Original Article

Bottleneck Bandwidth And Round-Trip Propagation Time Algorithm Using TFRC Protocol By Artificial Intelligence Algorithm

Ehab Husam Husni Al Shiekh Saleh[1]*, Mohd Fadzil Bin Abd Kadir[2], Yousef Abubaker El-Ebiary[3]

*[1]Ph.D., Faculty of Informatics and Computing, UniSZA, Malaysia, Email: si2764@putra.unisza.edu.my.
[2]Assoc. Prof. Dr., Faculty of Informatics and Computing, UniSZA, Malaysia. Email: fadzil@unisza.edu.my
[3]Assoc. Prof. Ts. Dr. Faculty of Informatics and Computing, UniSZA, Malaysia, Email: yousefelebiary@unisza.edu.my

***Corresponding Author:** Ehab Husam Husni Al Shiekh Saleh

*[1]Ph.D., Faculty of Informatics and Computing, UniSZA, Malaysia, Email: si2764@putra.unisza.edu.my.
Doi: 10.47750/pnr.2022.13. S05.133

Abstract

E-government services will play an outstanding role in the next generation of the internet. With growing real-time requirements, internet generation has to offer Quality of Service (QoS) for various types of real-time streaming services. When the bandwidth required exceeds the to be had community resources, community paths can get congested, which leads to a postponement in packet transport and packet loss. This situation leads to the design of new techniques for congestion avoidance and control. One of the popular and suitable congestion management mechanisms which are useful in transmitting multimedia applications in the transport layer is TCP Friendly Rate Control Protocol (TFRC). The fact that bridging the existing e-government security service gap between developed and developing countries. In addition, revealed that system security is one of the major barriers that prevent citizens from adopting E-Government services. Therefore, the network reliable and secure communication channel among government agencies and the entire system, and the Gap related to system quality were found to the security issues among the strongest barriers to hindering E-Government performance. The aim of this study is to examine some of the emerging issues surrounding the Security detection of E-Government Systems in Jordan. Furthermore, the main objective of this research enhances the speed up of training the TFRC protocol through the receiver to group losses and marks that occurred during the same round-trip time. In this paper, we increase stop-to-stop probing strategies which could degree bottleneck bandwidth alongside arbitrary, Accurate measurement of network bandwidth is crucial for network management applications as well as flexible Internet applications and protocols which actively manage and dynamically adapt to changing utilization of network resources. The constructed dataset physically resides in the (dataset) file stored on the data computer, but the configuration files for the dataset reside within a directory for software programs. A software program contains a set of configuration files that construct a dataset (including its extended dimensions) for a specific analysis purpose. It's not easily possible with standard testing approaches such as JUnit, because a node relies on the KNIME Core framework that handles tasks such as execution and data handling. Therefore, a node must be tested within a running KNIME instance.

Keywords: Bottleneck Bandwidth, Round-Trip, Propagation Time Algorithm, TFRC Protocol, Artificial Intelligence Algorithm

I. INTRODUCTION

Information and communication technology (ICT) have transformed the ways we produce and consume. In particular, the widespread use of smart devices has enabled practicing a wide variety of "sharing economy" activities among people, both locally and globally. Digital platforms provide a more rapid (accessed through digital devices), low cost (no/low intermediary costs), and creative (innovative forms of offering services) way for practicing the sharing economy and sharing resources. The basic idea behind the sharing economy is to promote the utilization of available and underused resources, such as transportation means, accommodation, or consumables. The economic activities necessary for providing these goods have – over their whole life cycle, from "cradle to grave" – an impact on the use of natural resources, since economic systems and the environment are closely interrelated (Pouri & Hilty, 2018). The increasing trend in using natural resources already surpassed sustainable levels and the disruption of environmental systems is stated to be one of the crucial consequences of increasing resource use (Pouri & Hilty, 2018). As a subsequent effect, environmental deterioration affects economies and economic growth as increasing use of natural resources may end up with higher resource prices and damaged environmental systems (Pouri & Hilty, 2018).

The advances in Information and Communication Technology (ICT) have made many digital offerings possible. The offerings are frequently mentioned with the prefix "e", for instance e-Commerce for digital trade offerings, e-Banking for digital banking offerings, e-Learning for distance gaining knowledge of offerings, and e-Government for digital authority's offerings. E-Government refers to the usage of new (ICTs) with the aid of using governments as applied to the total variety of authority's tasks, in particular, the networking ability supplied with the aid of using the Internet and associated technology have the ability to convert the structures and operation of authorities. additionally, currently is society facing the concept of informatization. The informatization process means the implementation of information and communication technologies in all areas of citizens' everyday life with the aim of quality improvement. Therefore, is the

society informatization one of the main aims of Manifesto of the Government. The Internet has become a driving force of the informatization. The information and communications technologies has started to be used for communication and services provision in public administration due to the Internet. The informatization brings transparency as well as simplification of the information retrieval and creation, which leads to more efficient communication and the living standards improvement. In practice the government seeks the expansion of the broadband Internet, the public administration services electronation and the digital content quality (Katarina Gasovaa, 2017).

E-authorities offerings attention to four primary customers: Citizens, Business Community, Government Employees, and Government Agencies. E-authority's objectives to make interplay with citizens, businesses authorities' employees authorities' agencies, and other governments extra convenient, friendly, transparent, cheaper and effective. Information and communication technologies (ICTs) are playing an increasingly vital role in the daily lives of people, revolutionizing work and leisure and changing the rules of doing business. In the realm of government, ICT applications are promising to enhance the delivery of public goods and services to citizens not only by improving the process and management of government, but also by redefining the traditional concepts of citizenship and democracy. The ICTs' effect on societies are both far-reaching and uneven. On the one hand, ICT is fueling the transition from industrial-based economies to knowledge-based societies. On the other hand, ICT still has little or no impact in the lives of people in many countries. This wide disparity in the impact of ICT around the world today underscores the uneven progress of economic development. It also highlights the critical role of government in the information age. The goal of this article is to provide a brief overview of E-government studies and their evaluation, to clarify the major issues, which can make E-government to be more effective, transparent and responsive. (Phonepaseuth Solinthone, 2016). The Working Group on E-government withinside the growing global has diagnosed 5 wide classes of goals usually pursued for E-government. E-government is a method to perform those broader social goals, goals that pass past the mere performance of government procedures to that of standard reform and development through.

1. Creating a higher enterprise environment.
2. Customers online, now no longer in line.
3. Strengthening true governance and broadening public participation.
4. Improving the productiveness and performance of government agencies.
5. Improving the high-satisfactory of lifestyles for deprived communities.

The goals are not indexed in any unique order of importance, as every need to decide its priorities in E-government Business model gives a description of the relevant services, processes and activities of the public administration institutions, characterizes how are information, products and services, that create added value for society, created and controlled. The model considers various tools (procedural, strategic, complying with the society requirements), ensuring the creation of sustainable added value for society. ICTI e-Government Business Model consists of four separate models: Information, Communication, Transaction and Integration model (Katarina Gasovaa, 2017).

II.BACKGROUND AND SIGNIFICANCE OF THE STUDY

Information communication technology driven projects often need to be aligned with innovations and new technologies and the changing nature of technology results in the constant upgrade and update of the electronic government infrastructure, creating an extra financial burden for governments. Similarly, when a government extends its department or makes any change in governance, it needs to modify or build a new infrastructure to accommodate those changes that demand significant amount government resources. Therefore, governments throughout the world are developing strategies to migrate to cloud-based e-government to reduce spending on technology infrastructure. Besides the cost factors, upgrading the conventional e-government system requires a significant amount of time—Microsoft UK government industry manager, Richard Shipton says, "Traditionally you might be looking at a six month or a year's project to buy and install extra storage. Now you can do it just by going to a web page and using your government procurement card." According to Gartner Inc. (Stamford, CT, USA) - the world's leading information technology research and advisory company—by 2018, at least 30 percent of service-centric companies will have moved the majority of their Enterprise Resource Planning (ERP) applications to the cloud in order to address the growing financial challenges requiring the cutting of the costs of ICT infrastructure. (Chen, 2017) Zhang and Chen have discussed the impact of shrinking budget in e-government projects and government initiatives to shift from traditional to cloud based e-government. While electronic government projects are facing a number of challenges, cloud computing is considered as a future solution for addressing those challenges. Cloud computing has opened new channels in which governments can deploy electronic government projects and creates new business opportunities while improving performance and cost reduction efficiently for both business and government. the researchers suggest that the integration of the cloud computing in e-government could solve a number of problems including data duplication, low resource utilization rate, repetitive infrastructure construction and information isolated island. Besides this, governments could be benefited from overall cost reduction, distributed data storage, scalability, accountability, modifiability and security management by using cloud computing. Traditional e-governments are not scalable and cost a lot to change their capacity. A typical example of the traditional e-government system failure because of the lack of scalability is Transport for London's (TFL) real-time train tracking system failure in 2010. The app became so popular that the TFL's servers struggled to cope with the sudden increase in demand. To address the problem TFL moved the application from its server to the Microsoft Azure Cloud for example to transfer data over public network infrastructure. The current system is comfortably handling about 2.3 million hits it receives each day. Michael Gilbert, transport of London (TFL)'s chief technology officer accepts that if they had

to run the application on their own servers it would have financially prohibiting as it would have cost them a huge amount to build a new infrastructure inside their data centers (Pusp Raj Joshi, 2017).

E-Government is the use of information and communication technologies in organizations to provide user services, improve job efficiency, and elevate democratic values; as well as a regulatory framework that simplifies information-intensive initiatives and enhances the knowledge society. An e-Government system provides a number of advantages over the conventional or manual system.

Universities use E-Government as a program for efficient, transparent, and timely delivery of services to all the Students. The main purpose of E-Government is to fetch transparency and efficiency in the activities of universities. This push for transparency and efficiency derived from the demand of the ever-increasing ambition of the information in the world.

E-government can be defined as the use of ICT in the public sector to improve operations and the delivery of services and is directly linked to the term e-governance and the concept of good governance. UNESCO (2010) defines e-governance as follows: the public sector's use of information and communication technologies with the aim of improving information and service delivery, encouraging citizen participation in the decision-making process and making government more accountable, transparent and effective (Kristiansand, 2017).

The provision of enhanced public services to citizens and the general public, improved interaction between public sector agencies and citizens, and the engagement of citizens in the governance process of the state has been a deeper concern for governments. Achieving these ideas/goals by the government can best be undertaken under the strong inclusion of ICT in the public administration of government operations. The introduction of Information and Communication Technologies (ICTs) into the public administration of government business and its public sector agencies is known as e-government. E-government is considered the use of electronic devices, information, and communication technologies to provide enhanced public services to citizens, businesses, and the general public (Gomes & Laureano, 2018). It is also defined as the delivery of government public services which has the capacity to increase the citizens' access to government, reduce government bureaucracy, increase citizen participation in decision making and importantly enhance public sector agencies' responsiveness to the needs of citizens (Mensah, 2018).

In the early days, E-Government was not deeply concerned with the adverse effects that could arise from the system because it had great significance for the convenience of the public and the efficiency of public affairs, To understand the Jordanian E-Government model and survey it within the framework of this Socio-Technical model. To reduce the probability of the failures of E-Government projects, due to different factors such as resistance to change from within the enterprise, technical barriers, and lack of training (ICT).

The program is confrontation internal and external challenges, which include limited treasury, speedy development in technological and criterion software, public accessibility to the Internet, and regard of privacy and security (Omer Gibreel, 2017).

The current study work uses the heuristic method to identify any abnormal activity that the ordinary activity. The claim that the BBR algorithm improves throughput and reduces latency compared with NEW RENO. However, the BBR has problems in specific situations (Mühlethaler, 2018).

The BBR flows to obtain a lower share of bandwidth when computing with loss-based through a bottleneck with large Bandwidth*Delay Product (BDPs) buffer, and unexpected package losses (Mühlethaler, 2018).

The Bandwidth*Delay Product, or BDP for short determines the amount of data that can be in transit in the network. It is the product of the available bandwidth and the latency, or RTT. BDP is a very important concept in a Window based protocol such as TCP.

In DCCP, every packet including pure Acknowledgment occupies sequence space, and uses a new sequence number.
The choice made via congestion control IDs (CCID) that name standardization control mechanisms. In the congestion control framework, DCCP the application might prefer TFRC congestion control in DCCPs (CCID3) uses a different approach the sender use and depend on sending rate and receiver send a feedback report on each round-trip time.

If any packet loss means that, no feedback report from the receiver the direct sender halves its rate. The Datagram Congestion Control Protocol (DCCP) and Stream Control Transmission Protocol (SCTP) is a computer networking communications protocol in the transport layer of the Internet Protocol Suite protocols send their packets in bursts. The buffer of the intermediate router has overflowed, and many packets are dropped (Rashmi Rajput, 2015).

On the other hand, the protocol with the smallest percentage of packet loss is the User datagram Protocol (UDP) protocol and the higher loss is again the SCTP and the DCCP and with the worst performance of protocol efficiency (Rashmi Rajput, 2015).

This study fills the gap by Comparison with the performance of the developed in this study and the performance of those in previous shows that the algorithm created in the present study submit training more efficiently than previous algorithms:

1. Enhancing the accuracy rate of improved TFRC's slow start algorithm.
2. Increase the amount of useful data delivered per-time unit through the TFRC slow start algorithm.
3. Reducing the Training time of the TFRC slow start algorithm to allow the receiver to group losses and marks that occurred during the same round-trip time.

III. PROBLEM STATEMENT

The current study's main area is "A framework for detecting the Security Performance of E-Government Systems" There are three reasons for focusing on this topic. First, Given the fact that bridging the existing e-government security service gap between developed and developing countries, the Jordanian rank among 2014 to 2018 indicated retreated (19) degree (NATIONS, 2018). In addition, revealed that system security is one of the major barriers that prevent Jordanian citizens from adopting E-Government services (Al-rawahna, 2018). Therefore, the network reliable and secure communication channel among Jordan government agencies and the entire system, and the Gap related to system quality were found the security issues among the strongest barriers to hinder E-Government performance (Al-rawahna, 2018).

Second, critical information assets and/or the underlying infrastructure are exposed to more and in some cases to security risks and threats. Security threats pose many security challenges to organizations and e-government services. This is vital to achieving high protection against action that compromises the confidentiality, integrity, and availability of computer system Intrusion Detection systems (IDS). Can be broadly categorized into two groups: signature-based intrusion detection system (SIDS), and Anomaly-based detection system (AIDS) (Ansam Khraisat ,. I., 2019). An (AIDS) method can be categorized into three main groups static-based, knowledge-based, and machine learning-based lack of a taxonomy for an anomaly-based intrusion detection system, we have identified five sub-class on their features: static-based, pattern-based, rule-based, state-based, and heuristic-based.

The evolution of malicious software (malware) poses a critical challenge to the design of intrusion detection systems (IDS). Malicious attacks have become more sophisticated and the foremost challenge is to identify unknown and obfuscated malware, as the malware authors use different evasion techniques for information concealing to prevent detection by an IDS. In addition, there has been an increase in security threats such as zero-day attacks designed to target internet users. Therefore, computer security has become essential as the use of information technology has become part of our daily lives. As a result, various countries such as Australia and the US have been significantly impacted by the zero-day attacks. According to the 2017 Symantec Internet Security Threat Report, more than three billion zero-day attacks were reported in 2016, and the volume and intensity of the zero-day attacks were substantially greater than previously (Symantec, 2017). As highlighted in the Data Breach Statistics in 2017, approximately nine billion data records were lost or stolen by hackers since 2013 (Breach Level Index, 2017). A Symantec report found that the number of security breach incidents is on the rise. In the past, cybercriminals primarily focused on bank customers, robbing bank accounts, or stealing credit cards (Symantec, 2017). However, the new generation of malware has become more ambitious and is targeting the banks themselves, sometimes trying to take millions of dollars in one attack (Symantec, 2017). For that reason, the detection of zero-day attacks has become the highest priority.

High-profile incidents of cybercrime have demonstrated the ease with which cyber threats can spread internationally, as a simple compromise can disrupt a business' essential services or facilities. There are a large number of cybercriminals around the world motivated to steal information, illegitimately receive revenues, and find new targets. Malware is intentionally created to compromise computer systems and take advantage of any weakness in intrusion detection systems. In 2017, the Australian Cyber Security Centre (ACSC) critically examined the different levels of sophistication employed by the attackers (Australian, 2017). So, there is a need to develop an efficient IDS to detect novel, sophisticated malware. The aim of an IDS is to identify different kinds of malware as early as possible, which cannot be achieved by a traditional firewall. With the increasing volume of computer malware, the development of improved IDSs has become extremely important.

In the last few decades, machine learning has been used to improve intrusion detection, and currently, there is a need for an up-to-date, thorough taxonomy and survey of this recent work. There are a large number of related studies using either the KDD-Cup 99 or DARPA 1999 dataset to validate the development of IDSs; however, there is no clear answer to the question of which data mining techniques are more effective. Secondly, the time taken for building IDS is not considered in the evaluation of some IDSs techniques, despite being a critical factor for the effectiveness of 'online' IDSs.
there are studies that provide an up-to-date taxonomy, together with a review of the significant research works on IDSs up to the present time; and classification of the proposed systems according to the taxonomy. It provides a structured and comprehensive overview of the existing IDSs so that a researcher can become quickly familiar with the key aspects of anomaly detection. This paper also provides a survey of data-mining techniques applied to design intrusion detection systems. The signature-based and anomaly-based methods (i.e., SIDS and AIDS) are described, along with several techniques used in each method. The complexity of different AIDS methods and their evaluation techniques are discussed, followed by a set of suggestions identifying the best methods, depending on the nature of the intrusion. Challenges for the current IDSs are also discussed. Compared to previous survey publications (Patel et al., 2013; Liao et al., 2013a), this

paper presents a discussion on IDS dataset problems which are of main concern to the research community in the area of network intrusion detection systems (NIDS). Prior studies such as those (Sadotra & Sharma, 2016; Buczak & Guven, 2016) have not completely reviewed IDSs in terms of the datasets, challenges, and techniques. In this paper, we provide a structured and contemporary, wide-ranging study on intrusion detection systems in terms of techniques and datasets; and also highlight the challenges of the techniques and then make recommendations.

IV. INTRUSION DETECTION SYSTEMS

Intrusion can be defined as any kind of unauthorized activity that causes damage to an information system. This means any attack that could pose a possible threat to the information confidentiality, integrity or availability will be considered an intrusion. For example, activities that would make the computer services unresponsive to legitimate users are considered an intrusion. An IDS is a software or hardware system that identifies malicious actions on computer systems in order to allow for system security to be maintained (Ranjit Panigrahi, 2018). The goal of an IDS is to identify different kinds of malicious network traffic and computer usage, which cannot be identified by a traditional firewall. This is vital to achieving high protection against actions that compromise the availability, integrity, or confidentiality of computer systems. IDS systems can be broadly categorized into two groups: Signature-based Intrusion Detection systems (SIDS) and Anomaly-based Intrusion Detection systems (AIDS).

Signature intrusion detection systems (SIDS) are based on pattern matching techniques to find a known attack; these are also known as Knowledge-based Detection or Misuse Detection (Khraisat A., 2018). In SIDS, matching methods are used to find a previous intrusion. In other words, when an intrusion signature matches with the signature of a previous intrusion that already exists in the signature database, an alarm signal is triggered. For SIDS, the host's logs are inspected to find sequences of commands or actions which have previously been identified as malware. SIDS have also been labeled in the literature as Knowledge-Based Detection or Misuse Detection (Khraisat A., 2018). Figure 5 demonstrates the conceptual working of SIDS approaches. The main idea is to build a database of intrusion signatures and to compare the current set of activities against the existing signatures and raise an alarm if a match is found.

V. RELATED WORK

Electronic government (e-government) or e-Gov is the use of ICT tools and applications, whether it was internet-based or non-internet based to make better interaction through different delivery models and activities between government and citizens (G2C), government and business/commerce (G2B), between government agencies (G2G), or government and Households (G2H), but it may face a number of limitations that affect the way of interaction. Privacy and security of information is a priority issue in dealing with E-government.

1. most e-government applications depend on the Internet to deliver a wide service for citizens, the increased transparency and easier access will be considered as an advantage, on the other hand, it will raise a significant issue risk will be increased because there are vulnerabilities (Rabah, 2012), however, if the vulnerability been known there will be a mechanism to recover it otherwise it will be exploited by attackers.
2. E-government needs to store detailed information about all citizens' profiles; this sensitive information might use by attackers that yield a potential exposure to confidentiality, or even information being modified in an unexpected way to produce lack of integrity (Tamy Guberek, 2018).
3. A problem arises when someone wants to verify and authenticate the owner of information/object and sometimes vice versa in order to access some information in e- government application such as e-voting, e-passports or e-transactions through the e-government portal (Tamy Guberek, 2018).
4. A breach of security may be compromised to yield lack of availability of information to citizen, where majority of e-government projects in developing countries fail (Jessica Vitak, 2018).

E-government in Saudi Arabia: Barriers, Challenges and its Role of Development of e-government is a complicated task both technically and politically. The quality of e-government depends on many factors; critical among these are the government's information policy, the number of users and their educational level, and motivation. Up to now, no country has successfully met all the requirements necessary for an ideal form of e-government. Based on this viewpoint, a customized approach to the development and implementation of e-government is needed to satisfy the prerequisites for its success (Abdullah Basahel, 2017).

During the last decade, research on congestion control algorithms has been quite active and has been essentially focused on congestion control for "best-effort" reliable data traffic. The current version of TCP congestion control is still largely based on the cornerstone paper and its modifications. TCP congestion control architecture assumes that the network is a "black box" that does not supply any explicit feedback to sources. Therefore, it is designed following the end-to-end principle that is one of the major keys to the success of the Internet. In particular, a TCP source follows an additive increase mechanism to grab all available bandwidth and a multiplicative decrease mechanism to drastically decrease the window when congestion is revealed by a timeout or reception of three duplicate acknowledgments (3 packs).

5.1 MEASURING BOTTLENECK BANDWIDTH OF TARGETED PATH SEGMENTS

Accurate dimension of community bandwidth is important for community control programs in addition to bendy Internet programs and protocols which actively manipulate and dynamically adapt to converting usage of community resources.

Extensive paintings have targeted tactics to measuring bandwidth: measuring it hop-through-hop and measuring it stop-to-stop alongside a route. Unfortunately, best-exercise strategies for the previous are inefficient and strategies for the latter are simplest capable of look at bottlenecks seen on the stop-to-stop scope. In this paper, in this paper, we increase stop-to-stop probing strategies which could degree bottleneck bandwidth alongside arbitrary, Accurate measurement of network bandwidth is crucial for network management applications as well as flexible Internet applications and protocols which actively manage and dynamically adapt to changing utilization of network resources.
which could degree bottleneck bandwidth alongside arbitrary, centered sub paths of a route with inside the community, inclusive of sub paths shared through a hard and fast of flows. We examine our method via full-size simulations, then offer a comparative Internet overall performance assessment in opposition to hop-through-hop strategies. We additionally describe some of the programs that we foresee as a status to gain from answers to this problem, starting from community troubleshooting and potential provisioning to optimizing the format of application-degree overlay networks, to optimized reproduction placement.

Measurement of community bandwidth is vital for plenty net programs and protocols, mainly the ones related to the switch of huge documents and people related to the transport of content material with real-time QoS constraints, which includes streaming media. Some precise examples of programs that could leverage correct bandwidth estimation consist of end-gadget multicast and overlay community configuration protocols, content material area and transport peer-to-peer (P2P) networks, community-conscious cache or duplicate placement rules, and waft scheduling and admission manipulate rules at massively accessed content material servers. In addition, correct measurements of community bandwidth are beneficial to community operators involved with issues which includes capacity provisioning, site visitors engineering, community troubleshooting, and verification of provider stage agreements (SLA's).

Bandwidth Measurement: Two unique measures used in give up-to-give up community bandwidth estimation are bottleneck bandwidth, or the most transmission fee that would be executed among hosts on the endpoints of a given direction in the absence of any competing site visitors, and to be had bandwidth, the part of the bottleneck bandwidth alongside a direction that would be received by a given glide at a given immediate in time. Both of those measures are important, and every capture unique applicable residences of the community. Bottleneck bandwidth is a static baseline degree that applies over lengthy time scales (as much as the time-scale at which community paths change), and is unbiased of each the precise site visitors' dynamic at a time immediate. Available bandwidth presents a dynamic degree of the burden on a direction, or extra precisely, the residual capacity of a direction. Additional application-particular records must then be implemented earlier than making significant use of either degree; for example, the fee appropriated by an additional TCP glide is pretty unique than the unused capacity along a direction. While measures of to be had bandwidth are certainly more beneficial for manage or optimization of approaches running at brief time scales, approaches running at longer time scales (e.g. server choice or admission manage) will discover estimates of each measures to be helpful, even as many community control applications (e.g. capacity provisioning) are worried primarily with bottleneck bandwidth. In this paper, we consciousness on measuring bottleneck bandwidth.

5.2 DATASET SETUP

Dataset configuration refers back to the manner of modifying the configuration documents whose parameters offer the guidelines for dataset construction.

The constructed dataset physically resides in the (dataset name) file stored on the data computer, but the configuration files for the dataset reside within a directory for software programs. A software program contains a set of configuration files that construct a dataset (including its extended dimensions) for a specific analysis purpose. In addition, a profile contains the definitions of entities such as Number of Test Cases, Number of Class Label, Number of Coverage, Number of Covered Instruction, Number of Missed Instructions, Number of Total Instructions and, Number of calls that enable analysts to interact with the dataset and obtain information from it.

The dataset configuration files you are editing are referred to as your dataset for programs. A dataset references multiple inherited profiles, which can be any profiles that create and maintain so that can configure the KNIME application to best fit your analysis needs. A dataset also may reference internal profiles that are provided with the KNIME application to form the basis for all of the functionality available in the application.

CNNs are normally utilized in pc imaginative and prescient and visual view analysis; its miles characterized with the aid of using the presence of 1 or extra hidden layers, that could extract the functions discovered in pictures or videos, and a totally connected layer to provide the desired output.

The fundamental additives of convolutional neural networks are the convolutional layer, the activating function, the pooling layer, and the fully linked layer.

Long short-term memory (LSTM) is an artificial recurrent neural network (RNN) architecture used in the field of deep learning. Unlike standard feed forward neural networks, LSTM has feedback connections. It cannot only process single data points (such as images), but also entire sequences of data (such as speech or video). For example, LSTM is applicable

to tasks such as unregimented, connected handwriting recognition, speech recognition and anomaly detection in network traffic or IDSs (intrusion detection systems).

A common LSTM unit is composed of a cell, an input gate, an output gate and a forget gate. The cell remembers values over arbitrary time intervals and the three gates regulate the flow of information into and out of the cell.

LSTM networks are well suited to classifying, processing and making predictions based on time series data, since there can be lags of unknown duration between important events in a time series. LSTMs were developed to deal with the vanishing gradient problem that can be encountered when training traditional RNNs. Relative insensitivity to gap length is an advantage of LSTM over RNNs, hidden Markov models and other sequence learning methods in numerous applications.

The Constructed DBN could be composed of RBMs (Restricted Boltzmann Machines for deep learning), decreased, and better RBM layers. The quantity of seen nodes of decreased RBM is the characteristic quantity and the number of hidden nodes of the better RBM is the to-be had elegance quantity. While the number of hidden nodes inside the decreased RBM layer and the quantity of seen nodes inside the better RBM layer are the identical and identical to a random quantity, e.g. 13. Each hidden node inside the better RBM represents one of the instructions below testing, such that if ”0” is the elegance label related to the input, then the primary node inside the hidden nodes inside the better RBM is 1, and the relaxation of nodes could be of cost 0. E.g., if the output inside the first hidden node is 0.6 and if the elegance label is 0, because of this the predicted output on this node is 1, then there's a blunder of a cost of 0.4. Algorithm 1 indicates the steps of the DBN classifier.

VI. ALGORITHMS CNN PREDICTION

In the convolution layer, a clear-out is applied (additionally referred to as a kernel) that determines the presence of sure functions or styles inside the original image (input), after which it's miles viable to apply numerous filters so as to extract extraordinary functions.

It's not easily possible with standard testing approaches such as JUnit, because a node relies on the KNIME Core framework that handles tasks such as execution and data handling. Therefore, a node must be tested within a running KNIME instance.

Table I: The Test Prediction

Algorithm	Accuracy	Number of classify	Correct	wrong
CNN	82.4%	427	352	75
DBN	83.417%	199	166	33
DNN	87.5%	184	161	23
LSTM	80.562%	427	344	83

VII.CONCLUSION

It's not easily possible with standard testing approaches such as JUnit, because a node relies on the KNIME Core framework that handles tasks such as execution and data handling. Therefore, a node must be tested within a running KNIME instance.

REFERENCES

1. Abdulla K. Al-Ali, K. C. (2017). TFRC-CR: An equation-based transport protocol for cognitive. ELSEVIER, 1-12.
2. Abdullah Basahel, M. Y. (2017). Measuring success of e-government of Saudi Arabia. International Journal of Information Technology, 16-22.
3. Alazab, A. K. (2021). A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. JOUR, Cybersecurity, 2-27.
4. Albandari Mishal Alotaibi, B. F. (2017). Security issues in Protocols of TCP/IP Model at Layers Level. International Journal of Computer Networks and Communications Security, 1-10.
5. Al-rawahna, A. S.-C.-W. (2018). The Barriers of E-Government Success : An Empirical Study from Jordan. Alrawahna2018TheBO, 12-35.
6. Alshehri, M. D. (2016). E-Government Fundamentals. Proceedings of the IADIS International Conference ICT, Society and Human Beings, 35-42.
7. Ansam Khraisat, ,. I. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. Springer Open Access Cybersecurity, 2-20.
8. Ansam Khraisat, A. A. (2021). A critical review of intrusion detection systems in the internet of things. Cybersecurity, 1-27.
9. Arash Molavi Kakhki, S. J. (2017). Taking a Long Look at QUIC, An Approach for Rigorous Evaluation of Rapidly Evolving Transport Protocols. IMC, 290-303.
10. Aslam, N., Xia, K., Ali, A., & Ullah, S. (2017). Adaptive TCP-ICCW Congestion Control Mechanism for QoS in Renewable Wireless Sensor Networks. IEEE, 1-2.
11. Babu, M. M., & Brahmaiah, V. (2017). Performance evaluation of interoperation on TFRC-UDP in wired environment. International Conference on Intelligent Sustainable Systems (ICISS), 7-8.
12. Deshpande, P. S. (2019). HIDS: A host based intrusion detection system for cloud computing environment. International Journal of System Assurance Engineering and Management, 567-576.
13. Eddie Kohler, M. H. (2006). Designing DCCP: Congestion Control Without Reliability. SIGCOMM, 2-12.
14. Effelsberg, M. H. (2000). Equation-Based Congestion Control. Diploma Thesis, 35-104.
15. Floyd, B. W. (2008). The Middle Management Perspective on Strategy Process: Contributions, Synthesis, and Future Research. Journal of Management, 1190-1221.

16. Hrvoje Stancic, T. I. (2017). Government to Business E-Services –Accountability and Trust. Tidsskriftet Arkiv, 8(1). https://doi.org/10.7577/ta.1958, 1-16.
17. Jessica Vitak, Y. L. (2018). Privacy Attitudes and Data Valuation Among Fitness Tracker Users. Transforming Digital Worlds, 2018, Volume 10766, 49-58.
18. Katarina Gasovaa, *. K. (2017). E-Government as a quality improvement tool for citizens' services . International scientific conference on sustainable, modern and safe transport, 225-230.
19. Khraisat A., G. I. (2018). An Anomaly Intrusion Detection System Using C5 Decision Tree Classifier. Springer, Cham, 6-14.
20. Kristiansand, N. (2017). The role telecentres play in providing e-government services in rural areas. http://wileyonlinelibrary.com/journal/isd2, 1-14.
21. Laila Al-Azizi, A. H.-B.-Z. (2018). Exploring the Factors Influencing Employees' Willingness to Use Mobile Applications in Oman: Using UTAUT Model . Journal of e-Government Studies and Best Practices, 1-27.
22. Mensah, I. K. (2018). E-Government Services Adoption: The Important Elements of Trust and Transparency. International Journal of Electronic Government Research (IJEGR) 14(3), 8-20.
23. Michele Polese, S. M. (2019). A Survey on Recent Advances in Transport Layer Protocols. IEEE Communications Surveys & Tutorials, DOI 10.1109/COMST.2019.2932905., 1-26.
24. Moritz Geist, B. J. (2019). Overview of TCP Congestion Control Algorithms. Network Architectures and Services, 11-15.
25. Mühlethaler, P. (2018). Machine Learning for Networking. First International Conference, 5-43.
26. Nalavala Ramanjaneya Reddy, P. C. (2017). Efficient Traffic Engineering Strategies for Improving the Performance of TCP Friendly Rate Control Protocol. Future Computing for Real Time Intelligent Systems, 1-12.
27. NATIONS, U. (2018). UNITED NATIONS E-GOVERNMENT SURVEY 2018. New York: 2018.
28. NEAL CARDWELL, Y. C. (2016). BBR Congestion-Based Congestion Control. acmqueue, 20-53.
29. Omer Gibreel, A. H. (2017). A Holistic Analysis Approach to Social, Technical, and Socio-Technical Aspect of E-Government Development. Sustainability 2017, 9, 2181; doi:10.3390/su9122181, 1-12.
30. Phonepaseuth Solinthone, T. R. (2016). E-GOVERNMENT IMPLEMENTATION. MATEC Web of Conferences, 79.
31. Polese, M. (2019). A Survey on Recent Advances. IEEE Communications Surveys & Tutorials, 1-26.
32. Pouri, M., & Hilty, L. (2018). ICT-Enabled Sharing Economy and Environmental Sustainability - A Resource-Oriented Approach. Zurich Open Repository and Archive, 1-14.
33. Pusp Raj Joshi, S. I. (2017). A Framework for Cloud Based E-Government from the Perspective of Developing Countries. MDPI, 1-26.
34. Ramanjaneya Reddy Nalavala, C. R. (2016). An Enhanced Queue Management Scheme for TFRC Over Wired Networks. International Journal of Intelligent Engineering and Systems, 1-6.
35. Ranjit Panigrahi, S. B. (2018). A detailed analysis of CICIDS2017 dataset for designing Intrusion Detection Systems. International Journal of Engineering & Technology, 479-482.
36. Rao, V. R. (2017). Improving Government to Employee (G2E) Services through Mobile Technology – A Survey. International Journal of Computer Applications (0975 – 8887), 33-45.
37. Rashmi Rajput, G. S. (2015). Comparing Stream Control and Datagram Congestion Control with Traditional Transmission Control Protocol. International Journal of Computer Science and Mobile Computing, 570-577.
38. Samuel Jero, E. H. (2018). Automated Attack Discovery in TCP Congestion Control Using a Model-guided Approach. Network and Distributed Systems Security (NDSS) Symposium , 1-15.
39. Srinivasan, E. M. (2018). A Brief Analysis of Recent ISO Tolerancing Standards and Their Potential Impact on Digitization of Manufacturing. 15th CIRP Conference on Computer Aided Tolerancing – CIRP CAT 2018, Milano, IT, 7-22.
40. Tamy Guberek, A. M. (2018). Keeping a Low Profile? Technology, Risk and Privacy among Undocumented Immigrants. CHI 2018 Best Paper Award, 1-16.
41. Tanjia Chowdhury, M. J. (2019). Performance Evaluation of TCP Vegas over TCP Reno and TCP New Reno over TCP Reno . INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION, 275-282.
42. The top vendors winning in the Data Center & Virtualization space depend on TechTarget to fuel their pipelines. (2021). Retrieved from techtarget: https://www.techtarget.com/
43. Tobias Flach, ,. N. (2013). Reducing Web Latency: the Virtue of Gentle Aggression. SIGCOMM, 159-170.
44. Wheeb, A. H. (2017). Performance Analysis of VoIP in Wireless Networks . IRACST – International Journal of Computer Networks and Wireless Communications, 1-5.
45. Wheeb, A. H. (2018). Performance Evaluation of Transport Protocols for Mobile Ad Hoc Networks. Journal of Engineering and Applied Sciences, 1-6.
46. Wilson, P. (2021). APNIC. Retrieved from APNIC: https://blog.apnic.net/2017/05/09/bbr-new-kid-tcp-block/ World Bank Group. (2018). 8 International Bank for Reconstruction and Development / The World Bank, 5-32. x. (2017). xxxx. xxx, 33-45.
47. Y. Narasimha Reddy, P. V. (2018). A Combined TCP-friendly Rate control with WFQ Approach for Congestion Control for MANET. I. J. Computer Network and Information Security, 2018, 6, 52-59, 52-59.
48. ZAHOOR AHMED ALIZAI, H. T. (2019). Key-Based Cookie-Less Session Management Framework for Application Layer Security. Digital Object Identifier 10.1109/ACCESS.2019.2940331, 1-11.
49. Yousef A.Baker El-Ebiary, Samer Bamansoor, Waheeb Abu-Ulbeh, Wan Mohd Amir, Syarilla Iryani A. Saany, M. Hafiz Yusoff. "Using Interval Manager Mobile Application in Saving Time and Cost" Vol. 68, Editor's Issues, Oct. 2020, pp. 82-85, IJETT, Doi: 10.14445/22315381/CATI1P214. Scopus, ISSN: 2231-5381
50. Yousef A.Baker El-Ebiary, Samer Bamansoor, Waheeb Abu-Ulbeh, Wan Mohd Amir, Syarilla Iryani A. Saany, M. Hafiz Yusoff. "A Prognosis of Chinese E-Governance" Vol. 68, Editor's Issues, Oct. 2020, pp. 86-89, IJETT, doi: 10.14445/22315381/CATI1P215. Scopus, ISSN: 2231-5381
51. Yousef A.Baker El-Ebiary, Waheeb Abu-Ulbeh, Najeeb Abbas Al-Sammarraie, M. Hafiz Yusoff , W. M. Amir Fazamin W. Hamzah, Syarilla Iryani A. Saany. "The Role of ICT in Special Educational Needs – A Case Study of Malaysia" Vol. 68, Editor's Issues, Oct. 2020, pp. 90-93, IJETT, doi: 10.14445/22315381/CATI1P216. Scopus, ISSN: 2231-5381
52. W. M. Amir Fazamin W. Hamzah, Waheeb Abu-Ulbeh, Najeeb Abbas Al-Sammarraie, Yousef A.Baker El-Ebiary, M. Hafiz Yusoff, Syarilla Iryani A. Saany, Azliza Yacob. "The Integration of Learning Management Systems with PLE – a Review Paper" Vol. 68, Editor's Issues, Oct. 2020, pp. 94-96, IJETT, doi: 10.14445/22315381/CATI1P217. Scopus, ISSN: 2231-5381
53. Syarilla Iryani A. Saany, Waheeb Abu-Ulbeh, Najeeb Abbas Al-Sammarraie, Yousef A.Baker El-Ebiary, M. Hafiz Yusoff, W. M. Amir Fazamin W. Hamzah, Yanty Faradillah. "A New E-Learning Technique Using Mobility Environment" Vol. 68, Editor's Issues, Oct. 2020, pp. 97-100, IJETT, doi: 10.14445/22315381/CATI1P218. Scopus, ISSN: 2231-5381
54. Aledinat Lowai Saleh, Syed Abdullah Fadzli, Yousef El-Ebiary. "Arabic Language Documents' Similarity and its Challenges (A Review)" Vol. 68, Editor's Issues, Oct. 2020, pp. 88-96, IJETT, doi: 10.14445/22315381/CATI2P214. Scopus, ISSN: 2231-5381
55. Belal Alifan, Mokhairi Makhtar, Yousef El-Ebiary. "Propose Model for Consumers' Perceptions and Acceptance of e-Health Systems and Services in Jordan" Vol. 68, Editor's Issues, Oct. 2020, pp. 1-10, IJETT, doi: 10.14445/22315381/CATI3P201. Scopus, ISSN: 2231-5381
56. Hazem M Bani Abdoh, Syarilla Iryani A. Saany, Hamid H. Jebur, Yousef El-Ebiary. "The Effect of PESTLE Factors on E-Government Adoption in Jordan: A Conceptual Model" Vol. 68, Editor's Issues, Oct. 2020, pp. 19-23, IJETT, doi: 10.14445/22315381/CATI3P203. Scopus, ISSN: 2231-5381

57. Y. A. B. El-Ebiary, N. A. Al-Sammarraie, Y. Al Moaiad and M. M. S. Alzubi, "The impact of Management Information System in educational organizations processes," 2016 IEEE Conference on e-Learning, e-Management and e-Services (IC3e), 2016, pp. 166-169, doi: 10.1109/IC3e.2016.8009060.