state-owned enterprises, associations, or organizations, or by individuals, to improve assessment of their protection capability against business security risks based on big data technology.

1.1 Scope

This standard describes security risk assessment methodologies of user behavior, the applicable analysis layer, and the fundamental analysis layer for big data.

1.2 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).[1,2]

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

[1]The use of the word *must* is deprecated and cannot be used when stating mandatory requirements, *must* is used only to describe unavoidable situations.
[2]The use of *will* is deprecated and cannot be used when stating mandatory requirements, *will* is only used in statements of fact.