The Impact of Intrusion Detection Systems upon Healthcare Environments: A Research Review

Tasfia Bari
Eastern Michigan University
College of Technology
tbari@emich.edu

Munther Abualkibash
Eastern Michigan University
College of Technology
School of Information Security and Applied Computing
mabualki@emich.edu

Abstract

As healthcare systems throughout the globe face an influx of new information exchange due from a variety of different network transferences, the caution that arises from utilizing such technologies can distinguish which healthcare systems are equipped to handle potential cybersecurity attacks and breaches in comparison to those who are not. This study seeks to review research that is currently available pertaining to the impact of Intrusion Detection Systems (IDS) upon different healthcare systems and the networks in which they exchange patient health information (PHI) and electronic health records (EHR) pertaining to their hospital and clinical experiences. The growing concern for patient information assurance is brought forth and substantiated as more and more healthcare providers switch to digital platforms for storing patient information and their staff exchange information for efficient healthcare practices. Whilst different researchers approach IDS from different perspectives in regard to healthcare, the outcome suggests neural network approaches such as autoencoding and fuzzy logic can help dispel potential breaches and network security threats from intercepting PHI as it is shared.

Keywords
Intrusion, Detection, System, Network, Healthcare

1. Introduction

With the global expansion of technology across various settings, groups, individuals and apparatuses the integration of technology has deeply been embedded within society. Technology has become so well encompassed within our world that we depend upon it under the most dire and unforeseen circumstances. Its diverse input has allowed society to excel in manners that were once unheard of. Nevertheless, with such progress and benefit brought forth by technology, there are stipulations and subsequent consequences that also develop as a result. Such threats include and are not limited to cybersecurity threats such as malware, phishing and distributed denial of service attacks (DDOS) (Richterich, 2018). Over the past decade alone, the rise of cybersecurity threats has been observed on numerous occasions (Ghadamyari & Samet, 2020).

Such occurrences have been observed on large and small scales impacting groups of people who will either carry the outcomes of such threats and or breaches with them for decades or may hardly notice its impact upon their livelihood (Mookherjee, 2011). Often times the underlying cause of cybersecurity threats are brought forth when key components of a network are under attack. Such components include Intrusion Detection Systems (IDS) which provide a framework of review of a network's unsolicited or malicious activity (Skrobanek, 2011). The most integral aspect and role of intrusion detection systems include monitoring and surveillance of a network's processes through a management system (Daniels & Bhatia, 2020). Its presence can be anticipated in any wireless technology which communicates with similar structured systems (Ghadamyari & Samet, 2020). In fast-paced environments such as healthcare, the integration of technology has followed the steady demand of increased access to care throughout society (Graetz, 2014).

With the digitalization of many key societal establishments such as education and e-learning or finances and electronic banking and digital transactions the call for healthcare settings such as clinics and hospitals to digitize their health records has gained growing momentum in recent decades (Gupta & Srinivasagopalan, 2020). As the consumer experience has become heavily vitalized and synonymous with quality healthcare and treatment, efficiency has been a key factor in determining how satisfied patients are with the resources given to them by their healthcare provider. The digitization of health records does not solely benefit the patient. Its presence can also further streamline their healthcare provider's job, regardless of their position of the exact role they play within an overall team (Mookherjee, 2011). This is key to note as the streamlining of one position within a healthcare atmosphere can allow a relay of information which can expedite the patient treatment process. With this notion, the establishment of Electronic Health Records (EHR) has become revolutionary in the daily practices of many healthcare professionals throughout the world Ghadamyari & Samet, 2020).

With the usage and implementation of tools such as electronic health records, healthcare practitioners within the United States have had to abide by protocols which allow them to ensure that the tools they utilize to collect and transfer EHR is done in accordance to the Health Insurance Portability and Accountability Act of 1996 (Bace & Mell, 2001). This is especially pertinent to the transfer of EHR which is conducted by various healthcare professionals on an individual patient's overall healthcare provider team (Gadamyari & Samet, 2020). The specific exchange of healthcare information regarding a patient's history, data and treatment presented as EHR is done through health information exchange (HIE) (Graetz, 2014). With such exchange, providers must be able to assure that their patient's information and identity is secure by HIPAA guidelines therefore they use Healthcare Information Systems (HCIS) such as EPIC or Cerner which are widely known to support and streamline such information in a secure and compliant manner (Schneider, 2014).

With such protocols in place, especially in regard to such highly personal, secure and private information of many individuals it is important to assure that quality HCIS provide strong networks and IDS to support the overall exchange of healthcare data. While EHRs are becoming increasingly mandated and utilized throughout the world, a patient's healthcare experience becomes smaller and therefore more readily accessible to them and their different healthcare providers (Klein, 2012). This packaging of information can be both beneficial but also pose risk to their personal security as the same conveniences brought forth by such innovative efforts can also be in jeopardy if accessed by the wrong party (Pietro & Mancini, 2011). Therefore, it is key to understand the extent to which IDS can provide network security to healthcare providers and allow their services and exchange of valuable patient information to be conducted in a secure manner.

With the processes of healthcare becoming increasingly streamlined throughout American society, healthcare professionals are now tasked with becoming equipped with the skills needed to properly and efficiently utilize these digital resources to the best of their abilities and to the benefit of their patient's care. While the efficiency of healthcare providers is streamlined given such digital solutions, patient care and their personal healthcare information is also in jeopardy as unforeseen threats may be provide consequential outcomes impacting both healthcare providers and patients on a circumstantial level (Richterich, 2018). This is observable in situations which feature data breaches in healthcare systems.

As healthcare systems range in terms of size and variety, the level to which a breach of information. Such breaches can depend upon the size and capacity of the healthcare systems and the different formats of EHR which they utilize (Schneider, 2014). Larger healthcare conglomerates which are more prominent in larger areas of the United States may feature healthcare systems which feature cloud-based apparatuses that provides a cloud-based network that allows different providers to share information regarding patient updates, patient history and their on-going profiles with other members of their healthcare team (Richterich, 2018). Whereas in contrast, smaller healthcare conglomerates such as clinics and consulting offices may utilize similar EHR systems, which provide dated features to contain PHI and limited features for healthcare provider access. Going between these different systems in order to communicate patient data may result in consequential outcomes such as patient information data loss and data breaches.

With such discrepancies amongst healthcare providers, and systems to which they utilize and process patient information it is imperative that the networks they utilize and provide a secure mainframe for safe transactions containing vital patient information (Kim et al, 2018). Thus, healthcare providers must take on an additional task of ensuring that intrusion detection systems are faceted and equipped with providing that additional security in ensuring that patient information is kept private and secured within these digital transactions between different healthcare providers. With the argument for healthcare intrusion detection systems benefitting HIPAA security (Barney, 2015).

Lack of the increasingly outdated act may benefit from incorporating further details pertaining to IDS within its bylines. Therefore, with this notion, this review seeks to observe the impact on how the presence of IDS provides additional and necessary security measures towards securing patient healthcare information.

2. Related work

Researchers sought to observe the impact of IDS upon mobile healthcare information systems as a protection mechanism against digital attacks upon exchange of data. Seven different IDS were observed and compared against one another in terms of their ability to protect patient health information (PHI) and healthcare data from outside intruders attempting to reach the system. A novel approach is proposed by the authors to utilize a recurrent neural network (RNN). Through a third-party dataset, researchers concluded that their novel approach increased detection rates and subsequently decreased false alarm rates through methods of neural networking (Al-Dhafian et al, 2017).

In a similar study, researchers observed the challenges of how healthcare data found within commonly used applications can be compromised due to breaches and lack of patient information upkeep. They utilize a system titled the Wireless Body Area Network (WBAN) which allowed them to utilize remote techniques of monitoring patient health information (PHI) through their electronic health records (EHR). To ensure that PHI is being maintained in a secure manner. This was done through a research review technique comparing different articles which observed similar approaches in topic (Al-Janabi et al, 2016).

Another article described how the inevitability of intrusion detection can at least be minimized in the occurrence of computer-based attacks. The author mentions that two different intrusion detection methods such as those which are anomaly-based and namely-misuse approaches towards a CIIDS can create an alerting algorithm which can inform users of such oncoming attacks. The article goes on to compare and contrast different articles observed the difference between the two. The outcomes of this review suggested that varying techniques such as fuzzy-logic, soft-computing and other approaches can be utilized to reduce the amount of false-alarms observed in IDS while bringing forth the necessary attention needed in actual detection needs (Elshoush & Osman, 2010)

A different study observed the impact of online sequence extreme learning machines (OS-ELM) are IDS in regard to interfering and understanding cybersecurity attacks upon advanced metering infrastructures (AMI) in what is considered to be “Smart Grid” technologies. OS-ELM approaches were conducted through a simulation apparatus which suggested that comparative algorithms found that the IDS method in observing such attacks were more beneficial in comparison to similar, yet different, approaches on AMI. The outcomes suggested that OS-ELM had the most accuracy in comparison to other learning algorithms upon the presence of IDS. It had 97% accuracy, whereas its closest competing learning algorithm (RBF) had an accuracy of 96% (Li & Jing, 2017).

In an article observing the impact of IDS upon different neural network systems which employ fuzzy logic-based technologies. Researchers sought to distinguish the impact of IDS which utilized genetic fuzzy logic practices on pairwise learning. The study, found that the benefits of using neural networking in IDS to better understand such practices brings forth better identification of which aspects of information transfer should heed warning, given the type of information that is being brought forth, versus everyday patient information that is being transferred within the healthcare facilities (Elhag et al, 2014).

Hady et al, 2020 reviews the impact of IDS upon healthcare systems in regard to medical and network data through a comparison approach. The article mentions general issues in regard to healthcare privacy and security concerns within different medical settings including the compromise of patient health information (PHI) and other forms of identifiable information on their behalf. The authors built an EHMS monitoring system established within patient’s beds which would monitor network flow metrics throughout their stay. The data was then automatically submitted to a network server for additional review which would act as a third-party reviewer to determine any potential cybersecurity attacks on patient information going out. Overall, the outcome of this study suggested a notable increase in interfering in cybersecurity attacks ranging from 7-25% on a case-by-case basis. Thus, suggesting a beneficial impact due to the presence of third party, EHMS security systems.

According to (Chen et al, 2016), the authors of this study describe how the impact of society’s ongoing increased dependencies upon portable technology can benefit them from an information security standpoint. Therefore, the authors observed the impact of cloud-based medical data exchanges using wearable devices by medical device users and patients. The cloud-based data is analyzed through two models of approach. The first model was one which transmitted cloud-based data through trustable devices while the other allowed patients with the same prognosis and diagnosis to share and or communicate about their experiences through a different cloud-based platform. The authors took information from these two different models to distinguish them into three aspects based on categories pertaining to the different types of information they can be considered to be. This allows them to develop a newfound approach towards the issue by establishing a different technique of IDS which allows them to combine different cloudlet apparatuses and exchange information within them to provide a preemptive approach towards breaches.

Another study observes the impact of connected healthcare systems (CHS) on patient health information (PHI) exchange amongst different healthcare providers across medical technology platforms. This study primarily focuses upon the technology utilized to monitor patient’s physical condition development. The cybersecurity related threats

that were focused upon in this study's observations included threats both from within the system as well as external threats coming in through data exchanges as well as malware. The outcome of this study denotes the different types of potential security threats which can be aided through the presence of newfound IDS methods which the authors propose as a "Stacked autoencoder" approach towards protecting PHI. The authors claim that moving forward, IDS should become more efficient if they reduce the workload of the IDS and utilize methods which best utilize their resources as they did with their stacked approach (He et al, 2019).

Researchers also observe the differences amongst different approaches towards IDS. Some of which featured differing methods of anomaly-based intrusion detection systems in comparison to those IDS without anomaly-based techniques. Additionally, they sought to observe other deficits in utilizing IDS mechanisms. Amongst the challenges the authors observed, included those which included limitations in machine learning as well as the algorithm utilized by many systems which featured principle component analysis. The authors found that compared to IDS mechanisms which featured a neural network technique, those which featured machine learning techniques for overcoming issues in IDS were more versatile in comparison to those which observed machine-learning techniques (Vinchurkar & Reshamwala, 2012).

Researchers observed the impact of specific algorithms in different domains. Amongst the domains observed in this study, researchers noted the difference in impact between big data, uncertain data, time series data and high dimensional data. Therefore, based on this, the authors proposed two competing algorithms. One of which was a distance-based outlier algorithm in contrast to a cluster-based outlier algorithm. The outcome of this study suggested that cluster-based algorithms provided more accurate results in navigating a variety of healthcare domains in comparison to the distance-based approach (Christy et al, 2015). It was further noted that connected healthcare systems which featured remote monitorization to observe incoming threats such as malware and data temperament. Amongst the variety of different vulnerabilities observed within the connected healthcare system (CHS), researchers found in their experimental evaluation that through offline analysis, a stacked autoencoder approach would allow for more efficient intrusion detection (Daojing et al, 2019).

3. Usage of Datasets

While different authors mentioned throughout this review have consulted different data sets in accordance to the focus' of their research and studies, this review has sought to understand how those articles utilized them from a perspective of IDS within healthcare settings. Of the numerous datasets conferred and reviewed throughout this process, Hady et al, focuses on the overall topic of this study at a depth in which we would like to further expand upon. Therefore, the study's dataset was conferred in further detail to better understand the impact of different and contrasting healthcare systems which transfer patient health information (PHI) and electronic health record (EHR) exchange throughout medical facility networks.

Amongst the various different articles and publications reviewed throughout this study, it is important and relevant to note that different authors with similar and differing approaches towards healthcare IDS utilized datasets which best fit their methods. Some authors utilized datasets which depended upon patient biometric data and network metrics to identify patterns and deficits in IDS (Hady et al, 2020). Whereas other authors utilized and or referred to larger datasets which followed techniques common to practices observed in datamining procedures. This was beneficial to reflect upon techniques necessary for networks and servers which catered to larger hospital and healthcare information exchange dynamics. Furthermore, for anomaly detection methods, KDD99 IDS datasets, which are derived from DARPA 98 datasets, were also commonly observed amongst different research techniques in regard to identifying relevant features amongst different systems (Kushwaha et al, 2017). Figure 1 describes the different techniques observed by authors who sought to identify anomaly detection based on information exchange traffic patterns which were then compared to different datasets such as NSL-KDD which is considered to be a follow up on its preceding model, KD99 (Daojing et al, 2019).

Despite finding common factors amongst the methodology, design techniques and overall dataset usage amongst different authors and researchers, others were adamant on noting that such similarities in anomaly identification standards were due to a small number of outliers in the different datasets they observed. Thus, suggesting consistencies in their overall observations (Christy et al, 2015). For future approaches, it was also noted that researchers wanted to shift their methodologies and take on proactive approaches which would feature an elimination of training datasets to allow unfiltered focus upon the initial and primary datasets observed in the study to train and better understand the algorithm in motion. It was further implored that such changes would allow researchers to minimize the size in "hops" of information exchange throughout the network (Thamilarasu et al, 2020).

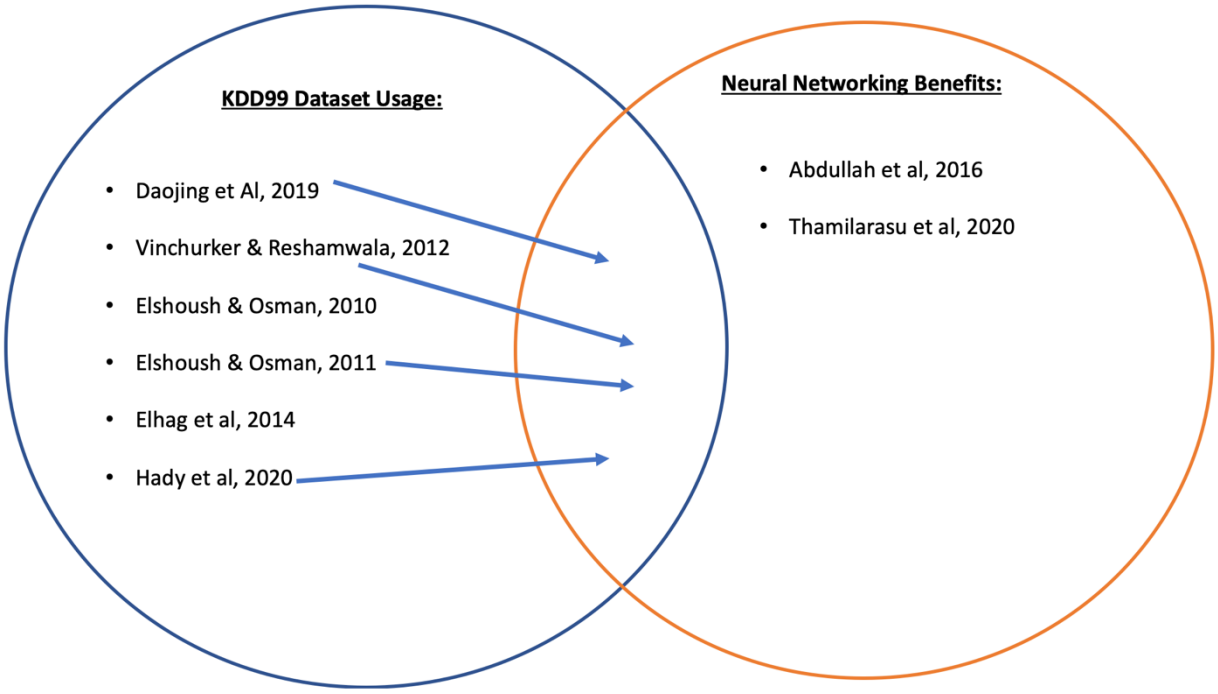

Figure 1. Displays a venn-diagram comparison illustrating the reviewed articles which observed and utilized a KDD99 dataset versus those which found or noted the impact of neural networking techniques in healthcare IDS.

4. Conclusion

Overall, as healthcare systems and settings continue to expand and evolve beyond the context of small, highly specialized clinical settings and larger, in-patient healthcare conglomerates, the networks in which they utilize for information exchange and the maintenance of EHR must follow suit. As the components of EHR expands with on-going factors such as each patient's healthcare experience, age and treatment outcomes, the exchange and relay of their PHI becomes increasingly extravagant to maintain, let alone assure in terms of privacy and security. Therefore, it is important that healthcare providers, especially those which partake in patient information exchange on a frequent if not continuous basis take into consideration the variety of security threats that may affect them and those they care for. Such measures may be considered a preemptive and proactive approach towards potential liabilities and against incoming risks from both internal and external threats.

Ultimately, the outcome of this research review suggests that novel approaches towards regulating and reviewing information exchange that is transferred throughout healthcare system networks are better regulated and ensured through newfound approaches within intrusion detection systems (Chen et al, 2016). Amongst such novel approaches, included those which prominently featured neural networking approaches in their methodology and techniques. Amongst the variety of different networks that utilize IDS, multiple articles noted that neural networking techniques such as fuzzy logic (Elshoush & Osman, 2011). In addition to this, other approaches such as stacked autoencoder was also commonly observed amongst different authors in suggesting alternative models of methodology. This neural network approach features multiple layers of autoencoders which are dispersed in an infrequent format. Each of these layers is connected to one another through producing a "stacked" formation and relaying information accordingly. In contrast to this, the fuzzy logic methodology of neural networking features a Boolean approach which allows numerous different variables to be condensed as they are processed through a single or similar component (Singh et al, 2013).

References

Bace, R. G., & Mell, P. (2001). *Intrusion detection systems*. Gaithersburg, MD: U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology.

Barney, B. (2015, December 7). Intrusion Detection System: What's Missing in HIPAA Security. Retrieved October 13, 2020, from https://www.securitymetrics.com/blog/intrusion-detection-system-whats-missing-hipaa-security

Daniels, J., & Bhatia, S. (2020). Legislation and the Negative Impact on Cybersecurity in Healthcare. *Proceedings of the 6th International Conference on Information Systems Security and Privacy*. doi:10.5220/0009157906910697

Ghadamyari, M., & Samet, S. (2020). Decentralized Electronic Health Records (DEHR): A Privacy-preserving Consortium Blockchain Model for Managing Electronic Health Records. *Proceedings of the 6th International Conference on Information and Communication Technologies for Ageing Well and E-Health*. doi:10.5220/0009398101990204

Graetz, I. (2014). The Next Step Towards Making Use Meaningful: Electronic Information Exchange and Care Coordination Across Clinicians and Delivery Sites. *Medical Care, 52*(12), 1037-1041. Retrieved September 29, 2020, from http://www.jstor.org/stable/10.2307/26417862?refreqid=search-gateway:97bb49c4f83cccfcfd27f803289678be

Gupta, B., & Srinivasagopalan, S. (2020). *Handbook of research on intrusion detection systems*. Hershey, PA: Information Science Reference.

Han, J., Kamber, M., & Pei, J. (2012). *Data mining: Concepts and techniques*. Amsterdam: Morgan Kaufmann.

Hájek, P., Godo, L., & Gottwald, S. (2001). *Fuzzy logic*. Amsterdam: Elsevier.

Introduction to Intrusion Detection Systems. (2003). *Cisco Security Professional's Guide to Secure Intrusion Detection Systems,* 1-38. doi:10.1016/b978-193226669-6/50021-5

Introduction: Cybersecurity and Society. (2018). *New Solutions for Cybersecurity*. doi:10.7551/mitpress/11636.003.0001

Kim, K., Aminanto, M. E., & Tanuwidjaja, H. C. (2018). *Network Intrusion Detection using Deep Learning: A Feature Learning Approach*. Singapore: Springer Singapore.

Klein, J. D. (2012). Do We Control Technology or Does Technology Control Us? *2012 ASEE Annual Conference & Exposition Proceedings*. doi:10.18260/1-2—21234

Lemaitre, L. (1996). Design Automation of Fuzzy Logic Circuits. *Fuzzy Logic,* 237-264. doi:10.1007/978-3-322-88955-3_8

Mitcham, C. (1989). In search of a new relation between science, technology, and society. *Technology in Society, 11*(4), 409-417. doi:10.1016/0160-791x(89)90026-2

Mookerjee, V. (2011). When Hackers Talk: Managing Information Security Under Variable Attack Rates and Knowledge Dissemination. *Information Systems Research, 22*(3, IT Value in Healthcare), 606-623.

Özgür, A., & Erdem, H. (2016). A review of KDD99 dataset usage in intrusion detection and machine learning between 2010 and 2015. doi:10.7287/peerj.preprints.1954v1

Pietro, R. D., & Mancini, L. V. (2011). *Intrusion detection systems*. New York: Springer.

Richterich, A. (2018). The Big Data Agenda: Data Ethics and Critical Data Studies. *Vol. 6*.

Singh, H., Gupta, M. M., Meitzler, T., Hou, Z., Garg, K. K., Solo, A. M., & Zadeh, L. A. (2013). Real-Life Applications of Fuzzy Logic. *Advances in Fuzzy Systems, 2013*, 1-3. doi:10.1155/2013/581879

Skrobanek, P. (2011). *Intrusion detection systems*. Rijeka, Croatia: InTech.

Schneider, E. C. (2014). Promoting Patient Safety Through Effective Health Information Technology Risk Management. Retrieved October 13, 2020, from http://www.jstor.org/stable/10.7249/j.ctt14bs3z5?refreqid=search-gateway:2ddc50a2cfebe3d65d60c22f4dede7ac

Elshoush, H. T., & Osman, I. M. (2010). Reducing false positives through fuzzy alert correlation in collaborative intelligent intrusion detection systems: A review. *International Conference on Fuzzy Systems*. doi:10.1109/fuzzy.2010.5584418

Elshoush, H. T., & Osman, I. M. (2011). Alert correlation in collaborative intelligent intrusion detection systems—A survey. *Applied Soft Computing, 11*(7), 4349-4365. doi:10.1016/j.asoc.2010.12.004

Kushwaha, P., Buckchash, H., & Raman, B. (2017). Anomaly based intrusion detection using filter based feature selection on KDD-CUP 99. *TENCON 2017 - 2017 IEEE Region 10 Conference*. doi:10.1109/tencon.2017.8227975

Parker, M. (2020). Healthcare Regulations, Threats, and their Impact on Cybersecurity. *Cybersecurity for Information Professionals,* 173-202. doi:10.1201/9781003042235-9

Ramasamy, B., & Hameed, A. Z. (2019). Classification of healthcare data using hybridized fuzzy and convolutional neural network. *Healthcare Technology Letters, 6*(3), 59-63. doi:10.1049/htl.2018.5046

Sangaiah, A. K., Thangavelu, A., & Sundaram, V. M. (2018). *Cognitive computing for big data systems over IoT: Frameworks, tools and applications*. New York, NY: Springer Berlin Heidelberg.

Thamilarasu, G., Odesile, A., & Hoang, A. (2020). An Intrusion Detection System for Internet of Medical Things. *IEEE Access, 8*, 181560-181576. doi:10.1109/access.2020.302626

Biographies

Munther Abualkibash is an assistant professor and graduate coordinator within the Eastern Michigan University College of Technology. His interests and expertise include computer and network security, cloud computing, machine learning and parallel and distributed systems. He received his master's degree from the University of Bridgeport, in Bridgeport, Connecticut. There, he also earned his Ph.D. in computer science and engineering.

Tasfia Bari is a PhD candidate and graduate research assistant in Eastern Michigan University's College of Technology. She earned her Bachelor of Science at Eastern Michigan University in Ypsilanti, Michigan. She has graduate research experience throughout her time in the College of Technology as both a master's and Doctoral candidate. She is currently working towards earning her PhD while conducting research as a graduate assistant under the supervision of Dr. Munther Abualkibash.