IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Method For Endpoint Aware Inspection In A Network Security Solution

Mohd Imran[1], Mohammed Waheeduddin Hussain[2], Subramanian K.M[3]

[1]PG Scholar, Department of Information Technology, Shadan College of Engineering and Technology, Hyderabad,

[2]Professor, Department of Information Technology, Shadan College of Engineering and Technology, Hyderabad,

[3]Professor, Department of Computer Science and Engineering, Shadan College of Engineering and Technology, Hyderabad,

ABSTRACT

Due to the flood in remote work after the episode of Covid, network security has gained a giant fixation. The issue of mixed-up audit decisions in network security plans has for quite a while been reprimanded, but the meaning of the decision precision has never been overall around as critical as today. In this paper we offer a response for additional fostering the assessment decision accuracy by deciding a method for endpoint careful survey in an association security plan prepared for performing significant package examination. The method utilizes a subset of the protected association to gather hash fingerprints from the endpoint application network traffic plans. The information collected from this subset is then utilized for procuring endpoint care for the rest of the protected organization. We use strategies that work on the application layer of the show stack. This makes the strategy fitting not only for neighborhood executions, as NGFWs and IPSs, yet also for SaaS and SASE game plans. The methodology is, regardless, conveniently utilized with lower layer information, for instance, association and transport layer information, for working system care too. We similarly present a proof-of-thought context-oriented examination where that is the thing we see, of the relevant association affiliations, 100% could be recognized while the functioning system and endpoint application were accessible in the source pack. All things considered, this is the primary method to redesign the assessment cycle accuracy by using a subset of the protected association to secure endpoint care.

INTRODUCTION

In a Supportive Unpremeditated Connection (MANET), each center point is outfitted with a radio transmitter and a recipient, which grants them to talk with the plan through distant bidirectional correspondence. The focal inspirations driving why MANETs grant data transmission with proportionate attributes while staying aware of their dynamic strategy are as demonstrated by the going with: It is puzzling for sort out that the transmission level of this transmission is more confined than the past transmission scope, making data exchanging all through the structure immeasurable for the larger part place centers. An essential issue with wi-fi Off the cuff affiliations is the way that restricted spots rely on batteries, which will routinely be underpowered in different locales, and it requires a great deal of speculation to recharge or displace them. A huge block to the all over utilization of battery invigorated contraptions has persevered, paying little regard to advancements in battery term improvement. More focus on reachable show, stage, and improvement strategy ought to vanquish this obstacle. Power for centers in an especially picked structure is as often as possible given by batteries or gigantic electrical power sources, depend on the situation. The remarkably delegated development's show is genuinely hampered by its inability to get power supplies given their short possibilities. Perhaps of the most inescapable way by which power is mishandled is through conversation. More prominent assessment ought to achieve the objective of killing incredibly additional practicality from their for the most part goliath battery length resources, which has moved back to a crawl of late and there have been no famous achievements around here. Right when a cell place point's remote port is turned off, which happens when the contraption is inert or snoozing, energy use has been shown to probably package transport. This has incited stresses over how much energy is wasted. Contraptions used in cell especially picked structures need adaptability since they are beneficial. Incidentally, they have weight and size limits, as well as resource necessities in regards to bind and information transmission. To revive past what many would consider conceivable, the center centers ought to end up being more awkward and less adaptable. As such, the monstrousness reasonableness of MANETs continues to be a major arrangement brand name. MANETs, as other radio-based correspondence structures, are feeble against various risks. Outside aggressors, as well as getting into wickedness objects inside, are among the dangers. Along these lines, an arrangement of information certificate systems, including data security, access control and character the supervisors ought to be done to protect these structures against cyberattacks. The use of faraway affiliations and the versatility of different contraptions in such affiliations has different fundamental results, and some striking deterrent confirmation cycles and executions don't quickly become hazy from establishment-based web show (IP) address affiliations. Man-in-the-Middle attacks are ending up being more normal as the interest for fast and web contraptions makes. The constraint of misleading alarms and wrong cases of center concentrations from networks is by and large high because of

the opportunity of inefficient show pack move. These potential extensions when the client moves about in the system, which upsets conveys and makes a goliath number of pathways. There are no fundamental segments of the plan, similar to switches, switches, and firewalls in wired IP affiliations, where all fitting visitors may be seen and analyzed to see criminal method for managing acting. The principal control of this assessment is to help significant solid areas for a controlling evaluation for MANET. It relies on a Microorganisms for Making Improvement Evaluation (BFOA). The safeguarded iterative controlling system depends on CH affirmation and infringe center point area. The CH affirmation depends on the craziest trust of mischievous, direct, and propelling trust values. The end regard accepted is used to see the meddled center point for capable and conspicuous preparation. It has a major effect on start by picking the CHs from the MANETS standard space that have the best worth of traffic circle, direct, and propelling notion to proceed. This is steadfastly followed by an impedance confirmation system for seeing burst in concentrations and ensuring that their social affairs are constantly given from starting to objective, as well as all strong organizing, which is gotten to by the BFOA. It is given, past what many would think about conceivable, and relationship of the way, the depicted explanation limit is subject to those credits. A positive concordance may be made among mining and control times of the computation, paying little heed to what the way that the proposed strategy takes use of the potential increments of the BFOA. Following the exposure of a social occasion dropping attack, the rehashed results will be stood separated from the affirmed results. The remainder of this work is created as follows: The connected works are shown To some extent II. The proposed BFOA is grasped in Area III. The consequences of the proposed framework, as well as an explanation, are presented in Segment IV. Region V gives an end.

SYSTEM ARCHITURE

Technologies that effectively safeguard data in a shared environment. For numerous applications, a variety of approaches for data protection in the cloud environment have been investigated and developed. This article focuses on providing effective protection by avoiding leakage and identifying the malevolent entity responsible for leakage as shown in Fig. 2. Typically, data protection is performed by leakage prevention and leaker detection. The primary strategies for preventing data leakage are customized using machine learning techniques, access control systems, differential privacy, and cryptography, whereas the main methods for detecting leakers include watermarking and probabilistic methods.

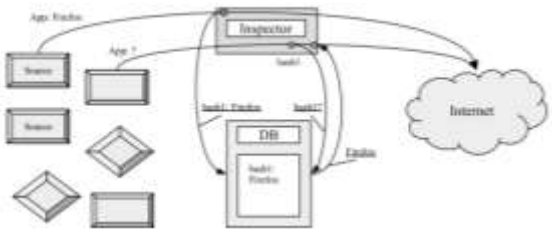


Fig 1: Block Diagram of Sharing Moment

MOTIVATION

The use of dynamic scanners is one of the most notable deals with any consequences regarding giving detectable quality to the endpoints. Dynamic scanners may be presented freely, or they can be an integrated part of the association security structure itself. Models of dynamic scanners are Nmap and Nessus. Nmap is permitted to use open-source programming. It contains a part named "Structure revelation'', which reveals information on the endpoint application considering a working result. Nmap can as have now recognize more than 8800 unmistakable endpoint applications additionally, interpretations. Nessus on the other hand is a business scanner which completes components like port checking and shortcoming sifting. Dynamic analyzing has its motivations, especially in perceiving the server applications. Regardless, client applications can't be covered with dynamic inspecting. Moreover, dynamic scanning ought to be performed every time to keep awake with the most recent data base of the assets, which can take time. Despite everything, toward the day's end, it is possible that the version or even the endpoint application changes between the scopes.

OUR CONTRIBUTION

The following is a summary of the article's significant contributions:

1) The main and important methods for data security through safe sharing in a cloud context are reviewed in this paper.

2) We offer the following information regarding each strategy. (a)How it functions in terms of data protection, and (b) the superior, ground-breaking options available.

In order to make it simple for readers to understand the essence of the approach as well as its applications, we also include potential and valuable information about each presented solution in a tabular manner, such as its working, implementation environment, success, range of the provided model, etc.

3) A thorough and comparative study of the methodologies covered is conducted and presented in an accessible manner. Additionally, research is done to determine which technique will best meet the needs.

EXISTING SYSTEM:

In light of the flood in remote stir after the eruption of Covid, network security has obtained a gigantic fixation. The issue of wrong assessment decisions in network security courses of action has for quite a while been censured, but the meaning of the decision precision has never been just similarly huge as today. The association security scene experienced a startling change in light of the Covid pandemic, as remote work transformed into the norm inside two or three months. The serious necessity for network security plans put additional pressure on the association security course of action providers as well, and issues that might have been centered around lower before the pandemic quickly ended up being high need. One of such issues is the accuracy of significant group evaluation related insights. An association security course of action, which is used for giving additional security to the association, may involve different components for separating the association traffic. These features habitually consolidate significant pack evaluation, interference contravention structures, network application conspicuous confirmation, URL and content plan and TLS unscrambling. Dependent upon the association security course of action, it could have the choice to end content it considers noxious, or it may very well give extra the accomplice editor arranging the review of this creation and supporting it for

appropriation was Tiago Cruz Information for the association director.

Existing System Disadvantages:

- Many privacy-preserving schemes have been proposed in recent years.
- While the file is uploading we can't have a security.

LITERATURE SURVEY

Cybersecurity Fingerprinting Techniques for OS Recognition.

This paper describes a prototype system for continual health monitoring at home. The system consists of an unobtrusive wireless body area network (WBAN) and a home health server. The WBAN sensors monitor user's heart rate and locomotive activity and periodically upload time-stamped information to the home server. The home server may integrate this information into a local database for user's inspection or it may forward the information further to a medical server. The prototype may be used for ambulatory monitoring of patients undergoing cardiac rehabilitation or for monitoring of elderly at home by informal caregivers.

HTTPS traffic analysis and client identification using passive SSL/TLS fingerprinting.

This paper presents a novel energy-efficient MAC Protocol designed specifically for wireless body area sensor networks (WBASN) focused towards pervasive healthcare applications. Wireless body area networks consist of wireless sensor nodes attached to the human body to monitor vital signs such as body temperature, activity or heart-rate. The network adopts a master-slave architecture, where the body-worn slave node periodically sends sensor readings to a central master node. Unlike traditional peer-to-peer wireless sensor networks, the nodes in this biomedical WBASN are not deployed in an ad hoc fashion. Joining a network is centrally managed and all communications are single-hop. To reduce energy consumption, all the sensor nodes are in standby or sleep mode until the centrally assigned time slot. Once a node has joined a network, there is no possibility of collision within a cluster as all communication is initiated by the central node and is addressed uniquely to a slave node. To avoid collisions with nearby transmitters, a clear channel assessment algorithm based on standard listen-before-transmit (LBT) is used. To handle time slot overlaps, the novel concept of a wakeup fallback time is introduced. Using single-hop communication and centrally controlled sleep/wakeup times leads to significant energy reductions for this application compared to more ldquoflexiblerdquo network MAC protocols such as 802.11 or Zigbee. As duty cycle is reduced, the overall power consumption approaches the standby power. The protocol is implemented in hardware as part of the Sensium trade system-on-chip WBASN ASIC, in a 0.13- mum CMOS process.

Analyzing HTTPS encrypted traffic to identify user's operating system, browser and application.

Integration of miniature sensors composes a wireless body area network (WBAN), which enables remote health monitoring. To make this technology widely acceptable in the society, some studies suggest commonly used gadgets such as cell phones or laptops as a hub for WBANs. In these cases, envisaged medical and non-medical applications of WBANs must have the same priority unless in emergency situations. Also, medical applications of WBANs need some strict requirements that are not that important for non-medical applications, such as very low-power consumption or reliability. In addition, channel condition may change in WBANs because of fading effects and this causes packet loss. Therefore proper traffic prioritization, high reliability and efficient channel utilization are vitally important issues in these networks. In this study, the authors improve the performance of the medium access control (MAC) protocol of WBANs using an adaptive resource allocation and traffic prioritization according to the medical situation of user and channel condition. Through adaptively separating and managing the possible traffics of WBANs, the heterogeneous requirements of different applications are provided. Analytical and simulation results show that the proposed MAC protocol outperforms IEEE 802.15.4 and IEEE 802.15.6 MAC protocols in terms of power consumption as well as the channel utilization and reliability.

Some applications of Rabin's fingerprinting method,'' in Sequences.

We investigated different encryption algorithms for sport wearable devices by utilizing a newly developed data generator for the testing purposes. Additionally we investigated different data encryption algorithms for a NoSQL DBMS. Testing results for data generator, data encryption and NoSQL database stress testing are presented and discussed as well. The research project was conducted in support of NSERC grant "GAUGE: Exact Positioning Systems for Sport and Healthcare Industries".

Evaluating the detection accuracy of JA3 and JA3S in security monitoring of SSL communication.

Wearable devices such as smart watch and bracelets continually broadcast Bluetooth Low Energy (BLE) signals, which can be easily captured by monitoring devices such as WiFi routers and Bluetooth scanners. As more and more wearable devices emerge, unauthorized monitoring and tracking by adversary becomes great privacy threats not only in the cyber world, but also in the physical world. To protect location privacy, this paper presents a real-life location monitoring system that is based on BLE privacy feature that changes the device physical address periodically. To enable users to better control their privacy level while still providing monitoring and tracking service to authorized parties (e.g., for child and elderly care), we extend BLE privacy by enriching its privacy semantics with a comprehensive set of metrics, such as simple opt-in/out, k-anonymity, and granularity-based anonymity. The system has been implemented and evaluated in terms of accuracy and user study.

PROPOSED SYSTEM

In this paper we offer a response for additional fostering the survey decision accuracy by deciding a method for endpoint careful assessment in an association security plan prepared for performing significant bundle examination. The strategy utilizes a subset of the safeguarded association to collect hash fingerprints from the endpoint application network traffic plans. The information gathered from this subset is then utilized for procuring endpoint care for the rest of the protected organization. We use strategies that work on the application layer of the show stack. This makes the method material not only for neighborhood executions, as NGFWs and IPSs, yet also for SaaS and SASE game plans. The system is, nevertheless, easily utilized with lower layer information, for instance, association and transport layer information, for working structure care as well. We moreover present a proof-of-thought logical examination where that is the thing we see, of the relevant association affiliations, 100% could be recognized while the

functioning system and endpoint application were accessible in the source bundle. All things considered, this is the chief method to redesign the examination collaboration accuracy by using a subset of the shielded association to gain endpoint care.

ADVANTAGE

- Providing more security
- Reducing storage cost.
- For secure semantic optimal matching on the cipher text.

MODULES NAME

1. Client

In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.

2. Server

This is the first module Data User can register and Login. After login Data User have an option of searching the files as a file name. Data user can also have a download file it will show an encrypted data. Data user can also send a trapdoor request to the server. Server can accept the the request and then data user can takes permissions from the owner then the file it will downloaded in plain text.

3. Inspector

This is the Second module of this project. In this module Data Owner should register and Login. Data Owner will Uploads the files into the database. Data owner can also send request to the data user.

4. Result

This is the third module of this project. In this module Cloud Server can login. After login it will see all data owners' information. Cloud server can see all users' information. Cloud server can see an all-stored data files. Cloud server can give keys request to the user. Cloud server can also see an attacker information of file.

PROPOSED ALGORITHM

Inspection decision accuracy

In this section we specify a method for endpoint aware inspection in a network security solution capable of performing deep packet inspection. Utilizing this method, a network security solution can have higher confidence in its deep packet inspection-based decisions by gaining an awareness of the protected endpoint application. The method consists of four components which are utilized in four steps.

The four components used by the method are the Target, the Source, the Inspector and the Database.

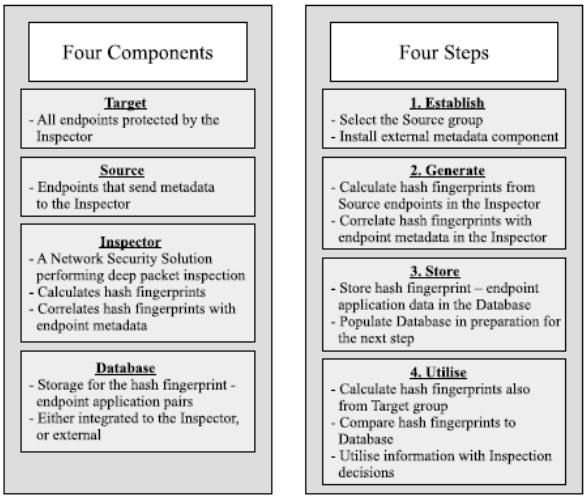
• The Target: The entire set of protected endpoints.

• The Source: A subset of the endpoints belonging to the Target that send metadata to the Inspector about the Endpoint applications for each connection.

• The Inspector: A network security solution which performs deep packet inspection on the traffic, is able to calculate hash fingerprints from it, and correlate them with the endpoint application based on the received Metadata.

The Database: A storage for the endpoint application - Hash fingerprint pairs. The database can be integrated to The Inspector, or it can be an external component.

These four components are then taken into use in four Steps: Establish, Generate, Store and Utilize. Provides a good sample of the Target group. Install to The selected endpoints an external component which Provides endpoint metadata for the Inspector on each new network connection.



2. Generate: For a suitable period of time, calculate hash Fingerprints in the Inspector for the network connections Initiated by endpoints in the Source group. Correlate Hash fingerprints with the endpoint application.

3. Store: Store the correlated hash-endpoint application Pairs in the Database. During this period the Database is populated so that enough information has been gathered to have a good coverage of the network traffic for the Next step.

4. Utilize: Start calculating hash fingerprints in the Inspector also for the network connections initiated by the endpoints in the Target group. Deduce the endpoint Application based on the information in the database, and use the information when making an inspection Decision. During this phase, the Database will continue to be populated from the data received from the Source Group to keep it current.

EXISTING ALGORITHM

Decision accuracy

Decision aids are increasingly in demand. Often implemented as computer algorithms, developments in data availability and computational capabilities have expanded the reach of these tools into much of everyday life. From the mundane, such as deciding which TV show to binge next, to the momentous, such as recommending surgery to a patient, algorithms synthesize vast amounts of information to provide users with on-demand recommendations. In three experiments, we sought to understand when and why people use an algorithm decision aid. Distinct from recent approaches, we explicitly enumerate the algorithm's accuracy while also providing summary feedback and training that allowed participants to assess their own skills. Our results highlight that such direct performance comparisons between the algorithm and the individual encourages a strategy of selective reliance on the decision aid; individuals ignored the algorithm when the task was easier and relied on the algorithm when the task was harder. Our systematic investigation of summary feedback, training experience, and strategy hint manipulations shows that further opportunities to learn about the

algorithm encourage not only increased reliance on the algorithm but also engagement in experimentation and verification of its recommendations.

VIII. SCREENSHOTS

Index Page

CSP Home Page

Attacker Page

User Home page

File Attacker Page

FUTURE ENHANCEMENT

For future exploration, the inborn connections of potential disappointment modes and disappointment causes referenced above, for example, flowing disappointments and normal reason disappointment modes, can be researched to extricate greater unwavering quality data connected with disappointments. In the interim, the more perplexing successions, the delay between two V&V exercises, and emphases of V&V exercises ought to be thought of. What's more, the rot impacts of different iterative V&V exercises for a disappointment mode will likewise be viewed as in our further exploration. Finally, the presentation of other existing cutthroat message mining techniques will be examined to streamline the message mining strategies in our future examination.

CONCLUSION

The safe improvement steering calculation settles both the energy issue and the correspondence inertness between bounces. Microorganisms for Maturing Advancement Calculation has been utilized to create a productive steering approach (BFOA). The Fluffy bunching approach is the article previously researched the text digging strategies for mining the stowed away dependability data from the customary DFMEA report. In particular, two sorts of secret unwavering quality data, including the relationship between's the disappointment related watchwords in potential disappointment modes or disappointment causes, and the disappointment arrangement of potential disappointment modes or disappointment causes, were explored. These two bits of found secret unwavering quality improvement data have not been surely known and used through customary DFEMA reports.

Such newfound dependability data can give critical direction to item plan improvement at prior plan stage. Second, a quantitative item V&V exercises arranging model was proposed interestingly by thinking about the priority requirements of V&V exercises execution, as well as cost and time limitations for looking an ideally chosen V&V exercises. The proposed economy and time execution metric CET was utilized as the goal capability.

These new ideal V&V exercises arranging strategy can accomplish expected unwavering quality improvement adequacy with the most un-financial and time utilizations. At last, the contextual investigation of the DFMEA report of a diesel motor power age framework delineated the proposed text mining techniques and the proposed V&V enhancement model. Moreover, these three bits of unwavering quality improvement data can be additionally applied to the V&V interaction to actually recognize and moderate plan gambles.in the principal stage to work out the CHs with the most extreme trust values for immediate, backhanded, and late trust. In the subsequent stage, the CHs with the most extreme trust values for immediate, aberrant, and ongoing trust are registered. The discovery of meddled hubs is subject to the limit esteem that has been set. The CHs are responsible for steering information bundles to the channel, which should go through various bounces on their way there. In MANET, then again, the most encouraging contender for cutting edge directing is distinguished through the utilization of the Microscopic organisms for Maturing Streamlining Calculation enhancement (BFOA). The proposed approach has a quicker intermingling rate, and it improves capacity, throughput, and course association restrictions.

REFERENCES

[1] D. H. Stamatis, Failure Mode and Effect Analysis: FMEA from Theory to Execution. Milwaukee, WI, USA: Quality Press, 2003, pp. 80–81, 2003.

[2] N. Belu, D. C. Anghel, and N. Rachieru, "Application of fuzzy logic in design failure mode and effects analysis," Appl. Mechanics Mater., vol. 371, pp. 832–836, 2013.

[3] K. H. Chang and T. C. Wen, "A novel efficient approach for DFMEA combining 2-tuple and the OWA operator," Expert Syst. Appl., vol. 37, no. 3, pp. 2362–2370, 2010.

[4] P. G. Maropoulos and D. Ceglarek, "Design verification and validation in product lifecycle," CIRP Ann.—Manuf. Technol., vol. 59, no. 2, pp. 740– 759, 2010.

[5] I. Babuska and J. T. Oden, "Verification and validation in computational engineering and science: Basic concepts," Comput. Methods Appl. Mechanics Eng., vol. 193, no. 36, pp. 4057–4066, 2004.

[6] Q. Pengcheng, M. Ren, and Q. Qiu, "Research of application on DFMEA of diaphragm spring clutch cover assembly," J. Mech. Transmiss., vol. 38, no. 5, pp. 166–170, 2014.

[7] J. Huang, Z. J. Li, and H. C. Liu, "New approach for failure mode and effect analysis using linguistic distribution assessments and TODIM method," Rel. Eng. Syst. Saf., vol. 167, pp. 302–309, 2017.

[8] H. C. Liu, Z. J. Li, W. Y. Song, and Q. Su, "Failure mode and effect analysis using cloud model theory and PROMETHEE method," IEEE Trans. Rel., vol. 66, no. 4, pp. 1058–1072, Dec. 2017.

[9] H. C. Liu, Y. P. Hu, J. J. Wang, and M. Sun, "Failure mode and effects analysis using two-dimensional uncertain linguistic variables and alternative queuing method," IEEE Trans. Rel., vol. 68, no. 2, pp. 554–565, Jun. 2019.

[10] H. C. Liu, L. E. Wang, Z. W. Li, and Y. Hu, "Improving risk evaluation in FMEA with cloud model and hierarchical TOPSIS method," IEEE Trans. Fuzzy Syst., vol. 27, no. 1, pp. 84–95, Jan. 2019.

[11] H. C. Liu, J. X. You, and C. Y. Duan, "An integrated approach for failure mode and effect analysis under interval-valued intuitionistic fuzzy environment," Int. J. Prod. Econ., vol. 207, pp. 163–172, 2019.

[12] L. Wang et al., "A linguistic risk prioritization approach for failure mode and effects analysis: A case study of medical product development," Qual. Rel. Eng. Int., vol. 35, no. 6, pp. 1735–1752.

[13] S. F. Feng and S. C. Fu, "Reducer's design failure mode and effects analysis based on DFMEA," Mech. Engineer, vol. 2016, no. 11, pp. 199–202, 2016.

[14] A. H. Tan, "Text mining: The state of the art and challenges," in Proc. PAKDD Workshop Knowl. Discovery Adv. Databases, 1999, pp. 65–70.

[15] M. A. Hearst, "Untangling text data mining," in Proc. Meeting Assoc. Comput. Linguistics Comput. Linguistics Assoc. Comput. Linguistics, 1999, pp. 3–10.

[16] R. Feldman and I. Dagan, "Knowledge discovery in textual databases (KDT)," in Proc. Int. Conf. Knowl. Discovery Data Mining, 1995, pp. 112–117.

[17] H. P. Luhn, "A business intelligence system," IBM J. Res. Develop., vol. 2, no. 4, pp. 314–319, 2010.

[18] A. Hotho, A. Nürnberger, and G. Paass, "A brief survey of text mining," LDV Forum—GLDV J. Comput. Linguistics Lang. Technol., vol. 20, pp. 19–62, 2005.

[19] Q. Jian et al., "Text mining technique and application of lifecycle condition assessment for circuit breaker," Autom. Elect. Power Syst., vol. 40, no. 6, pp. 107–112, 2016.

[20] F. Wang, T. Xu, T. Tang, M. Zhou, and H. Wang, "Bilevel feature extraction-based text mining for fault diagnosis of railway systems," IEEE Trans. Intell. Transp. Syst., vol. 18, no. 1, pp. 49–58, Jan. 2017.

[21] Z. Yang and X. U. Tian-Hua, "Text mining based fault diagnosis for vehicle on-board equipment of high speed railway signal system," J. China Railway Soc., vol. 37, no. 8, pp. 53–59, 2015.

[22] O. P. Damani, "Improving pointwise mutual information (PMI) by incorporating significant co-occurrence," in Proc. 7th Conf. Comput. Natural Lang. Learn., Assoc. Comput. Linguistics, 2013, pp. 20–28.

[23] W. Jin, Z. J. Li, L. S. Wei, and Z. Han, "The improvements of BP neural network learning algorithm," in Proc. Int. Conf. Signal Process., 2002, vol. 3, pp. 1647–1649.

[24] J. Kukulies and R. Schmitt, "Stabilizing production ramp-up by modeling uncertainty for product design verification using Dempster-Shafer theory," CIRP J. Manuf. Sci. Technol., vol. 23, pp. 187–196, 2018.

[25] A. Chahin and K. Paetzold, "Planning validation & verification steps according to the dependency of requirements and product architecture," in Proc. IEEE Int. Conf. Eng., Technol. Innov., 2018, pp. 1–6.

[26] M.Mobin and Z. Li, "An integrated approach to plan the design verification and validation activities for the new product reliability improvement," in Proc. Annu. Rel. Maintainability Symp., 2018, pp. 1–7.

[27] H. Ahmed and A. Chateauneuf, "Optimal number of tests to achieve and validate product reliability," Rel. Eng. Syst. Saf., vol. 131, pp. 242–250, 2014.

[28] M. Mitchell, An Introduction to Genetic Algorithms, vol. 3. Cambridge, MA, USA: MIT Press, 1996, pp. 63–65.

[29] I. H. Witten and D. Milne, "An effective, low-cost measure of semantic relatedness obtained from Wikipedia links," in Proc. AAAI Workshop Wikipedia Artif. Intell., Evolv. Syn., Assoc. Advance. Artif. Intell., 2008, pp. 25–30.

[30] E. Agirre et al., "A study on similarity and relatedness using distributional and WordNet-based approaches," in Proc. Human Lang. Technol., Annu. Conf. North Amer., 2009, pp. 19–27.

[31] P. Hanks and P. Hanks, "Word association norms, mutual information, and lexicography," in Proc. Meeting Assoc. Comput. Linguistics Assoc. Comput. Linguistics, 1989, pp. 76–83.

[32] T. Dunning, "Accurate methods for the statistics of surprise and coincidence," Comput. Linguistics, vol. 19, no. 1, pp. 61–74, 1993.

[33] L. R. Dice, "Measures of the amount of ecologic association between species," Ecology, vol. 26, no. 3, pp. 297–302, 1945.

[34] D. Chaudhari, O. P. Damani, and S. Laxman, "Lexical co-occurrence, statistical significance, and word association," in Proc. Conf. Empirical Methods Nat. Lang. Process., Assoc. Comput. Linguistics., 2011, pp. 1058– 1068.

[35] J. Read, "Recognising affect in text using pointwise-mutual information," M.S. thesis, Univ. Sussex, Brighton, U.K., pp. 1–59, 2004.