Timnit Gebru's "Race and Gender"

Dillep Kumar Pentyala[1]
[1]Financial Analytics, JP Morgan Chase, UNITED STATES

ABSTRACT

There are a lot of real-life applications of artificial intelligence (AI), such as automated health diagnostic systems, decision systems that utilise machine learning to forecast crime recidivism rates, and huge face-recognition-based monitoring. Unfortunately, the social and political factors that make AI more harmful than helpful to some groups of people have not been adequately investigated alongside AI's fast penetration into society. For example, whereas commercial face recognition systems make very few mistakes when it comes to males with light complexion, they make a lot more mistakes when it comes to women with darker skin. Recidivism assessment systems in the United States that rely on machine learning are skewed against Black Americans, according to a 2016 ProPublica study. For example, the homemaker's completion of the comparison "Man is to computer programmer as woman is to X" demonstrates that natural language processing algorithms trained on newspapers have cultural prejudices, according to other studies. Books like Automated Inequality and Weapons of Math Destruction show how lower-class Americans are more likely to be subjected to automated decision-making technologies than upper-class Americans. As a result, these instruments are typically employed on those against whom they display the greatest prejudice. We need a comprehensive and multi-pronged strategy to address bias in machine learning systems, even if several technological solutions have been suggested. This involves standardisation bodies deciding which systems are applicable in which situations, ensuring that diverse backgrounds are represented in the development of automated decision tools, and gaining an understanding of the political and historical factors that disadvantage specific groups when these tools are used against them.

Keywords: AI Gender; Prejudice; AI Openness; AI Power; AI Ethics

Introduction

A lot of people think of science as a neutral field that seeks the truth. The idea that technology is fundamentally neutral and that goods created by a small fraction of the population may be used by everyone is also a possibility. A lack of representation among individuals with the power to create technology has led to a power imbalance globally and technology whose intended or unintended negative consequences hurt those who aren't involved in its production, according to an examination of 19th-century scientific thinking and significant technological advancements like automobiles, medical practices, and other fields [1–7]. Machine learning is also not an exception. Technology has the potential to improve people's lives, but it has also been demonstrated to discriminate against marginalised groups, whether intentionally or unintentionally, due to the concentration of power in a few global hubs and the continued dominance of the most powerful racial and ethnic groups in each region [8-25].

Those that perpetuate bias in this field, like many others, typically do so in the name of innovation. Nevertheless, scientists are often blinded to their own biases and encodings by the common belief that they are "objective." This prevents them from critically evaluating their own work and the goals they are advancing. One well-researched and well-considered alternative to creationism was Charles Darwin's theory of evolution, which he developed in

the nineteenth century. However, what many fail to mention is that he wrote: "The western nations of Europe... "in his book On the Origin of Species by Means of Natural Selection, or the Preservation of Favoured Races in the Struggle for Life. ..currently stand at the pinnacle of civilisation, having surpassed their earlier barbaric ancestors by an immense margin. ...It is highly probable that the more civilised human races will wipe out and replace the more barbaric ones on Earth. In his later work, The Descent of Man and Selection in Relation to Sex, he makes the observation that "[m]an is more courageous, pugnacious and energetic than woman, and has a more inventive genius." 2. Despite criticism of Darwin's work for its position against the church and the British empire, his brain is clearly bigger than hers. Her skull is believed to be at a transitional stage between childhood and adulthood.

British anthropologists such as James Hunt utilised Darwin's theory to legitimise slavery in works like The Negro's Place in Nature (1863) [25-57], which in turn served to legitimise colonialism by asserting that the ruled were inherently inferior scientifically and unable to govern themselves. Michael Yudell, a professor of public health, argues that race is "a concept we think is too crude to provide useful information, a concept that has social meaning that interferes in the scientific understanding of human genetic diversity and a concept that we are not the first to call upon moving away from [58-65]." This argument has been advanced repeatedly since Darwin's day, demonstrating that race is a social construct without any biological basis.

Notable scientists, such as evolutionary psychologist Steven Pinker, continue to insist on a genetic basis; for instance, in his books Groups and Genes7, Pinker asserts that Ashkenazi Jews possess an inherent intelligence. Papers posing the question "Why are males over-represented at the upper extremes of intelligence?" continue to be published by scientists in their pursuit of understanding gender related disparities in intelligence, echoing Darwin's claims about the links between genius and gender."

The assertion that men are disproportionately represented at the highest levels of intellect is not challenged by these enquiries. Claiming to have empirical evidence that men are more likely to score at the very top and very bottom of the IQ scale, researchers have extrapolated this finding to suggest that men display a wider range of "intelligence" in general, rather than just on the IQ test [66-88].

Claims like this, which seem to be supported by facts and "science," are less likely to be examined due to the illusion of scientific impartiality. A large number of modern scientists share Darwin and Hunt's belief that racial and gender differences in aptitude are intrinsic. Nevertheless, their opinions are likely to acquire respect due to the fact that their works appear to be supported by facts and empirical investigations. For instance, none of these assessments take into account the fact that White males conceived of, developed, and assessed the IQ test based on their own conceptions of "smartness" and "genius" [89-103].

As a matter of fact, American standardised testing has a long and racially charged history. 50 Years of Unfairness, edited by Ben Hutchinson and Margaret Mitchell, delves into the works of civil rights activists who championed testing equity at that time. The current

discussions and ideas in the field of artificial intelligence ethics and justice are reminiscent of those from that era.

So, assertions regarding gender and race based on evidence put forth by thinkers like Charles Darwin are relevant today and likely to remain so for some time. The choice of methodology to "corroborate" such assertions will be the sole variation. According to Reuters, Amazon disabled its automated recruiting system in 2019 after discovering it was biassed against women. The tool devalued alumni of two all-female institutions and "penalised resumes that included the word 'women's,' as in 'women's chess club captain,'" according to Reuters.

It is hardly unexpected that an automated employment tool like Amazon's would have these prejudices when viewed in the context of the society it was developed for. As a form of protest over how the corporation dealt with sexual harassment in 2018, Google employees went on strike. Not long after that, in 2019, news stories published testimonials from Microsoft employees detailing their experiences with toxic work environments, including unpunished sexual harassment, a lack of opportunities for advancement, and various types of discrimination [104-117].

The fact that women founded and still dominate the computer industry makes this unfriendly climate all the more paradoxical. While women historically held the majority of computing positions, this began to alter in the 1960s and 1970s as personal computers became economically viable, as Marie Hicks explains in Programmed Inequality.

This is not an issue specific to computers. Jobs that were traditionally associated with women (like cooking) are no longer seen as such if they start making a good living for their employers. As an illustration, males still hold much of the power in the restaurant industry in the United States, while women are traditionally expected to do the culinary duties at home. In a similar vein, computers had gone from being seen as a traditionally female occupation to being largely male by the 1970s. Similar to the IQ exam, IBM developed the Programmer Aptitude exam (PAT) to identify candidates with the "traits" of a good programmer. The emphasis on logic puzzles, word games, and mathematical trivia, for instance, did not permit any more, as pointed out by Nathan Ensmenger. Unfortunately, solving these kinds of problems that have nothing to do with the job that the candidate is applying for used to be a component of certain interview procedures until quite recently. Despite the fact that some tech organisations, like Google, have done away with mental teasers since they don't correlate to an applicant's future performance, many others have taken up Google's whiteboard interviewing technique [118–124].

Runaway Feedback Loops: Outcome Determination by Analysis of Previous Data

The subjective prejudices of the persons who created the aptitude test will inevitably seep in, causing it to exclude varied groups of people who do not conform to the strict, arbitrarily determined standards. Those who are stereotyped as being unwelcome in the IT business may find it even more difficult to advance in their careers, receive recognition for their efforts, or even break into the field altogether. Consequently, it should come as no surprise that in 2018, automated recruiting techniques utilised by companies like Amazon, which

innocently employ historical data to train models for future results, lead to runaway feedback loops that worsen preexisting social prejudices.

Amazon is notoriously hostile to people of colour, women, people of colour, Latinx, Native American descent, and individuals with disabilities, so any hiring model that tries to predict what factors determine a candidate's chance of success at Amazon would inevitably find that the undersampled majority (a term coined by Joy Buolamwini) is not likely to succeed those with disabilities, those who identify as LGBTQ+, and any other historically oppressed group in the United States and the technology sector. The individual might not have a chance of success due to an atmosphere that does not foster the growth of individuals from particular backgrounds, or they might not get employed due to bias in the interview process. When a model is developed using this data, it makes society problems worse, leading to even more marginalisation. Those from the non-marginalized group are given an advantage in the model's selection process, which increases their chances of being employed and their chances of success in the company's environment. As a result, the hiring tool receives more biassed training data, which in turn reinforces the bias, leading to an even more vicious cycle of marginalisation.

There are many more sorts of feedback loops that can exacerbate prejudice, and hiring models are no exception. Another example of a system that might display runway feedback loops is predictive policing, which uses a model trained on data such as the number of arrests in a certain neighbourhood or the number of recorded crimes to identify potential "hotspots" for criminal activity. There is a significant disparity between the number of reported crimes and the number of actual criminals in several US regions. For instance, while drug use is fairly distributed throughout Oakland according to the national study on drug use and health, reports of drug use to police are concentrated in neighbourhoods that are primarily Black. According to research by Kristian Lum and William Isaacs, the widely used predictive police algorithm, Predpol, actually makes things worse by labelling these areas, which are disproportionately Black, as crime hotspots. As a result, these areas get greater police attention, which appears to confirm the presence of higher crime rates as more persons are arrested there compared to areas with less police presence.

Number sixteen: Lum, Kristian, and Isaac William. Significance 13, no. 5 (2016): 14-19. "To predict and serve?." Semiconductor in such areas compared to others. An increase in over-policing in low-income areas and amplification of systemic prejudice result from the subsequent use of these additional arrests as training data.

The Unchecked Use of Prejudiced AI Facial Analysis Tools

The United States Department of Justice uses a variety of data-driven techniques, including predictive policing. One out of every two individuals in the US is already part of an unchecked database that law enforcement agencies may access whenever they want, according to the eternal lineup report by Jonathan Frankle, Alvaro Bedoya, and Clare Garvie, which details the unchecked use of facial recognition technology by American law enforcement. At this time, there is no rule that specifies when and how to employ these technologies, or that audits their correctness. Operators are not adequately educated on the

use of any of these instruments, and the paper goes on to talk about how people might end up in prison as a result of mistaken identity. After outlining a procedure for public discussion of the benefits and drawbacks of automated face analysis tools, the authors provide a model statute that would govern the government's use of these technologies.

The current state of affairs is such that automated face analysis techniques are being used unchecked in high-stakes areas like employment, in addition to law enforcement. In addition, new research by Buolamwini and Gebru reveals that these instruments may be systematically biassed against certain genders and skin types. Findings showed that darker-skinned women had mistake rates as high as, and lighter-skinned males had near-perfect classification (error rates of 0% to 0.8%) after evaluating the performance of commercial gender categorisation systems from three companies: IBM, Microsoft, and Face++ 35.5 percent. Within six months of the publication of this study, both IBM and Microsoft released updated application programming interfaces (APIs). Google and other large corporations also formed fairness organisations. In response, US Senators Cedric Richmond, Cory Booker, and Kamala Harris demanded that automated facial analysis tools be regulated by the government. The healthcare business was not the only one that voiced concerns about the unchecked use of AI.

The research by Buolamwini and Gebru demonstrates that societal views on gender and race impact the development and use of AI systems. For instance, although previous research has examined the reliability of automated face recognition systems by looking at how well they handle racial identification based on location, no studies have done the same for skin type, and even fewer have addressed intersectional accuracy discrepancies in commercial gender classification.

considering a variety of identities, including gender and skin tone. Race is a social construction that changes meaning throughout time and geography, according to Buolamwini and Gebru, two Black women in the United States with varying skin tones.

According to sociologist Ellis Monk in The Cost of Colour, "some studies even suggest that within-race inequalities associated with skin tone among African Americans often rival or exceed what obtains between Blacks and whites as a whole." Consequently, Buolamwini and Gebru utilised the Fitzpatrick skin type classification system to conduct their analysis, rather than based on race sort photos into those with darker skin and those with lighter skin tones, and then compare the performance of commercial systems on each subset.

Intersectional testing is necessary to reveal the weaknesses of AI systems, as pointed out in the work of Buolamwini and Gebru. A prominent figure in critical race theory, Kimberlé Crenshaw, who popularised the word "intersectionality" in her work, emphasises the need to consider not only one but all of a person's identities but also the ways in which these interact with various power structures.

She frequently cites the case of Emma DeGraffenreid, who sued General Motors (GM) in 1976, claiming that the company discriminated against Black women. The plaintiffs were unsuccessful in their action because the courts reasoned that GM could not have discriminated against Black women since the company employs both men and women.

They neglected to mention that General Motors recruited women for secretarial roles but refused to hire Black individuals for the same roles. Additionally, GM only considered male candidates for factory jobs and employed males. So, it's clear that GM discriminated against Black women, but the judges missed the mark because they didn't use an intersectional perspective that considers gender and race. The biggest differences were found when the systems were analysed by both gender and skin type in the work of Buolamwini and Gebru. The ladies explain that their inspiration for disaggregating accuracy by gender and skin type came from their own experiences and from reading works on intersectionality.

Gender Stereotypes are Being Perpetuated by AI-Based Tools.

Following on from the last section's discussion of how police departments are making use of automated facial analysis tools that perform unequally across subgroups, this section demonstrates how certain tools, regardless of how "accurate" they may be, can perpetuate damaging gender stereotypes.

Many aspects of how AI systems are developed reflect societal perspectives on gender and ethnicity. Articles like Gender Recognition or Gender Reductionism by Hamidi et al. address this issue within the framework of automated gender recognition systems, such the ones investigated by Buolamwini and Gebru, and the damage they wreak, especially on the transgender population.

One example is the inherent assumption in the very nature of automatic gender recognition (AGR): that gender is a fixed notion that seldom undergoes cultural or temporal changes. The problem is that these methods don't always take into consideration the fact that gender is presented differently across cultures. Many times, data used to train gender classification algorithms does not include any transgender or non-binary people at all. Transgender people may have serious consequences as a result of AGR, which just labels photos as "male" or "female." This can lead to misgendering or even public outings. The 2014 National Transgender Discrimination Survey found that 56 percent of people who participated who were frequently treated differently because of their gender at work attempted suicide.23 Although the negative effects of AGR systems are well-documented, the practicality of these tools is frequently debatable [125-129].

The use of AGR in targeted advertising (such as displaying a product to people who are assumed to be female) is rather widespread. Subliminal signals about which objects are appropriate for males and which are appropriate for women run the risk of reinforcing existing preconceptions. Urban Outfitters, for instance, began tailoring its online experience to the genders of its most loyal consumers. Many consumers were against gender-based marketing and its associated practices, which led to the program's cancellation. Some consumers frequently purchased items that did not correspond to their assigned gender, while others were just against the idea of gender-based targeting.

One of the several ways in which AI perpetuates gender-based social prejudices and preconceptions is through automatic gender recognition systems. Commercial AI systems are clearly designed around gender stereotypes, from the images used to depict cyborgs to the names, voices, and mannerisms portrayed by speech recognition systems like Alexa and

Siri, which are intended to comply with a customer's every command. Letters from Amy Chambers:

From real-life examples like Alexa, Cortana, Holly, and Siri to fictional ones like Samantha in Her, Joi in Blade Runner 2049, and Marvel's AIs, FRIDAY in Avengers: Infinity War, and Karen in Spider-Man: Homecoming, virtual assistants are becoming more commonplace and popular. From SatNav to Siri, all of these titles suggest that people expect female voices for virtual assistants. This just serves to solidify preconceived notions, biases, and gender norms regarding AI's potential in the future.25

How does it affect youngsters whose homes are populated with plainly subordinate feminised voices? The usage of AI systems in humiliating ways towards women is already prevalent, even without the explicit embedding of gendered names and voices. One example is the weaponization of generative adversarial networks (GANs), which are models used for generating pictures among other things, against women. The use of GANs to produce "deep fakes" allows for the creation of pornographic content featuring the unconsented use of stock images of women taken from social media.

Gap in AI and the Erasing of Marginalised Perspectives

There is nothing new about AI's history of being used as a weapon against particular groups or to uphold the status quo while supposedly freeing the powerless. Mitchell et al. draw comparisons to fields where goods were developed for a homogeneous population in Model Cards for Model Reporting. In the past, things that are designed and tested on a homogeneous group of people tend to work best for that group. For example, cars were crash tested on dummies with prototypical adult "male" characteristics, which led to accidents that killed more women and children than males. Another example is clinical trials that excluded many groups of people, which resulted in drugs that either didn't work or had far-reaching negative effects on women. According to an article published in Newsweek in 2018 that features scientist Charles Rotimi, "By 2009, less than 1 [130-134]

Despite the fact that "African genomes are the most diverse of any on the planet," only a small percentage of the hundreds of genome investigations included Africans. This underrepresentation has serious consequences, including the ineffective development of next-generation personalised drugs for people of African descent and the possibility of scientists drawing incorrect conclusions based on homogenous data due to overfitting. For example, they may find mutations that are common in Africans but rare in European genomes.

The evolution and future of AI appears to be following a pattern seen in many other fields. Ali Alkhatib draws connections between anthropology and the current state of artificial intelligence research, which he says has hurt marginalised communities. While anthropologists, similar to modern computer scientists, were ensnared in lucrative funding deals, he notes that the government, and the military in particular, were interested in their work. According to Alkhatib, "the danger of aligning our work with existing power is the further subjugation and marginalisation of the communities we ostensibly seek to understand" (emphasis added), and "[t]he voices, opinions, and needs of disempowered

stakeholders are being ignored today in favour of stakeholders with power, money, and influence—as they have been historically." We were asked to do something that seemed reasonable at the time some have criticised the rapid assimilation of the ideas of a group of marginalised individuals who risked their jobs to bring attention to the ways in which artificial intelligence (AI) may harm their communities. This year and the next both Stanford University and Massachusetts Institute of Technology (MIT) have announced interdisciplinary initiatives focused on artificial intelligence (AI) ethics. These initiatives will receive multi-billion dollar funding from various industries and venture capitalists. At the opening ceremonies of both universities, notorious war criminals such as Henry Kissinger were featured.

Like what happened in political anthropology, these well-funded projects put powerful entities at the centre, who have not dealt with AI ethics and, in many instances, have a vested interest in spreading immoral AI practices, while excluding the views of the marginalised people they profess to help. Ethical discourse has recently surpassed that of diversity and inclusion as a buzzword. The Human Centred AI effort at Stanford University was launched with a goal statement that "[t]he creators of AI have to represent the world." However, when it was first introduced, out of 121 professors from various fields, there were zero Black faculty members mentioned on the website.

A number of organisations are vying to be heard above all others when it comes to artificial intelligence. Amazon and the National Science Foundation (NSF) have launched a combined grant to support research on fairness, while the companies provide computerised face analysis technologies to law enforcement that may have systemic flaws. In an effort to debunk the findings of two Black women who had demonstrated prejudice in their automated face analysis tool, Amazon's upper management published a string of blog postings just before the firm and the NSF announced their combined funding.

While knowingly undermining the professional lives of two women from underrepresented groups and continuing to offer unregulated automated face analysis products to the police areas hit hard by Amazon's goods, the corporation announces a collaborative partnership with the National Science Foundation (NSF) in an apparent effort to address issues of justice. This event exemplifies the capture-and-neutralize technique, which seeks to undermine members of historically oppressed groups while claiming to speak in terms of diversity, inclusion, ethics, and justice in order to forward the corporate agenda.

After the fact, 78 scientists, including Yoshua Bengio, who won the 2019 Turing award, issued a letter to Amazon demanding that the company stop selling Rekognition to law enforcement agencies and outlining the truth about the misrepresentations made by Amazon personnel. The original authors were Buolamwini and Raji's collaborators, the Black lady Timnit Gebru, and Margaret Mitchell. This activity reveals a schism between the risk-takers in the ethics and justice movement and the center-seated, institutionalised activists at places like MIT and Stanford. Many in the academic world persist in publishing articles and doing abstract research on artificial intelligence and ethics, despite the fact that two Black women brought attention to the systemic problems with Amazon's goods and a third brought together a coalition of AI specialists to bolster their argument. The terms ethics and fairness have

entered the vernacular of machine learning as "hot" topics in 2019, and many in the field use them interchangeably. While many in the sector claim to be striving to make technology more "fair," very few actually challenge the existence of certain technologies and even fewer put the views of individuals most affected by these technologies front and centre. For instance, in 2018, at a premier machine learning conference, at least seven of the nine organisers discussed AI33's ethical, societal, and governance concerns.

White was the theme of the Neural Information Processing Systems (NeurIPS) conference. The field does more harm than good when it appropriates the suffering of marginalised communities, appropriates their language to describe their struggle, and then uses it to further the careers of individuals from more powerful communities. The present trend of excluding certain groups in favour of influential interests, who have either never given AI ethics any thought beyond the abstract or have only been compelled to do so due to the efforts of members of disadvantaged communities like Raji and Buolamwini, demonstrates that the movement for AI ethics, transparency, accountability, and fairness is heading down the path of "parachute science" similar to other fields that came before it. Author Ali Alkhatib states:

Computer scientists have completely disregarded the lessons taught by other disciplines, and as a result, we are engaging in the same kinds of fundamentally problematic and ethically unacceptable connections that other disciplines might have cautioned us against, and even attempted to do the same. By identifying methods to mould indigenous cultures to suit colonial powers, political anthropologists in the 1940s "tended to take colonial domination itself for granted" and essentially shaped themselves as a means to further the hegemonic sway of colonialism.

Right now, the field of artificial intelligence ethics is rife with this colonial mindset. The phrase "parachute research" or "helicopter research" has been used to describe scientists who "parachute in" to various underprivileged areas, collect data, surveys, or specimens as needed, and then depart. As Joy Buolamwini pointed out, this kind of study treats communities like caged curiosities, which further marginalises people without alleviating their misery, and it also leads to poor science since researchers don't grasp the context. Instead than performing extensive study, the greatest approach to help a community is to provide a voice to people who are already trying to improve it. Thus, researchers taking AI ethics seriously should make sure that the motivation and introduction paragraphs of their articles put the people whose stories they are examining at the centre. Rather than utilising them to further their own careers and solicit funding from venture capitalists, they should strive to make room for the oppressed and give amplification to its voices.

Choosing Who Gets a Seat at the Table is the First Step in Designing Ethical AI.

While the idea of ethical AI is not new, it is in critical need of a comprehensive strategy. Who is developing the technology, defining the purposes and principles of AI, and being at the table are all important first steps. Therefore, it's clear that a strategy that is developed, spearheaded, and promoted by those in positions of global authority would be unsuccessful. The ideals encoded in technology are determined by their creators.

For example, would we have created automated gender recognition systems that hurt transgender people and promote sexist gender norms if cisgender straight males did not control the computer industry? Were they more prevalent in AI research and development, what kinds of tools would we have created for them instead? Would today's algorithms that disproportionately disenfranchise Black and Brown communities in the US exist if the primary feedback for developing AI utilised in the criminal justice system had originated from individuals who were falsely accused of a crime and faced with high cash bail as a result of risk assessment scores? In the event if most studies examining AI were would we be developing drones that can detect and apprehend individuals of interest if they were financed by healthcare-focused government agency instead of military-oriented ones like DARPA?

An instance where Facebook Translate interpreted an Arabic word as "hurt them" in English or "attack them" in Hebrew—leading to the arrest of a Palestinian—illustrates the systemic problems in action. Releasing him after confirming that he had written "good morning," Israeli authorities reportedly did not bother to examine the original Arabic version before detaining the man, according to Ha'aretz. These events occurred as a result of a multitude of causes.

First of all, it's hard to believe that this kind of translation error would have happened if Palestinians and other Arabic speakers had dominated the profession of language translation. The majority of machine learning and NLP experts are from Western countries, so it's no surprise that Google and Facebook's translation tools are most effective when translating from English to Western languages like French. The majority of the corpora and articles produced in this field centre on languages that are highly valued by researchers, funders, and Silicon Valley giants like Google and Facebook. So, it should come as no surprise that the community and scholars are heavily skewed towards finding solutions to translation issues across languages like English and French.

Furthermore, the social biases inherent in the training data are incorporated into natural language processing techniques. While many countries without a large Arab population view Arab speakers with suspicion, to the extent that a math professor was detained on a plane after a fellow passenger mistook his mathematical writings for Arabic, the majority of people who speak English, French, or another western language do not share this view. For this reason, it's improbable that a translation error between French and English, for example, would imply anything as offensive as "attack them."

There is a lot of evidence that NLP tools have gender and racial biases. Word embeddings trained on corpora like novels or newspaper articles display behaviours that align with the social biases encoded in the training data, as demonstrated by Bolukbasi et al. and Caliskan et al. One study by Bolukbasi et al. discovered that word embeddings could be used to make comparisons; for instance, embeddings trained on Google News could finish the sentence "man is to computer programmer as woman is to X" with "homemaker." Another study by Caliskan et al. showed that, in word embeddings trained from web crawling, African American names are more commonly linked to negative ideas like illness, while European American names are more commonly linked to positive ones relate to positive ideas like

flowers.40 Dixon et al. have demonstrated that sentiment analysis systems frequently label texts on LGBTQ+ people as negative. The fact that the gaffe was translated as "attack them" is hardly shocking considering the widespread Western stereotype of Muslims as terrorists. People have a propensity to over-trust automated tools, which is highlighted by this instance. Scientists from Georgia Tech University conducted an experiment to test people's faith in robots. The results indicated that people were willing to follow the robots along paths that were obviously inconvenient in order to get to what appeared to be a burning structure. Authorities trusted the translation algorithm and did not bother to first read the original text before detaining the Palestinian for his "good morning" message.

As we examine what transpired, we cannot turn a blind eye to the systemic factors that were involved. Because Palestinians are oppressed, not only is there a higher chance of translation errors involving Palestinian Arabic dialects, but those that do occur are likely to have a greater negative impact on Palestinians. Because of the nature of the mistake it made, this translation system was just as damaging as the one that happened with Google Photos and the "gorilla" pair. There were just as many cases of white individuals being mistaken for whales as there were of black people being mistaken for gorillas in the Google Photos incident. Unlike the historical depictions of Black people as monkeys or gorillas, the meaning of being mistaken for a whale does not stem from racist and discriminatory practices. The structure of algorithmic gibberish will veer hazily towards that of historical biases, even if one could persuade themselves that algorithms occasionally spit forth gibberish.

Problems that some groups in natural language processing, computer vision, and machine learning focus on do not tackle the most pressing issues encountered by people who do not belong to that dominant group because of the underrepresentation of other groups in these fields. Actually, it may make these communities even more marginalised. If the preponderance of surveillance and automated technologies did not make Palestinians more susceptible to such treatment, the mistranslation of "good morning" into "attack them" would not have had such severe repercussions. The likelihood of monitoring and interaction with automated systems is disproportionately high for Black people and other oppressed populations in the US. Those already living on the margins may bear the brunt of the systemic mistakes that include prejudice and stereotyping, which arise from the datasets utilised and the demographic composition of those involved in this field. Proposals like the severe vetting initiative by the reveal the power imbalance and the disproportionate impact of systematic mistakes on marginalised communities.

Yet another terrifying and troublesome US agency: Immigration and Customs Enforcement (ICE). The 2018 plan calls for ICE to team up with tech companies to scour people's social media accounts for signs of potential terrorism, good citizenship, or appropriate immigration status. The goal is to use automated tools to determine whether people are likely to be good citizens or not. Even though science fiction films like Minority Report and TV shows like Black Mirror have warned us about the dangers of trying to predict someone's future criminal behaviour, the idea is much more terrifying when we consider the systematic errors that would be introduced by the automated tools that would be employed for these analyses. Tools based on computer vision and natural language processing tend to make more mistakes

and have more prejudices against marginalised people, who are also more likely to be targeted by organisations like ICE.

As encouraging as it sounds, 54 prominent AI researchers have spoken out against the severe screening initiative45. Nevertheless, the campaign is still going strong, and there are just a handful of AI developers that are actively fighting against these kinds of suggestions. It is already challenging for the second group to care since marginalised people are so underrepresented there. The minority tax already hits certain groups hard, and those who do speak out come from communities that bear a disproportionate share of the cost to diversify and educate their members. Science and engineering curricula must abandon "the view from nowhere" if they are to remain relevant.

Involvement of people from many backgrounds and regions is essential if we are to develop technology that benefits society as a whole. Who develops and uses technology in the future will determine who benefits from it. Several features of this technology reflect the sexist and racist beliefs of the culture that created it, as we have shown. Efforts to guide AI in a positive direction need scientists to acknowledge that their work is inextricably linked to global geopolitical dynamics, and that meritocracy and impartiality do not exist. Science, according to feminists, is all about discovering objective "truths" apart from human experience. This "view from nowhere" has been a point of contention for a long time. This, along with the concept of meritocracy, is the prevailing paradigm in the male-dominated fields of science and technology. Taking the place of "View from Nowhere," Sarah Marie Stitzlein penned:

Most feminists and even some pragmatists believe that putting subjects and objects of knowledge on equal ground is necessary for acknowledging that both are historically and politically situated. As a means of attending to the rights and welfare of both other subjects and the objects of scientific investigation, impartiality must be upheld when this is carried out. Accordingly, objectivity is attained when and to the degree that accountability in investigation is satisfied and enhanced. Therefore, scientists ought to own up to the political underpinnings of their work and take responsibility for the outcomes of their efforts. At its core, objectivity as a notion presupposes connections in among subjects, things, and research endeavours instead of teaching students about science and technology in a vacuum, classrooms should demonstrate how real-world factors have shaped these fields. The Ethical Nature of Cryptography by Phillip according to Rogaway, the cryptography community has failed with the proliferation of mass monitoring. He goes over a number of cryptographic proposals and explains how the field's high abstraction and failure to take into consideration the geopolitical environment have led to schemes that benefit the powerful at the expense of the powerless. After mentioning the physicists' push for nuclear disarmament, he asks cryptographers to join the chorus of scientists who are speaking out against the abuse of their technology.

Conclusion

Similarly, researchers in artificial intelligence should study the applications of their technology, challenge the current trajectory of institutions, and collaborate with experts from many fields to get insight into their methods. Researchers interested in AI ethics, justice,

accountability, transparency, and demographics should work together across disciplines, regions, institutions, and socioeconomic lines to make a difference for underrepresented groups. Researchers and practitioners, as well as the educational system, must radically alter their mindset and abandon the myth of meritocracy and "the view from nowhere" if we are to create AI that does not further marginalise people who have already been and are being marginalised.

References

[1] Yanamala, A.K.Y., S. Suryadevara, and V.D.R. Kalli. (2024) Balancing innovation and privacy: The intersection of data protection and artificial intelligence. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 15(1): 1-43.

[2] Yanamala, A.K.Y. and S. Suryadevara. (2024) Navigating data protection challenges in the era of artificial intelligence: A comprehensive review. Revista de Inteligencia Artificial en Medicina. 15(1): 113-146.

[3] Yanamala, A.K.Y. and S. Suryadevara. (2024) Emerging Frontiers: Data Protection Challenges and Innovations in Artificial Intelligence. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 15: 74-102.

[4] Yanamala, A.K.Y. (2024) Emerging challenges in cloud computing security: A comprehensive review. International Journal of Advanced Engineering Technologies and Innovations. 1(4): 448-479.

[5] Yanamala, A.K.Y. (2024) Optimizing data storage in cloud computing: techniques and best practices. International Journal of Advanced Engineering Technologies and Innovations. 1(3): 476-513.

[6] Yanamala, A.K.Y., S. Suryadevara, and V.D.R. Kalli. (2023) Evaluating the impact of data protection regulations on AI development and deployment. International Journal of Advanced Engineering Technologies and Innovations. 1(01): 319-353.

[7] Yanamala, A.K.Y. and S. Suryadevara. (2023) Advances in Data Protection and Artificial Intelligence: Trends and Challenges. International Journal of Advanced Engineering Technologies and Innovations. 1(01): 294-319.

[8] Yanamala, A.K.Y. (2023) Secure and private AI: Implementing advanced data protection techniques in machine learning models. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 14(1): 105-132.

[9] Yanamala, A.K.Y. and S. Suryadevara. (2022) Cost-Sensitive Deep Learning for Predicting Hospital Readmission: Enhancing Patient Care and Resource Allocation. International Journal of Advanced Engineering Technologies and Innovations. 1(3): 56-81.

[10] Yanamala, A.K.Y. and S. Suryadevara. (2022) Adaptive Middleware Framework for Context-Aware Pervasive Computing Environments. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 13(1): 35-57.

[11] Suryadevara, S., A.K.Y. Yanamala, and V.D.R. Kalli. (2021) Enhancing Resource-Efficiency and Reliability in Long-Term Wireless Monitoring of Photoplethysmographic Signals. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 12(1): 98-121.

[12] Suryadevara, S. and A.K.Y. Yanamala. (2021) A Comprehensive Overview of Artificial Neural Networks: Evolution, Architectures, and Applications. Revista de Inteligencia Artificial en Medicina. 12(1): 51-76.

[13] Woldaregay, A.Z., B. Yang, and E.A. Snekkenes. Data-Driven and Artificial Intelligence (AI) Approach for Modelling and Analyzing Healthcare Security Practice: A Systematic. in Intelligent Systems and Applications: Proceedings of the 2020 Intelligent Systems Conference (IntelliSys) Volume 1. 2020. Springer Nature.

[14] Suryadevara, S. and A.K.Y. Yanamala. (2020) Patient apprehensions about the use of artificial intelligence in healthcare. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 11(1): 30-48.

[15] Suryadevara, S. and A.K.Y. Yanamala. (2020) Fundamentals of Artificial Neural Networks: Applications in Neuroscientific Research. Revista de Inteligencia Artificial en Medicina. 11(1): 38-54.

[16] Chirra, B.R. (2024) Revolutionizing Cybersecurity: The Role of AI in Advanced Threat Detection Systems. International Journal of Advanced Engineering Technologies and Innovations. 1(4): 480-504.

[17] Chirra, B.R. (2024) Predictive AI for Cyber Risk Assessment: Enhancing Proactive Security Measures. International Journal of Advanced Engineering Technologies and Innovations. 1(4): 505-527.

[18] Chirra, B. (2024) Enhancing Cloud Security through Quantum Cryptography for Robust Data Transmission. Revista de Inteligencia Artificial en Medicina. 15(1): 752-775.

[19] Chirra, B. (2024) Leveraging Blockchain to Strengthen Information Security in IoT Networks. Revista de Inteligencia Artificial en Medicina. 15(1): 726-751.

[20] Chirra, B. (2024) Revolutionizing Cybersecurity with Zero Trust Architectures: A New Approach for Modern Enterprises. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 15(1): 586-612.

[21] Chirra, B.R. (2023) AI-Powered Identity and Access Management Solutions for Multi-Cloud Environments. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 14(1): 523-549.

[22] Chirra, B.R. (2023) Enhancing Healthcare Data Security with Homomorphic Encryption: A Case Study on Electronic Health Records (EHR) Systems. Revista de Inteligencia Artificial en Medicina. 14(1): 549-59.

[23] Chirra, B.R. (2023) Advancing Cyber Defense: Machine Learning Techniques for NextGeneration Intrusion Detection. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 14(1): 550-573.

[24] Chirra, B.R. (2023) Advancing Real-Time Malware Detection with Deep Learning for Proactive Threat Mitigation. International Journal of Advanced Engineering Technologies and Innovations. 1(01): 274-396.

[25] Chirra, B.R. (2023) Securing Edge Computing: Strategies for Protecting Distributed Systems and Data. International Journal of Advanced Engineering Technologies and Innovations. 1(01): 354-373.

[26] Chirra, B.R. (2022) AI-Driven Vulnerability Assessment and Mitigation Strategies for CyberPhysical Systems. Revista de Inteligencia Artificial en Medicina. 13(1): 471-493.

[27] Chirra, B.R. (2022) Strengthening Cybersecurity with Behavioral Biometrics: Advanced Authentication Techniques. International Journal of Advanced Engineering Technologies and Innovations. 1(3): 273-294.

[28] Chirra, B.R. (2022) Dynamic Cryptographic Solutions for Enhancing Security in 5G Networks. International Journal of Advanced Engineering Technologies and Innovations. 1(3): 249-272.

[29] Chirra, B.R. (2022) Ensuring GDPR Compliance with AI: Best Practices for Strengthening Information Security. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 13(1): 441-462.

[30] Chirra, B.R. (2021) Leveraging Blockchain for Secure Digital Identity Management: Mitigating Cybersecurity Vulnerabilities. Revista de Inteligencia Artificial en Medicina. 12(1): 462-482.

[31] Chirra, B.R. (2021) Intelligent Phishing Mitigation: Leveraging AI for Enhanced Email Security in Corporate Environments. International Journal of Advanced Engineering Technologies and Innovations. 1(2): 178-200.

[32] Chirra, B.R. (2021) Enhancing Cyber Incident Investigations with AI-Driven Forensic Tools. International Journal of Advanced Engineering Technologies and Innovations. 1(2): 157-177.

[33] Chirra, B.R. (2021) AI-Driven Security Audits: Enhancing Continuous Compliance through Machine Learning. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 12(1): 410-433.

[34] Chirra, B.R. (2020) AI-Driven Fraud Detection: Safeguarding Financial Data in Real-Time. Revista de Inteligencia Artificial en Medicina. 11(1): 328-347.

[35] Chirra, B.R. (2020) Advanced Encryption Techniques for Enhancing Security in Smart Grid Communication Systems. International Journal of Advanced Engineering Technologies and Innovations. 1(2): 208-229.

[36] Goriparthi, R.G. and S. Luqman. (2024) Deep Learning Architectures for Real-Time Image Recognition: Innovations and Applications. Revista de Inteligencia Artificial en Medicina. 15(1): 880-907.

[37] Goriparthi, R.G. (2024) Adaptive Neural Networks for Dynamic Data Stream Analysis in Real-Time Systems. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 15(1): 689-709.

[38] Goriparthi, R.G. (2024) Hybrid AI Frameworks for Edge Computing: Balancing Efficiency and Scalability. International Journal of Advanced Engineering Technologies and Innovations. 2(1): 110-130.

[39] Goriparthi, R.G. (2024) AI-driven predictive analytics for autonomous systems: A machine learning approach. Revista de Inteligencia Artificial en Medicina. 15(1): 843-879.

[40] Goriparthi, R.G. (2024) Reinforcement Learning in IoT: Enhancing Smart Device Autonomy through AI. Computing. 2: 89-109.

[41] Goriparthi, R.G. (2023) AI-Augmented Cybersecurity: Machine Learning for Real-Time Threat Detection. Revista de Inteligencia Artificial en Medicina. 14(1): 576-594.

[42] Goriparthi, R.G. (2023) AI-Enhanced Data Mining Techniques for Large-Scale Financial Fraud Detection. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 14(1): 674-699.

[43] Goriparthi, R.G. (2023) Leveraging AI for Energy Efficiency in Cloud and Edge Computing Infrastructures. International Journal of Advanced Engineering Technologies and Innovations. 1(01): 494-517.

[44] Goriparthi, R.G. (2022) Interpretable Machine Learning Models for Healthcare Diagnostics: Addressing the Black-Box Problem. Revista de Inteligencia Artificial en Medicina. 13(1): 508-534.

[45] Goriparthi, R.G. (2022) Deep Reinforcement Learning for Autonomous Robotic Navigation in Unstructured Environments. International Journal of Advanced Engineering Technologies and Innovations. 1(3): 328-344.

[46] Goriparthi, R.G. (2022) AI in Smart Grid Systems: Enhancing Demand Response through Machine Learning. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 13(1): 528-549.

[47] Goriparthi, R.G. (2022) AI-Powered Decision Support Systems for Precision Agriculture: A Machine Learning Perspective. International Journal of Advanced Engineering Technologies and Innovations. 1(3): 345-365.

[48] Goriparthi, R.G. (2021) AI-Driven Natural Language Processing for Multilingual Text Summarization and Translation. Revista de Inteligencia Artificial en Medicina. 12(1): 513-535.

[49] Goriparthi, R.G. (2021) AI and Machine Learning Approaches to Autonomous Vehicle Route Optimization. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 12(1): 455-479.

[50] Goriparthi, R.G. (2021) Scalable AI Systems for Real-Time Traffic Prediction and Urban Mobility Management. International Journal of Advanced Engineering Technologies and Innovations. 1(2): 255-278.

[51] Goriparthi, R.G. (2020) AI-Driven Automation of Software Testing and Debugging in Agile Development. Revista de Inteligencia Artificial en Medicina. 11(1): 402-421.

[52] Goriparthi, R.G. (2020) Neural Network-Based Predictive Models for Climate Change Impact Assessment. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 11(1): 421-421.

[53] Reddy, V.M. and L.N. Nalla. (2024) Real-time Data Processing in E-commerce: Challenges and Solutions. International Journal of Advanced Engineering Technologies and Innovations. 1(3): 297-325.

[54] Reddy, V.M. and L.N. Nalla. (2024) Leveraging Big Data Analytics to Enhance Customer Experience in E-commerce. Revista Espanola de Documentacion Cientifica. 18(02): 295-324.

[55] Reddy, V.M. and L.N. Nalla. (2024) Optimizing E-Commerce Supply Chains Through Predictive Big Data Analytics: A Path to Agility and Efficiency. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 15(1): 555-585.

[56] Reddy, V.M. and L.N. Nalla. (2024) Personalization in E-Commerce Marketing: Leveraging Big Data for Tailored Consumer Engagement. Revista de Inteligencia Artificial en Medicina. 15: 691-725.

[57] Nalla, L.N. and V.M. Reddy. (2024) AI-driven big data analytics for enhanced customer journeys: A new paradigm in e-commerce. International Journal of Advanced Engineering Technologies and Innovations. 1(2): 719-740.

[58] Reddy, V.M. and L.N. Nalla. (2023) The Future of E-commerce: How Big Data and AI are Shaping the Industry. International Journal of Advanced Engineering Technologies and Innovations. 1(03): 264-281.

[59] Reddy, V.M. (2023) Data Privacy and Security in E-commerce: Modern Database Solutions. International Journal of Advanced Engineering Technologies and Innovations. 1(03): 248-263.

[60] Reddy, V.M. and L.N. Nalla. (2022) Enhancing Search Functionality in E-commerce with Elasticsearch and Big Data. International Journal of Advanced Engineering Technologies and Innovations. 1(2): 37-53.

[61] Nalla, L.N. and V.M. Reddy. (2022) SQL vs. NoSQL: Choosing the Right Database for Your Ecommerce Platform. International Journal of Advanced Engineering Technologies and Innovations. 1(2): 54-69.

[62] Reddy, V.M. and L.N. Nalla. (2021) Harnessing Big Data for Personalization in E-commerce Marketing Strategies. Revista Espanola de Documentacion Cientifica. 15(4): 108-125.

[63] Reddy, V.M. (2021) Blockchain Technology in E-commerce: A New Paradigm for Data Integrity and Security. Revista Espanola de Documentacion Cientifica. 15(4): 88-107.

[64] Nalla, L.N. and V.M. Reddy. (2021) Scalable Data Storage Solutions for High-Volume E-commerce Transactions. International Journal of Advanced Engineering Technologies and Innovations. 1(4): 1-16.

[65] Reddy, V.M. and L.N. Nalla. (2020) The Impact of Big Data on Supply Chain Optimization in Ecommerce. International Journal of Advanced Engineering Technologies and Innovations. 1(2): 1-20.

[66] Nalla, L.N. and V.M. Reddy. (2020) Comparative Analysis of Modern Database Technologies in Ecommerce Applications. International Journal of Advanced Engineering Technologies and Innovations. 1(2): 21-39.

[67] Nalla, L.N. and V.M. Reddy. Machine Learning and Predictive Analytics in E-commerce: A Data-driven Approach.

[68] Nalla, L.N. and V.M. Reddy. (2024) AI-Driven Big Data Analytics for Enhanced Customer Journeys: A New Paradigm in E-Commerce. International Journal of Advanced Engineering Technologies and Innovations. 1: 719-740.

[69] Chirra, D.R. (2024) Blockchain-Integrated IAM Systems: Mitigating Identity Fraud in Decentralized Networks. International Journal of Advanced Engineering Technologies and Innovations. 2(1): 41-60.

[70] Chirra, D.R. (2024) Advanced Threat Detection and Response Systems Using Federated Machine Learning in Critical Infrastructure. International Journal of Advanced Engineering Technologies and Innovations. 2(1): 61-81.

[71] Chirra, D.R. (2024) AI-Augmented Zero Trust Architectures: Enhancing Cybersecurity in Dynamic Enterprise Environments. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 15(1): 643-669.

[72] Chirra, D.R. (2024) Quantum-Safe Cryptography: New Frontiers in Securing Post-Quantum Communication Networks. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 15(1): 670-688.

[73] Chirra, D.R. (2024) Secure Data Sharing in Multi-Cloud Environments: A Cryptographic Framework for Healthcare Systems. Revista de Inteligencia Artificial en Medicina. 15(1): 821-843.

[74] Chirra, D.R. (2023) AI-Based Threat Intelligence for Proactive Mitigation of Cyberattacks in Smart Grids. Revista de Inteligencia Artificial en Medicina. 14(1): 553-575.

[75] Chirra, D.R. (2023) The Role of Homomorphic Encryption in Protecting Cloud-Based Financial Transactions. International Journal of Advanced Engineering Technologies and Innovations. 1(01): 452-472.

[76] Chirra, D.R. (2023) Real-Time Forensic Analysis Using Machine Learning for Cybercrime Investigations in E-Government Systems. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 14(1): 618-649.

[77] Chirra, D.R. (2023) Towards an AI-Driven Automated Cybersecurity Incident Response System. International Journal of Advanced Engineering Technologies and Innovations. 1(01): 429-451.

[78] Chirra, D.R. (2023) Deep Learning Techniques for Anomaly Detection in IoT Devices: Enhancing Security and Privacy. Revista de Inteligencia Artificial en Medicina. 14(1): 529-552.

[79] Chirra, D.R. (2022) Collaborative AI and Blockchain Models for Enhancing Data Privacy in IoMT Networks. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 13(1): 482-504.

[80] Chirra, D.R. (2022) Secure Edge Computing for IoT Systems: AI-Powered Strategies for Data Integrity and Privacy. Revista de Inteligencia Artificial en Medicina. 13(1): 485-507.

[81] Chirra, D.R. (2022) AI-Powered Adaptive Authentication Mechanisms for Securing Financial Services Against Cyber Attacks. International Journal of Advanced Engineering Technologies and Innovations. 1(3): 303-326.

[82] Chirra, D.R. (2022) AI-Driven Risk Management in Cybersecurity: A Predictive Analytics Approach to Threat Mitigation. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 13(1): 505-527.

[83] Chirra, D.R. (2021) Mitigating Ransomware in Healthcare: A Cybersecurity Framework for Critical Data Protection. Revista de Inteligencia Artificial en Medicina. 12(1): 495-513.

[84] Chirra, D.R. (2021) The Impact of AI on Cyber Defense Systems: A Study of Enhanced Detection and Response in Critical Infrastructure. International Journal of Advanced Engineering Technologies and Innovations. 1(2): 221-236.

[85] Chirra, D.R. (2021) AI-Enabled Cybersecurity Solutions for Protecting Smart Cities Against Emerging Threats. International Journal of Advanced Engineering Technologies and Innovations. 1(2): 237-254.

[86] Chirra, D.R. (2021) Securing Autonomous Vehicle Networks: AI-Driven Intrusion Detection and Prevention Mechanisms. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 12(1): 434-454.

[87] Chirra, D.R. (2020) AI-Based Real-Time Security Monitoring for Cloud-Native Applications in Hybrid Cloud Environments. Revista de Inteligencia Artificial en Medicina. 11(1): 382-402.

[88] Chirra, D.R. (2020) Next-Generation IDS: AI-Driven Intrusion Detection for Securing 5G Network Architectures. International Journal of Advanced Engineering Technologies and Innovations. 1(2): 230-245.

[89] Gadde, H. (2024) AI-Powered Fault Detection and Recovery in High-Availability Databases. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 15(1): 500-529.

[90] Gadde, H. (2024) AI-Driven Data Indexing Techniques for Accelerated Retrieval in Cloud Databases. Revista de Inteligencia Artificial en Medicina. 15(1): 583-615.

[91] Gadde, H. (2024) AI-Augmented Database Management Systems for Real-Time Data Analytics. Revista de Inteligencia Artificial en Medicina. 15(1): 616-649.

[92] Gadde, H. (2024) Optimizing Transactional Integrity with AI in Distributed Database Systems. International Journal of Advanced Engineering Technologies and Innovations. 1(2): 621-649.

[93] Gadde, H. (2024) Intelligent Query Optimization: AI Approaches in Distributed Databases. International Journal of Advanced Engineering Technologies and Innovations. 1(2): 650-691.

[94] Gadde, H. (2023) Leveraging AI for Scalable Query Processing in Big Data Environments. International Journal of Advanced Engineering Technologies and Innovations. 1(02): 435-465.

[95] Gadde, H. (2023) AI-Driven Anomaly Detection in NoSQL Databases for Enhanced Security. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 14(1): 497-522.

[96] Gadde, H. (2023) Self-Healing Databases: AI Techniques for Automated System Recovery. International Journal of Advanced Engineering Technologies and Innovations. 1(02): 517-549.

[97] Gadde, H. (2023) AI-Based Data Consistency Models for Distributed Ledger Technologies. Revista de Inteligencia Artificial en Medicina. 14(1): 514-545.

[98] Gadde, H. (2022) AI in Dynamic Data Sharding for Optimized Performance in Large Databases. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 13(1): 413-440.

[99] Gadde, H. (2022) AI-Enhanced Adaptive Resource Allocation in Cloud-Native Databases. Revista de Inteligencia Artificial en Medicina. 13(1): 443-470.

[100] Gadde, H. (2022) Integrating AI into SQL Query Processing: Challenges and Opportunities. International Journal of Advanced Engineering Technologies and Innovations. 1(3): 194-219.

[101] Gadde, H. (2022) Federated Learning with AI-Enabled Databases for Privacy-Preserving Analytics. International Journal of Advanced Engineering Technologies and Innovations. 1(3): 220-248.

[102] Gadde, H. (2021) Secure Data Migration in Multi-Cloud Systems Using AI and Blockchain. International Journal of Advanced Engineering Technologies and Innovations. 1(2): 128-156.

[103] Gadde, H. (2021) AI-Driven Predictive Maintenance in Relational Database Systems. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 12(1): 386-409.

[104] Gadde, H. (2021) AI-Powered Workload Balancing Algorithms for Distributed Database Systems. Revista de Inteligencia Artificial en Medicina. 12(1): 432-461.

[105] Gadde, H. (2020) AI-Assisted Decision-Making in Database Normalization and Optimization. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 11(1): 230-259.

[106] Gadde, H. (2020) AI-Enhanced Data Warehousing: Optimizing ETL Processes for Real-Time Analytics. Revista de Inteligencia Artificial en Medicina. 11(1): 300-327.

[107] Gadde, H. (2020) Improving Data Reliability with AI-Based Fault Tolerance in Distributed Databases. International Journal of Advanced Engineering Technologies and Innovations. 1(2): 183-207.

[108] Gadde, H. (2019) Integrating AI with Graph Databases for Complex Relationship Analysis. International Journal of Advanced Engineering Technologies and Innovations. 1(2): 294-314.

[109] Maddireddy, B.R. and B.R. Maddireddy. (2024) Advancing Threat Detection: Utilizing Deep Learning Models for Enhanced Cybersecurity Protocols. Revista Espanola de Documentacion Cientifica. 18(02): 325-355.

[110] Maddireddy, B.R. and B.R. Maddireddy. (2024) The Role of Reinforcement Learning in Dynamic Cyber Defense Strategies. International Journal of Advanced Engineering Technologies and Innovations. 1(2): 267-292.

[111] Maddireddy, B.R. and B.R. Maddireddy. (2024) A Comprehensive Analysis of Machine Learning Algorithms in Intrusion Detection Systems. Journal Environmental Sciences And Technology. 3(1): 877-891.

[112] Maddireddy, B.R. and B.R. Maddireddy. (2024) Neural Network Architectures in Cybersecurity: Optimizing Anomaly Detection and Prevention. International Journal of Advanced Engineering Technologies and Innovations. 1(2): 238-266.

[113] Maddireddy, B.R. and B.R. Maddireddy. (2023) Automating Malware Detection: A Study on the Efficacy of AI-Driven Solutions. Journal Environmental Sciences And Technology. 2(2): 111-124.

[114] Maddireddy, B.R. and B.R. Maddireddy. (2023) Enhancing Network Security through AI-Powered Automated Incident Response Systems. International Journal of Advanced Engineering Technologies and Innovations. 1(02): 282-304.

[115] Maddireddy, B.R. and B.R. Maddireddy. (2023) Adaptive Cyber Defense: Using Machine Learning to Counter Advanced Persistent Threats. International Journal of Advanced Engineering Technologies and Innovations. 1(03): 305-324.

[116] Maddireddy, B.R. and B.R. Maddireddy. (2022) Real-Time Data Analytics with AI: Improving Security Event Monitoring and Management. Unique Endeavor in Business & Social Sciences. 1(2): 47-62.

[117] Maddireddy, B.R. and B.R. Maddireddy. (2022) Blockchain and AI Integration: A Novel Approach to Strengthening Cybersecurity Frameworks. Unique Endeavor in Business & Social Sciences. 5(2): 46-65.

[118] Maddireddy, B.R. and B.R. Maddireddy. (2022) AI-Based Phishing Detection Techniques: A Comparative Analysis of Model Performance. Unique Endeavor in Business & Social Sciences. 1(2): 63-77.

[119] Maddireddy, B.R. and B.R. Maddireddy. (2022) Cybersecurity Threat Landscape: Predictive Modelling Using Advanced AI Algorithms. International Journal of Advanced Engineering Technologies and Innovations. 1(2): 270-285.

[120] Maddireddy, B.R. and B.R. Maddireddy. (2021) Cyber security Threat Landscape: Predictive Modelling Using Advanced AI Algorithms. Revista Espanola de Documentacion Cientifica. 15(4): 126-153.

[121] Maddireddy, B.R. and B.R. Maddireddy. (2021) Enhancing Endpoint Security through Machine Learning and Artificial Intelligence Applications. Revista Espanola de Documentacion Cientifica. 15(4): 154-164.

[122] Maddireddy, B.R. and B.R. Maddireddy. (2021) Evolutionary Algorithms in AI-Driven Cybersecurity Solutions for Adaptive Threat Mitigation. International Journal of Advanced Engineering Technologies and Innovations. 1(2): 17-43.

[123] Maddireddy, B.R. and B.R. Maddireddy. (2020) AI and Big Data: Synergizing to Create Robust Cybersecurity Ecosystems for Future Networks. International Journal of Advanced Engineering Technologies and Innovations. 1(2): 40-63.

[124] Maddireddy, B.R. and B.R. Maddireddy. (2020) Proactive Cyber Defense: Utilizing AI for Early Threat Detection and Risk Assessment. International Journal of Advanced Engineering Technologies and Innovations. 1(2): 64-83.

[125] Srinivas, N., N. Mandaloju, V. kumar Karne, P.R. Kothamali, and A. Tejani. A Unified Approach to QA Automation in Salesforce Using AI, ML, and Cloud Computing.

[126] Mandaloju, N. kumar Karne, V., Srinivas, N., & Nadimpalli, SV (2021). Overcoming Challenges in Salesforce Lightning Testing with AI Solutions. ESP Journal of Engineering & Technology Advancements (ESP-JETA). 1(1): 228-238.

[127] Mandaloju, N. kumar Karne, V., Srinivas, N., & Nadimpalli, SV (2021). A Unified Approach to QA Automation in Salesforce Using AI, ML, and Cloud Computing. ESP Journal of Engineering & Technology Advancements (ESP-JETA). 1(2): 244-256.

[128] Mandaloju, N. kumar Karne, V., Srinivas, N., & Nadimpalli, SV (2024). Integrating Machine Learning with Salesforce for Enhanced Predictive Analytics. ESP Journal of Engineering & Technology Advancements (ESP-JETA). 4(3): 111-121.

[129] kumar Karne, V., N. Srinivas, N. Mandaloju, and S.V. Nadimpalli. (2023) Optimizing Cloud Costs Through Automated EBS Snapshot Management in AWS. International Journal of Information Technology (IJIT). 9(4).

[130] kumar Karne, V., N. Srinivas, N. Mandaloju, and S.V. Nadimpalli. (2023) Infrastructure as Code: Automating Multi-Cloud Resource Provisioning with Terraform. International Journal of Information Technology (IJIT). 9(1).

[131] Nadimpalli, S.V. and S.S.V. Dandyala. (2023) Automating Security with AI: Leveraging Artificial Intelligence for Real-Time Threat Detection and Response. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 14(1): 798-815.

[132] Nersu, S., S. Kathram, and N. Mandaloju. (2020) Cybersecurity Challenges in Data Integration: A Case Study of ETL Pipelines. Revista de Inteligencia Artificial en Medicina. 11(1): 422-439.

[133] Nersu, S., S. Kathram, and N. Mandaloju. (2021) Automation of ETL Processes Using AI: A Comparative Study. Revista de Inteligencia Artificial en Medicina. 12(1): 536-559.

[134] Mandaloju, N. kumar Karne. V., Srinivas, N., & Nadimpalli, SV Enhancing Salesforce with Machine Learning: Predictive Analytics for Optimized Workflow Automation.