Technologies used in Services and Impact of Those in Providing Security

Dr Jyoti Batra Arora [1]*, Dr.Leela.M.H [2]

[1] Institute of Chartered Accountants of India, India.
[2] Dr. Ambedkar Institute of Technology, India.
*Corresponding Author Email: [1] jybatra@gmail.com

Abstract

Introduction: Technology may be utilised by security experts to conserve effort and money. Security practitioners may administer and monitor their own prevention programs and those of their "teammates or contractors successfully with the appropriate equipment". A healthier workplace has been made possible by "protective technologies", "robots", "artificial intelligence", "machine learning", and "information technology".

Aim: To recognise the various technologies applied to operations and their effect on security.

Material and Methods: "Numerous investigation techniques used during the study" have indeed been explored throughout the research subject. The "interpretivism research philosophy", which has been founded on a "conceptual model", was employed by the scholar. Additionally, the scholar has employed "secondary qualitative data-gathering techniques" that aid in "gathering reliable knowledge".

Results: The research study clarified the findings and covered a portion of the subject described concerning the "innovations utilised in offerings and their effects on supplying security". It has been made clear that a variety of technologies are being employed to counter the threat posed by digital security. While "AI and ML are extensively utilised technologies" that many organisations are progressively adopting to address security issues.

Conclusion: The world is gradually evolving and after the covid19 outbreak various new aspects have come forward where security has become a key part of organisations and individuals. The adoption of various technologies, especially, "AI and ML have been effective" and this trend is going to be high in the upcoming days.

Keywords

5G technologies, Artificial Intelligence, Covid19 outbreak, Cybersecurity, Detecting security intrusions, Machine Learning, Technologies, Virtual care innovations.

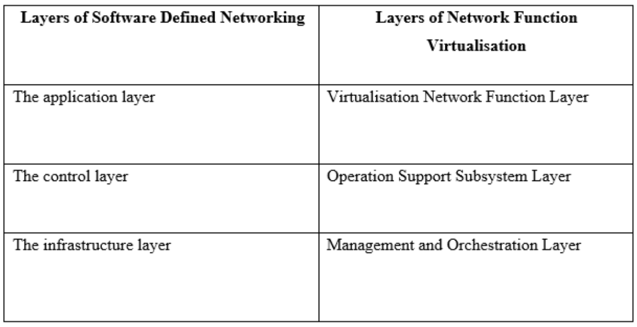
INTRODUCTION

The "functionalities of international stability are changing as a result of technological advancements", from "improving how individuals and organisations supervise their limits to lessening the effects of major calamities". "Surveillance aircraft, as well as artificial intelligence, looked to be technologies of the far beyond merely a handful of decades back". "Complex innovations are currently changing every element of the everyday life of humankind". "Security firms may well be slow to use the information to administer their labourers", however, when it is put in place, they "quickly see the immediate advantages of digital approaches". They are beginning to realise that "this seems to be no anymore possible to essentially station security personnel in a position". "Essential security measures are implemented via tangible protection technology". "Strong authentication restrictions", "process sensing", "identification and admission clearance verification", and "involvement evaluation are some of such measures". A "thorough programme of knowledge assurance vulnerability monitoring must include several measures". Today's "protection operators use innovation to increase their responsiveness and efficiency", gather "precise and comprehensive intelligence", and "provide additional commercial relevance to their patrons". The study has effectively analysed the various elements of the present study topic and also discussed the way of doing it. The end of this study is designed with a conclusion.

REVIEW OF ARTICLE

Since the "static structure of internet infrastructure, as well as installations", "standard technologies", "methods", and "practises-based networked countermeasures", are "unable to take into consideration the suspect's additional benefit". "Moving Target Defense (MTD) regularly changes the architecture" of something like the "supporting done to eliminate this unequal superiority", hence "lowering the successfulness of intrusions". The "most contemporary developments throughout the creation of MTDs had already previously been examined", and it's been "clearly indicated how such fortifications may be described using everyday language and improved employing computational intelligence tools" [19]. Additionally, this may be put into practice and assessed. It is clear that only an "MTD encapsulates the essential elements of certain countermeasures employing a straightforward but universal language". Furthermore, it is clear from the "implementation of numerous MTDs that base stations" like "Software Defined Networking" as well as "Network Function

Virtualisation" play a crucial role in “making such adaptive fortifications possible”.



Layers of Software Defined Networking	Layers of Network Function Virtualisation
The application layer	Virtualisation Network Function Layer
The control layer	Operation Support Subsystem Layer
The infrastructure layer	Management and Orchestration Layer

Table 1: “Various layers of SDN and NFV”

In order to “assist individuals in managing their hyperglycemia”, “virtual care innovation”, “particularly technological as well as healthcare apps”, has indeed been evolving quickly. There exist a “variety of well-being applications available for gadgets as well as various electronic connections to help persons with hyperglycemia” who are “required to make behavioural changes or change their prescription in accordance with information from diabetes management”. In “order to standardise how mobile medical applications are evaluated and tracked for patient protection as well as therapeutic effectiveness”, “legislation and standards have not yet been maintained with the rapidly developing industry” [8]. “Information on something like the feasibility and efficacy of medical apps, particularly for hyperglycemia”, is still scarce. “Worldwide organisations have accomplished progress in identifying various kinds of electronic medical technologies as well as incorporating telemedicine innovation into the realm of implantable implants”, notably the "World Health Organisation" as well as the "International Medical Device Legislators Council".

The “practical advantages of blockchain innovation in relation to several facets of any sector”, “marketplace”, and “institution or federal institution have gained increasing attention in subsequent seasons”, according to several specialists. In the “succinct existence of blockchain”, a “staggering number of advancements have already been achieved in terms of its potential applications as well as the effects it could have in many sectors”. It “may be challenging to approach the opportunities and complications of blockchain”, specifically, when “attempting to determine its function as well as suitability for a particular activity”, because of the “enormous quantity as well as the sophistication of such factors”. It is undeniable that the “architecture of blockchain as well as the contemporary cloud- as well as edge-computing methodologies are essential for permitting a wider adoption as well as expansion of blockchain applications for prospective participants in the unprecedentedly lively worldwide current market” [4]. In order to “effectively advance the protracted objectives of blockchain proponents”, it is imperative that “blockchain becomes publicly accessible using transparent and expansive programming toolkits”.

“Fifth Generation (5G) wireless communication innovation is gathering steam and aims to integrate nearly every area of existence across the connection with a substantially quicker pace”, “extremely minimal congestion, and an all-pervasive connection”. The “internet should safeguard its consumers, features, as well as applications because of its vital importance in people's lives”. Because of the massive growth in the quantity and variety of capabilities offered by 5G, the “vulnerability analysis environment has significantly expanded” [1]. In order to “deal with a variety of attacks on multiple operations”, “innovative innovations”, as well as “more useful information attainable via networking”, “cryptographic protocols”, if not currently implemented, should be explicitly conceived. It appears that the “security strategies, as well as topologies, utilised in earlier versions (such as 3G and 4G), won't work for 5G”. The “dynamism of emerging applications, as well as innovations in 5G, are the primary driver behind enhanced security approaches as well as layout”.

Since “vulnerabilities can entail serious repercussions”, “confidentiality has emerged as the top priority in several telecommunications sectors nowadays”. “Upcoming communications networks must transfer sensitive data of any kind strata”, specifically, since the “fundamental and accompanying capabilities will be linked to the 5G connection” [11]. Numerous events showed that the danger posed by an infiltrated wireless connection influences the complexities of something like the information landscape in addition to protection and confidentiality issues. The “identification or suppression of disruption has become a worldwide issue as a result of the rapid growth of diversity as well as the power of potential threats”. Since vulnerabilities could get serious repercussions, “privacy has emerged as the top priority in several telecommunications sectors presently”.

“Smart city administrators”, “developers”, “processors”, and “institutions face major governmental”, “technological and economical hurdles as a result of the interconnected and sophisticated architecture of such social concepts”. Assessments that “emphasise the vulnerabilities to digital protection”, as well as the “difficulties facing smart city facilities throughout the administration as well as the processing of personal data”, are “increasingly focusing on the confidentiality”, “transparency”, and “vulnerabilities inside pervasive computing” [10]. “Legislators and provincial governments face major economic”, “administrative”, and “technological hurdles as a result of the alteration to current infrastructure's increasing difficulties as well as the advancements of participatory democracy that are demanded”. The “acquisition as well as administration of information”, is among the “major issues facing the creation of a green infrastructure”.

Because of “societal conventions that encourage social isolation as well as widespread confinement”, the covid19 outbreak has inevitably resulted in a rise in the usage of digital devices. Worldwide, “individuals and organisations were required to adapt to modern styles of living and working". "Businesses and universities are converting to work-from-home policies as a result of increased digitisation" [15]. "Blockchain innovation will grow in importance", "necessitating development and regulatory studies". "Gig employment, as well as digitisation, is expected to grow in size", "generating issues with how employment is distributed", "how people collaborate", and "how people are motivated and how conscientiousness and workload pressure are affected". With more people online, concerns like "corporate surveillance and burnout will surface". "Digital deception is anticipated to increase as will study into security management" [23]. After the outbreak, "controlling online services", a valuable commodity, will be essential.

MATERIALS AND METHOD

This study was conducted using the "interpretivism research philosophy" to "collect diverse ideas or viewpoints". The "empirical concept study design outlines the methods that should be employed to gather data", "evaluate the data", and "apply the theoretical background". When analysing the data, it "neglects to take any consideration of the philosophical stance, methodology, or perspective". Additionally, the "interpretivism philosophy" benefit allows the scholar to "explore the investigation issue in-depth as well as incorporate key discoveries" [2].

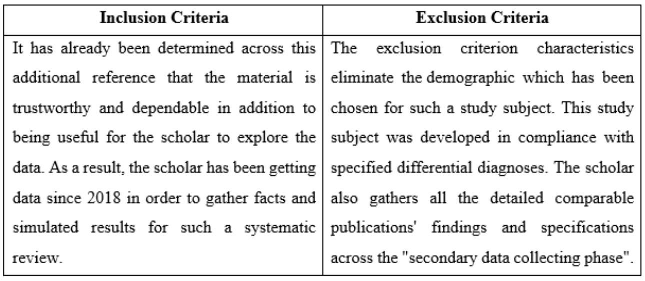
The "present assessment of the study issue has been completed" by the scholar using the "deductive research technique." As a result, "the set of intentions of conduct as procedures that the scholar followed and kept an eye on throughout initiating and conducting this investigation is mentioned including this design methodology" [24]. The scholar was "capable of identifying the connection between the investigation" and the "investigation methodology during this approach". This "deductive research technique" has allowed the author to "make extensive usage of all accessible collecting and analysing pertinent knowledge from the knowledge set". The scholar may "assist in understanding how the specific aims relate to the data" by using this "deductive research methodology". Additionally, the scholar has employed "this study methodology to confirm that the scholar is relevant in providing the permitted content following the study subject".

This "inquiry technique outlines the whole process used to implement a study plan", from a "conceptual foundation through the gathering and interpretation of data". In "order to gather data and comprehend" the "many approaches to obtaining conclusions that are appropriate for the scoping review", the scholar has used a "deductive research strategy". "Understanding the goal of something like the study subject" that has been carried out by the scholar via this "investigation procedure is one of the benefits of something like" the "explanatory research design". For just the scholar who has "satisfactorily met every requirement for the study objectives", this "explanatory research design" is beneficial. Alternatively, the "period of collecting appropriate outcomes and comprehending them across the major situations is productive for this efficient research strategy" [18].

In order to "gather effective information as well as outcomes through the proper process of the study operations", the "qualitative knowledge gathering approach" was utilised for such "particular research" [3]. With the "use of secondary dataset acquisition", the scholar may "use this qualitative studies approach to gather examples to show the study objectives and findings". The scholar has employed a "range of data-gathering techniques", involving "conversations", "newspaper publications or studies", "documentary assessment", as well as "monitoring". While using the empirical fact "qualitative data collecting approach," the scholar is "able to gather pertinent knowledge of the study issue".

The "study title's goals were discovered" by the author by using a "secondary data gathering method." It seems necessary for the scholar to "compile proof in addition to gathering knowledge from internet-relevant data" to maintain "precision." The study discussion "qualitative analysis" also "serves as a candidate for secondary information gathering across a variety of digital periodicals", "portals", "scientific papers", "statistical data repositories", "podcasts", and "conferences", as well as others [9]. As a result, this "method of data collecting is efficient for the scholar who has gathered the knowledge and preserves effort and budget". Furthermore, it is "simple to gather the large amount of data required for the full study issue".

Facility "sampling chooses a non-probability stratified selection that is incorporated into the population because it provides the most accessibility to the scholar". The scholar has amassed "relevant and suitable knowledge and proof about the study issue"; nonetheless, the "full analysis, as well as produced material, should be trimmed while adhering to a suitable sample strategy". The "preference sampling approach was utilised to gather evidence from applicable statistics as well as appropriate knowledge repositories in a bid to advance this investigation issue" [12]. The scholar is "required to gather a significant number of facts along with variables during this sampling method with a little level of inquiry activity", which has spared both "moments in addition to resources".



Inclusion Criteria	Exclusion Criteria
It has already been determined across this additional reference that the material is trustworthy and dependable in addition to being useful for the scholar to explore the data. As a result, the scholar has been getting data since 2018 in order to gather facts and simulated results for such a systematic review.	The exclusion criterion characteristics eliminate the demographic which has been chosen for such a study subject. This study subject was developed in compliance with specified differential diagnoses. The scholar also gathers all the detailed comparable publications' findings and specifications across the "secondary data collecting phase".

Table 2: "Inclusion and Exclusion Criteria"

For such a "secondary qualitative data gathering", the scholar used "thematic analysis," which compiles the key components of something like the "digital methodological approach". Consequently, "thematic analysis" has helped the study to lessen its goals, which are “evaluated throughout the discussion paper” [5]. This “information evaluation procedure helps to provide the study inquiry with a systematic conclusion by compiling some published documents”, “periodicals”, “and scholarly articles”, as well as “webpages”. The “concepts are centred on the priorities of something like the study subject”, which are to assist the scholar in “elucidating the investigation aim using evidence processing”.

In “order to maintain the standard of an investigation”, it is “important to take care of moral considerations” [14]. The scholar has made sure about all these “standards while implementing this piece of work”. The “examination procedure authorises its legitimacy regarding the many knowledge”, and themes, as well as “documents that are being obtained in terms of ensuring any kind of favourable consideration”. The “investigation procedure adheres to the research assumptions”. Additionally, the scholar “adheres to the entire study's professional conduct”, including those for “dependability”, “accuracy”, as well as “accountability”. The above "Data Protection Act" seems to be “consequently tremendously helpful for the scholar since it makes it easier when they gain insight”, “store it”, as well as “evaluate the findings while also still tying it in with the full study evaluation that is being continually monitored” [22].

RESULTS

Elevated business managers' “engagement in cybersecurity increased dramatically throughout 2018 and 2019”. A “growing number of individuals are constantly worrying about cybersecurity”, which is rapidly occupying people's thoughts [17]. A “yearly basis poll is conducted by TD Ameritrade of its own qualified investment advisers, who work for firms that oversee the investments of high-net-worth people”. On many digital acquisitions, “RIAs altered their minds between 2018 and 2019”. Approximately “1 in 10 RIAs reported that they were thinking about engaging throughout cybersecurity as humans enter 2018”. Approximately “6 out of 10 RIAs stated they planned to increase cybersecurity within the next year”. “Appraisal and reward technology”, “developments in electronic signatures and electronic paperwork”, “CRM tools”, “wealth management”, and “virtual communication technologies were among the additional areas where market volatility significantly increased”.

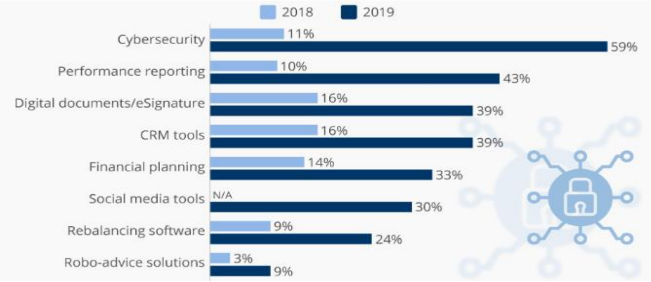


Figure 2: 2019 was a big year for Cybersecurity investment (Source: Statista, 2022)

The above figure depicts that in 2018 the cybersecurity investment was only eleven percent whereas in 2019 the investment was around fifty-nine percent. This reflects that organisations all over the world are more dependent on cybersecurity nowadays and they are more concerned about the protection of their data and assets. Additionally, authentication is crucial in this aspect. In order to ensure that a partner is really the one who has permission to enter an exact aspect, status authenticity is necessary [20]. For “authentication to be successful”, there must be at least 3 basic initially put.

The “international production of digital security has been expanding quickly”. This is mostly because “businesses are strengthening their protection regarding cybersecurity incidents and because there are more of them”, especially inside their own organisations. Entire teams, from “C-suite directors to everyday customers, are having trouble with cybersecurity as online scammers as well as cybercriminals trying to obtain secure data approach both groups”. “Artificial intelligence technologies are being used by businesses all over the world to identify and prevent protection vulnerabilities” [7]. This same “Consumers Technologies Federation poll of businesses revealed” that even below half said they were employing this innovation to that aim. “Equivalent findings have been reached by unaffiliated studies”, especially by “Technalysis Investigation as well as 451 Experiments”.

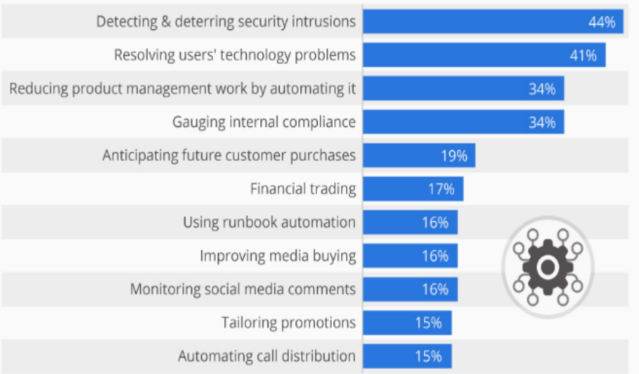


Figure 3: Detecting security intrusions are the top AI application in 2018
(Source: Statista, 2022)

According to the aforementioned statistic, "Detecting security incursions are the top AI application, comprising roughly 44%," in 2018. In addition, "Revolving users' technological difficulties" makes up around 41% of the list, and "Reducing product management effort by automating it" makes up another 34%. The last item on the list, "Gauging internal compliance," is the same as the one before it. Since “cyberattacks are growing progressively complex”, it is getting harder to reliably identify breaches. If incursions are not stopped, “security forces like database authenticity”, “validity, as well as resilience may lose their trust”. It is clear that several intrusion detection techniques are being presented to combat online security risks. These techniques may be generally categorised as "Signature-based Intrusion

Detection Systems) as well as Anomaly-based Intrusion Detection Systems" [25].

The “worldwide cyber security industry was estimated at USD 217.9 billion in 2021”, and “USD 240.27 billion this year”, and yet is expected to “increase at a compound annual development percentage of 12.3% from 2023 to 2030”, according to the below-mentioned graph. The expansion of digital sensors, the “rise of e-commerce channels”, and the “rise in cyberattacks are just a few of the drivers fueling the marketplace's expansion”. Moreover, the data also revealed that the “cybersecurity marketplace across the globe is expected to become USD 315.56 in 2025 and USD 345.4 in 2026”. Well with the “rise in the consumption of goods with cognitive as well as IoT technology”, “cyber dangers are expected to change”. In order to “identify”, “reduce,” and “limit the hazard of cyberattacks”, “enterprises are likely to acquire as well as implement sophisticated cybersecurity solutions, fueling the industry's expansion” [13].

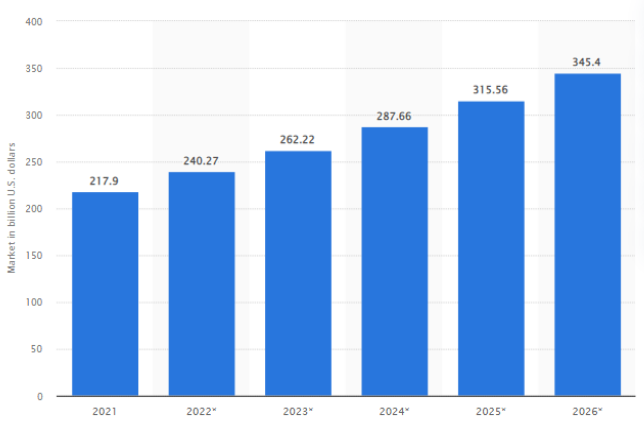


Figure 1: Size of the cybersecurity market worldwide from 2021 to 2026
(Source: Statista, 2022)

According to the “shutdown of various firms throughout the early as well as second phases of 2020”, cybersecurity saw a minor decline. Eventually, as “more businesses implemented virtual employment conditions together with cyber security technologies”, the “industry began to rebound by the conclusion of this same second period”. In order to “supervise and safeguard the vast amount of devices connected while also being protected from cyberattacks”, “many enterprises implemented cyber security technologies”. The “development of security mechanisms utilising AI as well as machine understanding by cybersecurity firms is helping businesses simplify overall IT defence” [21]. By “enabling intrusion detection system identification, these technologies let IT companies spend less effort tracking malevolent behaviours and strategies”.

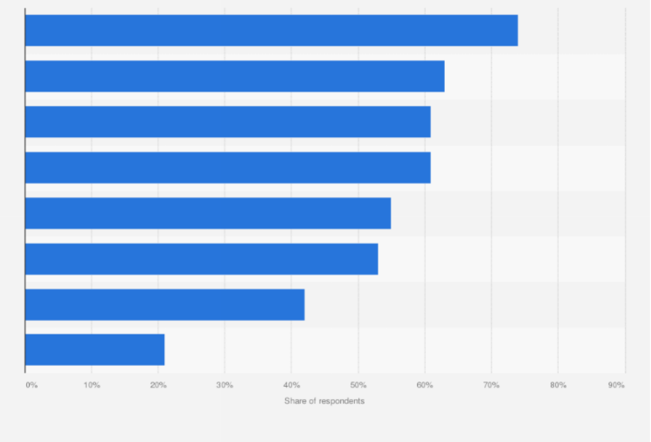


Figure 4: AI and ML cybersecurity application objectives 2021
(Source: Statista, 2022)

The above data reflects that many have already made their “concern regarding the use of AI and ML cybersecurity applications”. Many organisations, especially the IT ones have already adopted “many AI-based and ML-based cybersecurity applications which have made a huge impact on the business process also”. In order to safeguard corporate platforms, an “IT staff must guarantee interoperability” [16]. “Groups become worn out as they combine constant notifications with frequently performed assistance chores while using manual techniques for analysing layout security”. Groups might obtain prompt guidance on recently found problems with the help of intelligent, “adaptable automation”. They may receive suggestions on “how to progress and maybe have established mechanisms to dynamically change preferences as necessary”.

“Cybersecurity, as well as AI, has already been hailed as transformative technologies that are far nearer than consumers would realise”. This seems merely a simple lie, though, so organisations should proceed with caution. The truth is that at some point long term, individuals could have to deal with advances that appear quite gradually. When put into context, what could appear slow in comparison to a totally independent destiny is nevertheless well beyond what humanity has previously proven successful in accomplishing. It's crucial to contextualise the present specific problems in cybersecurity as the researcher "attempts to investigate the potential consequences of stability in machine learning as well as AI" [6]. “Designers may tackle numerous procedures and features that they have traditionally regarded as commonplace using AI technology”.

CONCLUSION

According to the study's findings, “security has been currently provided through a variety of solutions, as well as the practice has gained increasing significance and relevance over time”. Despite being viewed as a superset encompassing fields like "machine learning and deep learning cybersecurity", "artificial intelligence do possess distinct responsibilities to fulfil".

At its foundation, AI is focused more on "achievement" than "perfection," which is given less importance. The" overall purpose of complex problem-solving is spontaneous replies. Authentic AI uses judgements that are actually determined independently". Instead of only "drawing the hard-logical assumption from the information, its functionality is intended to identify the best answer for a given circumstance". In certain ways, "ML is the antithesis of actual AI". "Machine learning places a strong emphasis" on "precision," while less emphasis is placed on "accomplishment." This indicates that "ML moves forward intending to learn from a population that seems to be undertaking". Determining the performance's optimum efficiency brings the analysis to a close. Depending on various figures, this should seek the single viable answer, even though it is not the best one. "Due to the lack of genuine analysis of the information using ML", personnel assignment teams remain in charge of carrying out this duty.

REFERENCES

[1] Ahmad, I., Shahabuddin, S., Kumar, T., Okwuibe, J., Gurtov, A. and Ylianttila, M., 2019. Security for 5G and beyond. *IEEE Communications Surveys & Tutorials*, *21*(4), pp.3682-3722. https://ieeexplore.ieee.org/abstract/document/8712553/

[2] Alharahsheh, H.H. and Pius, A., 2020. A review of key paradigms: Positivism VS interpretivism. *Global Academic Journal of Humanities and Social Sciences*, *2*(3), pp.39-43. https://gajrc.com/media/articles/GAJHSS_23_39-43_VMGJbOK.pdf

[3] Archibald, M.M., Ambagtsheer, R.C., Casey, M.G. and Lawless, M., 2019. Using zoom videoconferencing for qualitative data collection: perceptions and experiences of researchers and participants. *International journal of qualitative methods*, *18*, p.1609406919874596. https://journals.sagepub.com/doi/abs/10.1177/1609406919874596

[4] Berdik, D., Otoum, S., Schmidt, N., Porter, D. and Jararweh, Y., 2021. A survey on blockchain for information systems management and security. *Information Processing & Management*, *58*(1), p.102397. https://www.sciencedirect.com/science/article/pii/S030645732030892X

[5] Braun, V. and Clarke, V., 2019. Reflecting on reflexive thematic analysis. *Qualitative research in sport, exercise and health*, *11*(4), pp.589-597. https://www.tandfonline.com/doi/abs/10.1080/2159676X.2019.1628806

[6] Capuano, N., Fenza, G., Loia, V. and Stanzione, C., 2022. Explainable Artificial Intelligence in CyberSecurity: A Survey. *IEEE Access*, *10*, pp.93575-93600. https://ieeexplore.ieee.org/abstract/document/9877919/

[7] Dash, B., Ansari, M.F., Sharma, P. and Ali, A., 2022. THREATS AND OPPORTUNITIES WITH AI-BASED CYBER SECURITY INTRUSION DETECTION: AReview. *International Journal of Software Engineering & Applications*, *13*(5), pp.13-21. https://www.researchgate.net/profile/Bibhu-Dash-5/publication/364011742_THREATS_AND_OPPORTUNITIES_WITH_AI-BASED_CYBER_SECURITY_INTRUSION_DETECTION_A_REVIEW/links/6336595476e39959d6858094/Threats-and-Opportunities-with-AI-based-Cyber-Security-Intrusion-Detection-A-Review.pdf

[8] Fleming, G.A., Petrie, J.R., Bergenstal, R.M., Holl, R.W., Peters, A.L. and Heinemann, L., 2020. Diabetes digital app technology: benefits, challenges, and recommendations. A consensus report by the European Association for the Study of Diabetes (EASD) and the American Diabetes Association (ADA) Diabetes Technology Working Group. *Diabetes care*, *43*(1), pp.250-260. https://diabetesjournals.org/care/article-abstract/43/1/250/35864

[9] Grodal, S., Anteby, M. and Holm, A.L., 2021. Achieving rigor in qualitative analysis: The role of active categorization in theory building. *Academy of Management Review*, *46*(3), pp.591-612. https://journals.aom.org/doi/abs/10.5465/amr.2018.0482

[10] Ismagilova, E., Hughes, L., Rana, N.P. and Dwivedi, Y.K., 2022. Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Information Systems Frontiers*, *24*(2), pp.393-414. https://link.springer.com/article/10.1007/s10796-020-10044-1

[11] Khan, R., Kumar, P., Jayakody, D.N.K. and Liyanage, M., 2019. A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. *IEEE Communications Surveys & Tutorials*, *22*(1), pp.196-248. https://ieeexplore.ieee.org/abstract/document/8792139/

[12] Lamm, A.J. and Lamm, K.W., 2019. Using non-probability sampling methods in agricultural and extension education research. *Journal of International Agricultural and Extension Education*, *26*(1), pp.52-59. https://scholar.archive.org/work/uohocfu7unf5fe7cocieeedc4y/access/wayback/https://www.aiaee.org/attachments/article/1742/7%20Non-Probability%20Sampling%20Methods%20in%20Ag_Lamm.pdf

[13] Li, Y. and Xu, L., 2021. Cybersecurity investments in a two-echelon supply chain with third-party risk propagation. *International Journal of Production Research*, *59*(4), pp.1216-1238. https://www.tandfonline.com/doi/abs/10.1080/00207543.2020.1721591

[14] Navalta, J.W., Stone, W.J. and Lyons, S., 2019. Ethical issues relating to scientific discovery in exercise science. *International journal of exercise science*, *12*(1), p.1. https://digitalcommons.wku.edu/ijes/vol12/iss1/1/

[15] Pandey, N. and Pal, A., 2020. Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. *International journal of information management*, *55*, p.102171. https://www.sciencedirect.com/science/article/pii/S0268401220309622

[16] Sarker, I.H., Furhad, M.H. and Nowrozy, R., 2021. Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science*, *2*(3), pp.1-18. https://link.springer.com/article/10.1007/s42979-021-00557-0

[17] Sawik, T., 2022. A linear model for optimal cybersecurity investment in Industry 4.0 supply chains. *International Journal of Production Research*, *60*(4), pp.1368-1385. https://www.tandfonline.com/doi/abs/10.1080/00207543.2020.1856442

[18] Seidel, S. and Watson, R.T., 2020. Integrating explanatory/predictive and prescriptive science in information systems research. *Communications of the Association for Information Systems*, *47*(1), p.49. https://aisel.aisnet.org/cais/vol47/iss1/49/

[19] Sengupta, S., Chowdhary, A., Sabur, A., Alshamrani, A., Huang, D. and Kambhampati, S., 2020. A survey of moving target defenses for network security. *IEEE Communications Surveys & Tutorials*, *22*(3), pp.1909-1941. https://ieeexplore.ieee.org/abstract/document/9047923/

[20] Simon, J. and Omar, A., 2020. Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *European Journal of Operational Research*, *282*(1), pp.161-171. https://www.sciencedirect.com/science/article/pii/S037722171930757X

[21] Tao, F., Akhtar, M.S. and Jiayuan, Z., 2021. The future of artificial intelligence in cybersecurity: A comprehensive survey. *EAI Endorsed Transactions on Creative Technologies*, *8*(28), pp.e3-e3. https://publications.eai.eu/index.php/ct/article/view/1418

[22] Wachter, S. and Mittelstadt, B., 2019. A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Colum. Bus. L. Rev.*, p.494. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/colb2019&section=15

[23] Wright, J.H. and Caudill, R., 2020. Remote treatment delivery in response to the COVID-19 pandemic. *Psychotherapy and psychosomatics*, *89*(3), p.1. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7179517/

[24] Young, M., Varpio, L., Uijtdehaage, S. and Paradis, E., 2020. The spectrum of inductive and deductive research approaches using quantitative and qualitative data. *Academic Medicine*, *95*(7), p.1122. https://journals.lww.com/academicmedicine/Fulltext/2020/07000/The_Spectrum_of_Inductive_and_Deductive_Research.41.aspx?context=FeaturedArticles&collectionId=8

[25] Zhong, W., Yu, N. and Ai, C., 2020. Applying big data based deep learning system to intrusion detection. *Big Data Mining and Analytics*, *3*(3), pp.181-195. https://ieeexplore.ieee.org/abstract/document/9142151/