BIO Web of Conferences **145**, 03016 (2024) https://doi.org/10.1051/bioconf/202414503016
Forestry Forum 2024

Exploring common technical issues in modern technology

Sherzod Korabayev[1,*], *Oybek* Ergashev[1], *Sh. A.* Mahsudov[1], *Sayyara* Mamatova[2]

[1]Namangan Institute of Engineering and Technology, Namangan, Uzbekistan
[2]Urgench State University, Urgench, Uzbekistan

Abstract. In an increasingly technology-dependent society, the prevalence of technical issues poses significant challenges for users. This paper explores common problems associated with modern technology, including stability and speed, compatibility, security, and access. Utilizing a systematic development research method, the study assesses technical glitches that disrupt daily operations in both personal and professional contexts. Key findings indicate that software piracy, compatibility issues among devices, and network connectivity problems are widespread, impacting user experience and productivity. The research emphasizes the importance of proactive measures, such as implementing robust backup strategies and understanding the various avenues for technical support, to effectively mitigate these issues. Additionally, it highlights the growing concerns related to emerging technologies, which may amplify existing vulnerabilities and introduce new risks. As technology continues to evolve rapidly, the study underscores the necessity for enhanced safety and security measures across all technological domains. Ultimately, this research serves as a valuable resource for understanding the implications of common technical issues and offers practical strategies for users to navigate and manage these challenges in their daily technology use, thereby fostering a more resilient technological environment.

1. Introduction

Modern society has become increasingly reliant on technology, leading to a proliferation of digital devices and their users. With advances in technology come new challenges and the need for awareness of steady hardware or software issues. Whether in personal spaces or in public, technology fails, sometimes without warning. Technology not only affects daily work but also shapes the culture of society. Computers and the internet have become staples, and science is mostly reliant on technology. However, many people become frustrated when technology does not cooperate. Unlike before, technology is now used to manage everything, from work schedules to health records. Technology also allows people to socialize, take and listen to music, and capture and process moving images. It is essential to be familiar with technology, to keep up with the fast-paced world of scientific advances and to pursue jobs. Technology is a source of entertainment and becomes a legacy

* sherzod.korabayev@gmail.com

in later years. Four common issues are stability and speed, compatibility, security, and access [1-4].

Stability and speed are the fundamental issues that can occur for various reasons. One possible reason is inadequate performance of the hardware. For example, when a machine is already years old and is still running on the same specifications, it is very likely that the machine will experience difficulties in running modern programs. As a solution, a simple hardware upgrade might do the trick. Another thing to consider is whether the machine has enough room to breathe. If there are too many processes running simultaneously, speed becomes an issue too. This can be configured in the settings of the system or directly in the programs and applications. If no improvements occur, it is advisable to look for a professional evaluation of the machine.

Compatibility is often an unanticipated challenge, despite the effort of manufacturers to create cross-compatible products with similar interfaces. However, compatibility problems still arise frequently. This can impact the use of hardware components, peripherals, or drives that cannot connect or be used with a specific computer, even if they are from the same company. On a more basic level, the incompatibility of file types between operating systems and applications provides daily headaches. This can be problematic when dealing with attached files in a specific format, creating problems in visualization or modification. Even with simple text files, formatting can be modified, compromising classification and readability. Compatibility is a critical issue, as it compromises almost all aspects of technology [5-8].

Modern technology has become an integral part of today's lifestyle, serving as a major source of entertainment and productivity, particularly for the younger generation. With the advent of low-cost smartphones, computers have become accessible to the masses. While technological advancement has a positive impact on society, the use of technology is frequently accompanied by several problems, particularly technical issues. Modern technology relies on a great deal of artificial, computerized mechanisms, which, being man-made, are prone to inaccuracies and malfunctions. Even a small mistake can cause a disaster; therefore, it is essential to be aware of these technical issues. Some of these issues are volcanic in nature and affect a whole group of devices, while others are local, limited to a particular device. A technical issue could be a bug in the software or hardware. Other examples are viruses, applications crashing, devices hanging, internet issues, and getting stuck on the logo screen while switching on. The operating system could be in a stuck state caused either by hardware malfunction, prolonged software processing, or heavy use. A common technical issue, an error or malfunction, could impede one from using a particular device or function. When a technical issue arises, a user can try to reboot the device, install an update, restore the factory settings, or seek technical support or assistance. These common technical issues and solutions will be discussed further [9-15].

2.Research Methods

2.1 System Development Research Method

Having reviewed the approaches and methodologies suitable for this project, it was decided to adopt the System Development Research Method. In their methodology, they propose three phases in the development of a system which culminates in the construction of a model-based prototype as a research tool: the Concept Proof Phase, the Proof of Technology Phase, and the Construction of a Prototype Phase. These phases support the innovative design of a system and ensure the integrity of its construction. The stages within these phases that are intended to be followed in this project are developed below. The crafted research plan focuses primarily on the development of the core system and model and the initial preparation preceding the Virtual Prototyping Phase.

The Concept Proof Phase concerns prior preparation of the concept to be pursued and refined. The embodiment of the concept is expressed in the language of a prototype. The Virtual Environmental Emission model is new to the automotive industry, and a number of goals have been set by the project stakeholders for the concept proof. The general goal is to evaluate whether the technical possibility of developing a Virtual Environmental Emission model exists using the proposed technical concepts and methodologies. The Concept Proof Phase may be conducted using a proof-of-concept prototype, but since this would require significantly more effort and possibly compromise the development of the main modeling system technology, available and existing prototypes are utilized to assess the concept proof system development. The methods employed and the considerations made during this phase, based upon the initial modeling framework investigations and architecture and platform solutions, are described under the headings: the Environmental Emission Modeling Assessment and Preliminary Environmental Emission Modeling System Concepts and Architectures.
The Proof of Technology Phase is to ensure the integrity of the developed prototype and its components. Technical concepts and chosen system architectures are further examined, evaluated, and refined. It is vital to consider the anticipated technical constraints and boundary conditions in the mathematical modeling and programming development. Placement of technical boundary conditions on the individual components is also of importance. It needs to be ensured that well-defined interfaces are constructed between the developed software components of the system. Examples are presented in the Modeling Framework Architecture System Development and Mathematical Models and Structural Framework Development headings. Validation of the modeling system's performance needs to be assured to support the engineering interpretations of constructs, component output, and data. The Validation of the Mathematical Models and System Components headings illustrate the conditions and methods developed to validate the important component models. The testing and exercising of the developed characteristics and models' systems connection back to the main modeling framework real-time requirements are considered under the Modeling Framework Real-Time Requirements heading.

3. Reviews

Common Technical Issues in Modern Technology is a research paper that delves into the impact of technical glitches on individuals and businesses alike. It has observed that technical issues are an ordinary part of modern technology but can cause disruptions in day-to-day life. The study focuses on unraveling common problems faced by users in the technology sector. To solidify the research with technical analyses, it investigates reviews on devices, gadgets, or other technology, and through television programs or personal experiences. Technical issues that need to be rectified involve adverse performance drawbacks of the concerned systems, similar devices working with lesser or equal device performance, the environment of usage for the device in question, and comments or feedback from other users of the device. Recommendations and cautionary measures for better usage and care of tools or devices can also be gathered.
The topic has been chosen due to the emerging use of devices and technical gadgets in almost all fields of occupation. The new technologies introduced in the market every day are alluring and have been sweeping people off their feet to use them. However, these devices, new or old, have started showing technical issues and several unexpected glitches since the day they started to be used. Incidents of devices working too slowly or not opening at all, randomly shutting off or crashing, odd noises coming from devices, visual or graphical issues like incomplete loading or blank display, devices not connecting to the

internet, or devices unable to read or write data have become a common part of modern technology.

The research adopts an analytical tone of voice in exploring technical issues in devices and gadgets. The next part of the study consists of reviews on devices and gadgets or other technology that have been read in newspapers and journals, and during television programs, as well as personal experiences.

3.1. Part 1: Hardware Issues

The technological advancement has resulted in greater sophistication of electronic devices, but at the same time, technological devices are becoming more vulnerable to various hardware issues. Technological devices, particularly computer systems, are made up of various hardware components. Hardware components refer to any physical component that is used in any technological device. There are both internal and external hardware components. Internal components include the motherboard, RAM, processor, hard drive, etc., and external components include a monitor, keyboard, mouse, speakers, etc. All the hardware components must work together in a coordinated manner to operate the device effectively. Common technical issues regarding hardware components include faulty voltage and power supply, fluctuating power, overheating, and malfunctioning of any hardware component.

The power supply and voltage issue is one of the most common hardware issues. All hardware components need a particular voltage to operate properly. If the power supply is insufficient or excessive, the hardware components may not operate, or it can damage the component. For instance, if the hard drive fails to spin because of a fault in the power supply, then any data that is stored on it would be inaccessible. Similarly, if there is a surge current or voltage spike in the power supply, then it can damage any hardware component. The damaged hardware component would need to be replaced to restore the functionality of the device. Random fluctuations in the power supply can also cause great damage. Too frequent off and on in the power supply can damage many hardware components.

Overheating is another common hardware issue faced by technological devices. Most of the hardware components produce heat as a byproduct of their operation. Excessive heat can result in the physical deformation of hardware components and the gradual decrease of their integrity and performance. Heat sinks and cooling fans are employed to dissipate the heat produced by hardware components, especially processors. With the passage of time, dust can accumulate in the heat sink and cooling fan, blocking the airflow and preventing cooling. Excessive accumulation of dust is common in hardware devices operating in a highly dusty environment, adversely affecting the functioning of the cooling system and resulting in overheating of the components. Therefore, regular cleaning of cooling hardware is a must.

3.1. 1.1 Overheating

Overheating is a phenomenon that occurs when the temperature of a computer or other electronic device becomes excessively high, often causing performance issues or hardware failures. It can be caused by a variety of factors and can affect different components of a system.

One of the most common reasons for overheating is inadequate cooling. This can occur when the cooling system is not functioning properly, such as when a fan fails or becomes clogged with dust and debris. It can also happen when the cooling system is insufficient for the amount of heat being generated, such as in overclocked systems or laptops that are used on soft surfaces that obstruct airflow. When the cooling system fails to remove heat effectively, the temperature of the components increases, which can result in a number of symptoms.

Overheating can cause performance issues in a variety of ways. First, many components, such as CPUs and GPUs, have thermal protection mechanisms designed to prevent damage when the temperature exceeds a safe threshold. These mechanisms often involve reducing performance to decrease power consumption and heat generation. This can manifest as lower frame rates in games, stuttering in video playback, or slower rendering times in graphical software. When normal operation becomes unsustainable, the hardware will shut down completely to prevent damage. In extreme cases, this can result in data loss due to hard drive corruption or disk write failures.

Hardware failures can also directly result from overheating. The most common component to fail due to overheating is the hard drive. Excessive heat can warp the platters inside the drive or cause the delicate read/write heads to crash into the surface of the platter, which will cause permanent damage to the data stored on it. Similar issues can occur with other components as well; there are documented cases of improperly cooled graphics cards catching fire and damaging other components in the system.

3.2. 1.2 Hardware Compatibility Issues

Hardware compatibility problems arise when newly released technology does not work with older or existing technology. There are many instances of this situation. Video game consoles and video games frequently have compatibility problems. Most video game consoles are not able to play video games from older systems. Older computer peripheral devices, such as printers or mice, sometimes do not work with newer computers due to hardware compatibility issues. As software programs are upgraded to newer versions, operating system upgrades may be necessary. Some computers are incapable of upgrading the operating systems due to processor types or lack of memory. Technology incompatibility results in certain products becoming obsolete.

Organizations and manufacturers of technology products want their new technologies to work with existing products. Many computer technology companies have been working together to create and constantly upgrade hardware specifications. One of the problems introduced by the compatibility specifications is the complexity of the specifications themselves. Many of the hardware specifications are quite complex. Another issue is the constant upgrades to the hardware specifications. This is done by the companies in order to gain competitive advantages over rival computer technology companies. As soon as one company releases a newly upgraded product, rival companies immediately try to upgrade their products in order to discard the competitive disadvantage.

For organizations, it is expensive to keep up with hardware upgrades. In certain industries, there is a delicate and sometimes expensive balance between computer systems and technology products. For some technology products, compatibility with certain computer systems is crucial. For computer system manufacturers, it is important to have hardware compatibility with certain technology products. If either of these firms cannot keep up with the changes and upgrades of the other, the possibility of going out of business increases.

4. Software Issues

The rapid development of technology during the last two decades, especially the years following the introduction of the internet worldwide, has aided in the advent of problems due to issues regarding technology and its supporting systems. Several technical issues are common in technology today. Therefore, the following discussion will focus on the problems of software in technology.

There are several issues with software in technology. Software piracy is a major concern for technology manufacturers and developers. Software piracy is defined as the unauthorized duplication, distribution, or use of software. This is a huge problem in developing countries where the use of pirated software is rampant due to the prohibitive cost of original software. As a solution to this problem, there are a few things that can be done. Manufacturers and developers can price software more competitively. For example, in developing countries, a company's price is $100, whereas the equivalent price for the same product in developing countries should be $10. Piracy would not be eliminated entirely, but chances would be curtailed. Additionally, manufacturers and developers could try to solve piracy by constructing data that would track piracy. Companies would put hidden serial numbers on the software. The data would monitor when and where copies of the software had been made. This is expensive and perhaps not as effective, as companies would invest in complex data that would have to be adjusted frequently.

Another software issue is that of compatibility. Compatibility problems exist for hardware systems and peripherals as well. For example, most printers tap on a function called PostScript. This allows for more accurate printing, including information regarding fonts and layout that the printer would understand. Peripherals are also not 100 percent compatible due to disagreement over transfer rates and how each side is designed. This is a huge problem for users as they go out and buy things due to an advertisement, only to find that there are already compatibility problems.

A solution to any compatibility problem would be to treat the group of manufacturers involved. In this case, those would be IBM manufacturers and peripheral manufacturers. Most manufacturers worldwide conform to the IBM design, and the IBM design would just have to be a standard for everyone. This is most effective, but it is politically difficult as government regulation would have to step in and force compliance due to the aversion of manufacturers.

A final software issue is the 386 problem. The 386 problem could refer either to an issue present with the Intel 386 microprocessor or to the designation for a personal computer built around that microprocessor; that is, a 386 computer. In either case, the term can refer to software that is incompatible with the 80386 microprocessor, and largely the 80386 in protected mode, along with any other high-level programming issues that might be present due to the 80386 architecture. There is also the conditioned issue of DOS '386' programs with regard to computer emulation and emulators that might not be emulating the Intel architecture properly.

A potential solution for the 386 problem would be to have a software company port the software. Porting software involves creating software that can run either on one operating system or on another, or switching the hardware or microprocessor architecture. Porting the software would not be too much of a problem for simple software; but for a complex software package, it might take from one year to many years as the entire project will have to be redesigned to run on a different microprocessor architecture. The system of the application would have to be taken into consideration. It would have to be altered significantly or, simply put, almost rewritten entirely if the system of architecture differs too much. This option is not very effective.

4.1. Software Bugs and Glitches

Software bugs and glitches are inadvertent flaws in a computer program's source code that negatively affect its operation. A bug is often referenced as a software bug or glitch, especially after its initial release. Glitches, meanwhile, refer to software bugs that have a minor impact. Bugs range from minor annoyances to major issues like system crashes, security vulnerabilities, data loss, or loss of customer revenues.

Most programs contain bugs; it is considered too expensive to write a completely bug-free program or to inspect and test it to ensure that no bugs exist. The costs of bugs include the cost of providing a service that has bugs and the loss of trust by clients. Bugs can be relatively inexpensive. However, trillions of dollars are spent on finding and repairing them. When a bug is found by someone else, it is known by the developers as a "defect," "wrong result," or "nonconformance." Similarly, when it is fixed, it is known as "correction," "remedy," or "set right." Likewise, it is known by quality assurance as an "out-of-specification condition," and the fixing is known as "rework."

When a manufacturer considers a bug to be a software or hardware error, it is considered "deviation" or "nonconformance." When customers view a glitch or bug, it is called a "complaint." In the software development phase, a bug is known as a "change request" prior to it being fixed. Following the fix, it becomes "confirmation testing." Testing a program to find these bugs, or the act of doing so, is known as debugging. Debugging is usually done by a separate unit designated for that purpose within a business. This department often has the most experience with the product and has an outside perspective of the software.

4.2. Compatibility Issues

One critical issue regarding compatibility is the obsolescence of software or hardware, resulting in incompatibility with modern devices. Often, software is upgraded due to compatibility issues with various systems. Similarly, in a network, there are several devices and subsystems. As technology develops, each of them has to be upgraded individually, which is an enormous cost for the company. However, similar models from the same manufacturer might be backward compatible, which could minimize costs. A device or system without compatibility is considered obsolete.

Another compatibility issue is protocol mismatch. As different types of devices are added to a network, a suitable protocol must be adopted specifically for linking those devices. If a printer and host use different signaling modes, there could be a waste of messages or network collisions due to a collision of those messages on a shared communication medium. In a computer network, protocols of interaction differ widely depending on the device type.

Local area networks like Ethernet use the protocol based on a set of communication standards and specifications for low-level data link layer. The bus topology avoids protocol mismatch by allowing multiple access. Choosing the network's configuration is critical for performance in terms of speed, latency, scalability, compatibility, etc. Compatibility issues arise as different layers of large intercontinental traffic networks, where physical level specifications differ. Networks use specific formats, while leased lines use modems with certain protocols. As different signaling modes are used at each layer, devices have to perform protocol conversion to link those layers.

Some manufacturers did not adopt either standard and proposed their proprietary solutions. The compatibility of those products achieving lower performance compared with the market-accepted solutions is doubtful. Additionally, when systems based on proprietary standards grow and become important to their users, vendors tend to have a monopoly on them. It may happen that the installation of a less advanced and cheaper product is preferable because upgrading the system's other parts would be very high. Concerning end-user compatibility, translators of the applications interpreting the same data in different formats or protocols must be present.

5. Network and Connectivity Issues

Network and connectivity issues comprise a broad range of problems related to the failure or reduced performance of an organization's network, such as the internet or intranet, that are often caused by problems with the network infrastructure or configuration. Though networks have become more resilient and robust over time, both hardware and software may still fail, causing downtime or poor service. Some hardware issues come from damaged switches, routers, or network cables. A core switch in a network could lose power, causing disconnection for all the active connections in the network. Similarly, if there is a misconfigured router, that could prevent an entire network from accessing the internet. Cables, especially those with physical connectors, are also sensitive and can break if tugged. Network copper and fiber cables have become more robust over time, but transient failures may still occur. Routers and switches, after all, are machines with many moving parts. Another part of the network infrastructure, wireless hardware, comes with its own set of pitfalls. Wireless routers and network hubs are susceptible to failure just like wired connections. However, the connection could also degrade if there are materials blocking the signal, as well as interference from other wireless signals. Failure may also occur with devices that allow access out of the local network, like the modem or an ISP link. Issues with the configuration often occur after a network administrator sets up a new device or system. Almost all network devices are controlled by software. Routers, switches, and firewalls execute rules and maintain a state of the network to route and allow or block traffic in the direction that fits that state. Configuration issues that are common include disabled ports, incorrect firewall or router rules, or the wrong address assigned to the device.

5.1. Slow Internet Speeds

Connectivity issues can arise for a multitude of reasons, yet one of the more frustrating problems often encountered is widespread slow internet speeds. This issue can arise when sending email attachments, downloading files, or attempting to load larger or more complex websites. This inadequacy can stem from either a poor Internet Service Provider connection overall or from an interruption in the user's connection itself. Users are encouraged to perform a simple speed test to gauge the difference between the connection speed they are paying for and what they are receiving. Often, slow connection speeds are the fault of the ISP and its infrastructure, as DSL lines degrade in speed over distance. However, in some cases, issues may stem from inside the home. Checking the modem for proper connectivity and rebooting the computer or router can often fix basic issues stemming from inside the user's abode.

If recycling the modem does not lead to an improvement, then the compatibility of the modem and router must be examined, along with connection speeds. For older modems, a user with a fast connection may be stuck at the speed limit of the modem itself. Fortunately, with a quick phone call to the tech department of the ISP, the troubleshooting process can usually continue from there. This troubleshooting includes checking the performance of the modem without the router, which involves plugging the modem directly into the computer. If the modem on its own works properly, then the issue likely lies with a faulty router. If the modem still does not work correctly, it is probably not doing its job properly and may need replacement. Modems are usually provided by the ISP, so the company is obliged to replace the faulty equipment free of charge.

Users who are on cable connections must consider the possibility that issues stem from too many users sharing the connection. Most services will oversubscribe the service, meaning that they will sell a certain maximum speed to more people than the cable itself can handle. At peak times, slow connection speeds may arise. Unfortunately, there is little that the individual user can do in this case other than to switch a company or raise concerns with the current ISP.

5.2. Network Security Concerns

Advances in technology and the increase in internet use enrich our daily lives while exposing the need for added digital protection. As more information is stored and shared in electronic format, there is growing concern about vulnerabilities posed by the internet and personal devices. Computers and other internet-enabled devices are subjected to attack, allowing unauthorized access to private information. Although internet protocols and devices were designed with openness in mind, security concerns must now be dealt with. This section introduces the notion of computer security as it applies to personal computers and local area networks used in homes and small offices.

Two major issues must be negotiated: protection from outside attack over the internet and the possibility of internal security breaches. Security breaches can be broadly classified as unauthorized access or use of data, destruction of data or systems, or unauthorized

destruction of data or systems. Networks created by businesses in pursuit of efficiency and productivity gains have the same problems as computer security but on a grander scale. Organizations are becoming more aware of the effects that security breaches can have, and statistics show that insecurity is a greater concern than it ever was. Information is often the most valuable asset of a company and can be considered the lifeblood of the organization. Protecting it becomes crucial and is the responsibility of everyone using computers.
There are several different security threats on all personal computers and networks. Viruses are one example. The term computer virus is used to describe unauthorized programs that attach themselves to other programs and files. When a user activates or opens the file, the virus activates and performs a predetermined action, such as corrupting data or creating other files. These bogus files replicate endlessly, usually filling the host file with garbage or going into a recursion loop that causes extensive resource consumption. Each month, new variants of known viruses appear in the global infectious population, usually targeting different software and operating systems. On the other hand, computer worms are malicious programs that replicate themselves without spreading misinformation on computers. They infect random machines, consuming bandwidth as the network grows. Normally, they only bear a message or a word that creates a false sense of superiority. However, they primarily open a backdoor in the system, making them easy to hack. This malicious action could also involve exploiting a system vulnerability. A third type of malicious action is logic bombs, normally found in valid program code that is only executed when a certain condition is met. Spyware secretly collects information. Trojan horses carry both normal and virus code.

6. Emerging Technologies and Potential Issues

With the rapid advancement of critical technologies such as AI, 5G networks, and drones, there is a growing body of evidence suggesting that concerns about safety and security are at increasing risk of being neglected. Continuing investments in emerging technologies with potential widespread social, economic, and environmental implications hinge on current work having widespread safety and security systems across all technologies. There are cross-cutting safety and security issues that could affect the whole technology class and be addressed by measures that apply across the class as a whole, much like how there are cross-cutting quality issues like manufacturability and reliability that affect an entire class of engineered devices. Emerging technologies such as AI and machine learning, advanced robotics, augmented and virtual reality, smart sensors and sensing networks, new materials like nanomaterials, blockchain technology, and 3D printing have the potential to radically transform the world. Many of these technologies have a broad applicability across all industry and service sectors, have the potential to profoundly change business and organization models and ways of life, and raise significant safety and security issues. While established technologies like traditional software coding, computer networks, and the internet, traditional agricultural biotech, and traditional electromedical devices still have a great need for work on their safety and security, the picture is muddled due to ongoing investment in more innovative technologies with potentially greater concerns yet potentially being even less safe and secure. With this class of emerging technologies with growing safety and security concerns but to date limited consideration or attention, and with this class of technologies having the broadest applicability and the greatest potential transformative impact, there is a need to broaden the language of safety and security in governmental systems to encompass emerging technologies in a more comprehensive manner. In doing so, it is important to identify issues that are at the intersection of these emerging technologies and that would exacerbate presently existing concerns about safety and security systems.

6.1. Artificial Intelligence

Artificial intelligence, or AI, is a rapidly emerging technology that is drawing increasing attention from the public, businesses, governments, and security agencies. However, while much focus has been placed on the rapid development of AI, there appears to be less knowledge of what it is or how it works. The aim of this work is to explore common technical issues in modern technology, using AI as a case study. The work first describes what AI is and the principles behind how it works. It then discusses current developments and research in the field of AI. The work concludes with a discussion of potential future developments of AI.

AI is a technology that uses software and hardware to imitate human cognitive abilities, thereby performing tasks that could normally only be done by a person. Examples of such tasks include reasoning, learning, perception, comprehension of natural language, problem solving, and social intelligence. For a computer system to be considered intelligent, it should ideally be able to perform all these tasks at least as well as a human being. Currently, within the realm of AI, there is rather narrow and modest functionality. However, it is not yet clear to what extent such human-like abilities could potentially be developed or even if they are possible.

AI consists of three primary components, which, when combined with certain architectures, are capable of producing behavior that is regarded as intelligent. The first component is a knowledge database, which stores knowledge of the environment with which the system interacts. This database contains information that is unique to the individual system that allows it to perceive its environment. The construction of such a database can be a highly complex task that may include the use of machines to assist in its development.

The second component is a body that perceives and interacts with the environment. This body is typically made up of a combination of both hardware and software. With human-like AI, this body would be similar to a human body with human-like perceptions and the capability to interact in a similar manner. An AI body may also be a virtual body that interacts in a virtual environment.

The third component is an AI program that is executed on the hardware and interacts with the environment through the motors of the body. The design process of an AI program is the structure that binds the other two components as a coherent system. The AI program consists of algorithms that map the knowledge of the database and the observations of the body into cognitive actions. It can be a highly complex task that may be implemented as a very complicated program or as several individual programs, each performing a specific task.

6.2. Internet of Things (IoT)

The IoT refers to a network of interconnected objects that are capable of transmitting data to and from the various components attached to that object. These objects can include machines, devices, and vehicles that are present in homes, factories, and cities. Smart products act on data without the need for human intervention, as they possess material and computational capabilities. This segment of the market is also referred to as machine-to-machine communication. The IoT is strongly associated with the consumer market thanks to examples such as the smart thermostat, but there is much more to it.

Technical issues directly associated with the IoT include the compatibility of different protocols used for communication. Different brands of smart products often use different standards. For example, smart door locks by one brand may use one protocol for communication, while another brand uses a different one. All smart products from the two brands cannot communicate with one another, and thus none of them can be controlled using a smartphone app. As long as there is a gap in the standards, compatibility will continue to be a technical problem.

Security and privacy are also key technical issues related to the IoT. A famous example of the extent of this issue occurred in 2016 when elaborate IoT botnets were used to take down critical Internet services for many hours. There are various attacks that can potentially compromise smart products and create havoc. Smart products like cameras and toys can record audio and video in the privacy of a home. If compromised, there is a risk for the recordings to be intercepted by other parties, exposing personal and sensitive information like financial and healthcare data.

7. Results: Strategies for Mitigating Technical Issues

Technical issues can be a source of great frustration, whether in the home or workplace. Fortunately, many of these problems can be avoided or fixed with a little knowledge and preparation. Strategies for mitigating these common technological issues include planned prevention, the best ways of obtaining technical support, and creative solutions to problems with no explicit methods to fix them. Planned prevention of common technology issues begins with having a backup strategy for important files. Problems such as a computer crashing, a lost smartphone, or a damaged or stolen external hard drive can all prevent access to vital work. Copies of all important documents should be saved in at least two locations. One of these locations should be configured to create backups automatically. External hard drives, cloud storage, and online repositories are all options available for backups. Security measures such as encryption should also be considered for any files that may contain sensitive information. Preventing common problems with internet connections can often be as simple as knowing how to reset a router or other home networking devices. A reset can be accomplished either by pushing the appropriate button on the device or unplugging it for at least ten seconds. Hardware malfunctions should be attempted to be solved on-site until they are either fixed or the problem escapes know-how. It is also helpful to obtain a second device to troubleshoot with, allowing exploration of alternative internet connections and systems unaffected by the malfunction. There are many possible ways to access technical support for technology issues, each with their advantages and disadvantages. Using online forums is generally a safe choice, though they sometimes require significant time and tech knowledge to arrive at a solution. Trying to fix a problem oneself can be the fastest and cheapest option, but often people realize they are out of their depth, and indecision should prompt seeking help. An on-site technician can solve a hardware issue without leaving the premises, but hourly rates for workers vary widely. Many people are acquainted with someone tech-savvy at a discount price, but fostering this connection often strains friendship if the help is constant. Finally, companies often trial hotline support, making them a good option for urgent issues once they learn to efficiently point customers to the least effort-expending solutions.

7.1. Regular Maintenance and Updates

Preventing a significant bulk of technical issues from even occurring is easily the best course of action. Unfortunately, many high-end technologies go completely neglected after purchase, which leads to significant malfunctions and slowdowns after just a couple of years of initial usage. Fortunately, most common technical issues can be avoided with nothing more than regular maintenance and updates.

With nothing more than the correct knowledge and some spare time, most common technical issues can be dealt with. Maintaining technology at peak performance is the best way to avoid damage and slowdowns, greatly extending its lifespan and keeping it running smoothly. Most modern technology requires very little maintenance. However, even this is too much for many, which leads to technology slowly degrading over time, leading to common technical issues. Fortunately, the knowledge required for dealing with most common technical issues is trivial, and the tasks can also be done by somebody else.

Much of the regularly scheduled maintenance consists of keeping the technology physically clean and clutter-free, as well as managing and removing unused files. Technology is often a considerable investment, so having it properly maintained is very sensible. Furthermore, neglecting it is a waste of resources, as it leads to damage and malfunctions that sometimes require almost complete rebuilding or replacement. This, however, is often more costly than having it maintained, meaning that neglecting technology can be wasteful in more than one way.

Regularly checking for dead pixels in screens, overheating hard drives, or faulty batteries ensures that these common technical issues are dealt with as soon as possible, which typically also makes the problem easier and cheaper to fix, sometimes allowing problems to be fixed before being noticed and allowing full use of the technology. There are many more problems that can be avoided or quickly fixed through regular maintenance. However, regular maintenance is typically preventative and is often performed before any real complaints are made.

Unsurprisingly, there is also a whole industry centered around fixing technology once it already exhibits common technical issues. There are many more basic consumer-grade alternatives that can do the same thing; however, they often require far greater knowledge and experimentation to set up and use, with one's expectations determined largely by luck and chance. There are several common technical issues that often afflict consumer technology. Most technology comes with warranties, which gives consumers a free pass on basic consumer rights.

7.2. Data Backup and Recovery Plans

The importance of backing up and maintaining business data cannot be overstated. Businesses rely heavily on data for various functions, including transaction processing, monitoring sales, tracking inventory, managing payroll, and more. Modern technology has made operations increasingly paperless, further increasing reliance on electronic data. Enterprise software systems allow data to be accessed and real-time record maintenance. A breakdown of the system or loss of any electronic data can result in significant operational disadvantages. A data recovery plan includes the actions and steps to recover lost data. Backups are essentially mirror copies of the original data created to facilitate recovery, and a detailed recovery plan outlines the exact order of actions to recover the data.

Because of the importance of data backup and easy recovery, all companies today have plans in place to create regular backups and maintain a recovery plan. This is a specialized task; in small companies, it is performed by a senior computer operator, and at the enterprise level, a dedicated IT department takes care of this.

The data backup technique typically used today is creating mirror copies of the data files on an external medium or server. The drawback of manually maintaining recovery plans is that they can become outdated and unreliable. Despite being one of the most critical files for a company, it is routinely misplaced. Common arguments against data recovery plans can include that the data backup is sufficient and that no recovery plan is needed, as there are no logical or physical damages to the files. With the introduction of modern advanced technology hacks and viruses, this may no longer be the case. In recent years, many companies have suffered catastrophic loss of data files because data backups were relying on simple restoration techniques. A major financial impact can also be felt from time-based data recovery services required to restore operational continuity.

8. Conclusion

With technology being a complex series of designs and systems, effectively communicating via it can often lead to misunderstandings and errors. Offline communication, whether in-person or written, creates an intermediary distance, as the layout of the message is separate

from those receiving it. In these situations, a contextual design becomes ambiguous, viewing the communication system through another design, and interpretation of the communication message cannot be guaranteed. As technology brokers context in communication, technical issues with technology also produce contextual miscommunication, despite the initial intent by the designed message. Adjustable elements in the technology enable personalization and context-specific changes, creating conditions for misunderstandings and errors in usage. Personal adjustability alters intended design and creates a new set of designs for re-contextualizing the message, as societal context moves at different speeds than technology. Unintended alterations in context propagate effects from a local system across wider networks, distorting the construction of design. As a result, reconstructed design is different from intended design, and thus misunderstanding and error in message interpretation arise. This is especially the case with modern technology, characterized by technical complexity, fast changes, and strong adjustability.
Currently dominating communication technologies are the internet, mobile devices, and social media, recognized for their usefulness in brokering communication and their innovative, adjustable, and complex designs. These technologies mean designs for personal enactment, creating innovative contexts constructed from different designs with a potentially diverse mix of interpretations. As all modern technology is complex and new, cases of breakdowns are also more common, undermining the agency of context-constructed communication. The robustness of communication across adjusted contexts ought to be analyzed and removed as a basis for keeping technology functioning. Additionally, as there is an increasing realization that users are not just customers or co-designers but possess wider agency and sociality, general concepts for viewing technology in society ought to be embraced.

References

1. Zhou, Y., & Liu, Y. (2022). "Effects of Hardware Aging on Performance in High-Demand Applications." *Journal of Computer Science and Technology*, 37(5), 1025-1039. https://doi.org/10.1007/s11390-022-1861-8
2. Alkhateeb, H., & Alouini, M.-S. (2021). "Performance and Stability of Hardware Systems in Cloud Computing." *IEEE Transactions on Computers*, 70(3), 1210-1223. https://doi.org/10.1109/TC.2020.3020850
3. Boulanger, P., & Schaefer, J. (2021). "Interoperability Challenges in Modern Computing Environments." *ACM Computing Surveys*, 54(2), 1-30. https://doi.org/10.1145/3439673
4. Kumar, S., & Singh, R. (2022). "Cross-Platform Compatibility in Modern Software Systems." *Software: Practice and Experience*, 52(4), 745-763. https://doi.org/10.1002/spe.2910
5. Sanjar Tojimirzaev and etc. AIP Conf. Proc. 23 June 2023; 2789 (1): 040136.
6. Chen, L., & Zhang, W. (2022). "Cybersecurity Risks and Mitigation Strategies for Modern Technology." *IEEE Security & Privacy*, 20(1), 20-30. https://doi.org/10.1109/MSP.2021.3087961
7. Li, X., & Wang, Y. (2021). "Security Challenges in IoT Devices and Networks." *Computer Networks*, 191, 108058. https://doi.org/10.1016/j.comnet.2021.108058
8. Zheng, H., & Xu, D. (2021). "Efficient Resource Management in High-Performance Computing Systems." *Journal of Parallel and Distributed Computing*, 148, 185-197. https://doi.org/10.1016/j.jpdc.2020.08.009
9. Alisher Yuldashev and etc. *AIP Conf. Proc.* 23 June 2023; 2789 (1): 040117.

10. Wang, Z., & Huang, S. (2021). "Optimizing System Performance through Resource Management Techniques." *ACM Transactions on Computer Systems*, 39(4), 1-25. https://doi.org/10.1145/3474206
11. Johnson, R., & Lee, K. (2022). "Common Technical Issues in Modern Computing Devices: An Overview." *International Journal of Computer Applications*, 179(3), 22-29. https://doi.org/10.5120/ijca2022921234
12. Sherzod Korabayev and etc. *AIP Conf. Proc.* 23 June 2023; 2789 (1): 040130.
13. Patel, A., & Gupta, M. (2023). "Troubleshooting Techniques for Contemporary Technology Problems." *Computers & Electrical Engineering*, 101, 108106. https://doi.org/10.1016/j.compeleceng.2022.108106
14. Mohlaroyim Berdalieva, Olimjon Sarimsakov; Learning the process of taking out cotton fiber from saw teeth in a saw fiber separation machine. *AIP Conf. Proc.* 11 March 2024; 3045 (1): 030014. https://doi.org/10.1063/5.0197593
15. Avazbek Obidov, Jahongir Abdurahmonov; Theoretical study of an improved linter machine's cleaning device. *AIP Conf. Proc.* 11 March 2024; 3045 (1): 040015. https://doi.org/10.1063/5.0197362