International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Security and Privacy in Intelligent Computing

Banashankari Kamat, Manjusha Pawar, Dr. Sunita Padmannavar

MCA Student, MCA Student, Associate Professor
Department of MCA, K. L. S. Gogte Institute of Technology, Belagavi, Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India

ABSTRACT:

Computing has been a key component in the development of human civilization. Intelligent computing is a new computing paradigm that has arisen in recent years due to the introduction of new computing theories, architectures, methodologies, systems, and applications. In the era of big data, artificial intelligence, and the internet of things, it is altering traditional computing and promoting the digital revolution. Intelligent computing has greatly broadened the field of computing, moving from traditional data-driven computing to increasingly diverse computing paradigms such as autonomous intelligence, cognitive intelligence, perceptual intelligence, and human–computer fusion intelligence. Although computing and intelligence have historically developed along different paths, in recent years they have become more and more integrated: intelligent computing is both intelligence-driven and intelligence-oriented.

Since intelligent computing is still in its infancy, a wealth of advancements in its theories, methods, and applications are anticipated in the near future. We offer the first thorough overview of the literature on intelligent computing, encompassing its theoretical underpinnings, the technological merger of computer and intelligence, significant applications, difficulties, and prospective applications. We think that this survey is very topical, will serve as a thorough reference, and give academic and corporate researchers and practitioners important new perspectives on intelligent computing.

KEY WORDS: Edge computing, Computer security ,Cloud computing, Privacy, Servers, Peer-to-peer computing, Data privacy, cloud computing, Multi-access edge computing (MEC).

1. INTRODUCTION:

We are seeing the emergence of a completely new paradigm for computing that will undoubtedly change the way we communicate with computers, other gadgets, real-world locations, and people. According to this new technology, digital communications, computers, sensors, and embedded processors will all be widely accessible, low-cost goods. By making services accessible to users at all times and locations, this removes obstacles based on location and time.

With the integration of physical and computational infrastructures into one cohesive habitat, ubiquitous computing will envelop users in a pleasant and comfortable information environment.

Thousands or even hundreds of thousands of sensors and computing devices will be scattered across this habitat to enhance productivity and interaction, offer specialized services, and add new capabilities. By adapting to their preferences and carrying out jobs and group activities in accordance with the physical space's requirements, context-awareness will enable this habitat to assume the role of servicing users. We refer to this dynamic, richly informative environment as a "active space." People can engage with adaptable apps in this area that can follow them, define and manage the space's functionality, or work together with other users and apps from a distance.This computer paradigm's realization is not so far-fetched. Nowadays, the typical person possesses a plethora of consumer electronics, gadgets, and appliances, such as TVs, VCRs, washers, and dryers that already have CPUs, microcontrollers, and memory chips built into them. Numerous embedded computers manage various vehicle subsystems, such as the ESP (Electronic Stability Program) and ABS (Anti-lock Braking System) in the cars we drive every day. Any small device can easily be equipped with networking capabilities thanks to technologies like Bluetooth and Wi-Fi [2]. Essentially, these technologies contribute to the widespread adoption of networking, making it possible to use it even with basic devices like paperclips and toasters.

2. REVIEW OF LITERATURE:

Advanced capabilities for data processing and decision-making are altering businesses through intelligent computing, which encompasses technologies such as artificial intelligence (AI), machine learning (ML), and big data analytics. However, serious security and privacy concerns are raised by these developments. This study highlights the primary problems and suggests remedies from important literature that addresses these topics.

1. **Data Collection and Consent**:

- Numerous personal data sets are often required for intelligent systems to function well. This raises issues about how data is collected, stored, and used.
- The research consistently emphasises the need of getting users' express consent and using open data gathering procedures. Tene and Polonetsky (2013), for instance, stress the value of user control over personal data and informed consent.

2. **Anonymization and De-identification**:
   - To protect privacy, data can be anonymized or de-identified, but studies like those by Narayanan and Shmatikov (2008) show that even anonymized data can sometimes be re-identified.
   - Researchers suggest enhancing anonymization techniques and combining them with other privacy-preserving methods.
3. **Differential Privacy**:
   - Differential privacy is a technique that adds random noise to data to protect individual identities while allowing useful data analysis.
   - Dwork (2006) introduces differential privacy as a robust method for maintaining privacy in statistical databases, and it has since been widely adopted in research and practice.

Security Challenges

1. **Data Breaches and Cyberattacks**:
   - Because intelligent systems handle important data, they are easy targets for hackers. This covers malware attacks, unapproved access, and data breaches.
   - Anderson (2001) addresses a range of security risks and the requirement for all-encompassing security plans in order to safeguard intelligent systems.
2. **Secure Data Storage and Transmission**:
   - Ensuring that data is securely stored and transmitted is crucial. Encryption techniques are commonly used to protect data in transit and at rest.
   - Stallings (2016) provides a detailed overview of encryption methods and their applications in securing data.
3. **AI-Specific Threats**:
   - Ensuring the safe transmission and storage of data is essential. Data encryption techniques are widely used to protect data while it's in transit and at rest.
   - A thorough description of encryption techniques and how they are used to secure data may be found in Stallings (2016).

Solutions and Best Practices

1. **Regulatory Frameworks**:
   - To ensure security and privacy in intelligent computing, organizations and governments are developing policies. The General Data Protection Regulation (GDPR), which sets strict criteria for privacy and data protection, is one significant example.
   - Academics that examine GDPR's effects on intelligent systems, such as Voigt and Bussche (2017), stress the necessity of international standards.
2. **Ethical AI**:
   - Designing systems with privacy and security as top priorities is a necessary step in developing ethical AI. Putting privacy-by-design and security-by-design ideas into practice is part of this.
   - Florid et al. (2018) argue for ethical AI practices and address the significance of ethical considerations in AI development.
3. **Collaboration and Education**:
   - Cooperation between industry professionals, policymakers, researchers, and other stakeholders is necessary to improve security and privacy.
   - Educational programs are essential for increasing awareness and providing people with the knowledge and abilities needed to handle privacy and security issues in intelligent computing.

3. FEATURE OF INTELLIGENT COMPUTING:

In this subsection, we first introduce the major characteristics of intelligent computing development and then reveal the innovation paths to obtain these critical characteristics.

- **Self-learning and evolvability**:

Intelligent computing, which draws inspiration from brain biology, creates a number of cutting-edge methods, including neuromorphic computing and biological computing, to advance the theories and models of von Neumann's computer architecture. Self-learning is gaining experience through the extraction of information and rules from large amounts of data, followed by the optimization of computation routes to produce useful outcomes. Simulating the evolutionary process of natural species, evolvability is also a heuristic self-optimization ability. In this process, machines learn from their surroundings and then modify themselves to fit in.

- **Security and reliability:**

The integration of intelligent computing with large-scale, pervasive, networked computing systems facilitates security protection and cross-domain trust. Enabling data fusion, sharing, and opening, it creates autonomous, manageable, and trustworthy security technologies and support systems. In terms of hardware, operating system, software, network, and private computing, high trust is defined as the confidence in identity, data, computing process, and computing environment. High security specifically refers to computing system circulation, storage, content, and network security, all of which can be ensured by combining a variety of privacy-preserving methods.

- **Automation and precision:**

Task-oriented, intelligent computing realizes automatic demand calculation, exact system reconstruction, matching of computer resources. The way a task is executed continuously modifies the architecture of the system. Both hardware and software are used to carry out directed coupling reconstruction. In order to assess the friendliness, availability, and service of intelligent computing, it is necessary to automate the computing process, which includes automatic resource management and scheduling, automatic service creation and provision, and automatic task life cycle management. The accuracy of computation outcomes underpins computer services; in addition, it resolves issues such as quick job processing and timely resource matching.

4.CHALLENGES IN COMPUTING:

Massive processing capacity is required because to the enormous growth in applications, connections, terminals, users, and data that the wave of digitalization has produced. For example, throughout the course of the next five years, it is anticipated that the computing power required for artificial intelligence will increase by over a million times, doubling every hundred days. As Moore's law slows down, it gets harder to keep up with the exponential development in processing capacity required. Moreover, the enormous duties in an intelligent society rely on the efficient combination of multiple specialized computer resources. Moreover, standard hardware modes are inadequate to support intelligent algorithms, which limits software development.

As of yet, no one has come to a universally accepted definition of intelligent computing. As per certain scholars, intelligent computing represents the amalgamation of artificial intelligence and computing technology. It marks three major turning points in the development of AI for intelligent computing systems. The limitations inherent in artificial intelligence (AI) are overlooked in this perspective, as is the crucial part that ternary interactions—interactions among humans, machines, and objects—play in defining intelligent computing as a discipline.

Another school of thinking refers to intelligent computing as computational intelligence. In order to create the best algorithms possible to solve specific problems, this field imitates biological or human intelligence and sees intelligent computing primarily as an algorithmic breakthrough [12]. However, it ignores how important computer architecture and the internet of things are.

5. CHALLENGES IN INTELLIGENCE:

Deep learning-based AI presently confronts significant obstacles with regard to interpretability, generality, evaluability , and autonomy. The majority of AI technologies available today only function poorly when compared to human intellect and only effectively complete particular activities or sectors. We still have a long way to go until we get powerful, ubiquitous AI. To sum up, there are significant theoretical and technological obstacles to overcome in order to go beyond data-based intelligence to more diversified forms of intelligence, such as autonomous intelligence, perceptual intelligence, cognitive intelligence, and human-machine fusion intelligence.

6. FOUNDAMENTALS OF INTELLIGENCE IN COMPUTING:

In the age of digital civilization, intelligent computing refers to new theoretical approaches, architectural frameworks, and technological capabilities that enable the interconnectedness of all things. It investigates novel approaches to tackle intricate scientific and societal issues in a variety of traditional and cutting-edge research domains. Human intelligence, machine capabilities, and the physical universe made up of everything are the fundamental components of intelligent computing. The cognitive powers and intelligence required by intelligent computing are introduced in this section. We also outline the characteristics of intelligent computing and how to integrate computation with intelligence in the domains of information, physics, and human behavior.

7. FUSION OF INTELLIGENCE IN COMPUTING:

Intelligent computing relies on two essential components—compute and intelligence—that function best when together. While intelligence allows computer technology to advance, computation is the foundation of intelligence. Advanced intelligence technologies that increase the efficiency and performance of computer systems are based on the idea of computing by intelligence. The idea of "computing for intelligence" refers to the robust and efficient computational technologies that make it possible to enhance computer intelligence. In order to achieve ubiquitous, transparent, trustworthy, real-time, autonomous services, the two core paradigms are redesigned from five angles, resulting in improvements to computational power, energy efficiency, data utilization, knowledge expression, and algorithm capabilities.

- **The paradigm of computing by intelligence**

Today's complicated models require computing power at a rate that is one or two times faster than that of earlier models. Notable differences exist between the basic processing mechanism of conventional computers and the calculation methods used by intelligent models, which contribute to low computing efficiency. The computing by intelligence paradigm encompasses new models, support, paradigms, approaches, and synergies that make use of cunning methods to boost computing power and effectiveness.

As of now, intelligent systems are limited to a limited number of activities in a closed environment due to their lack of imagination, common sense, and intuition. The study of biological, knowledge computing, and human brain mechanisms is carried out through research on xeromorphic computing, graph, and other new computer models. These novel models have the potential to significantly enhance intelligent algorithms' generalization impact, cognitive comprehension and reasoning learning capacities, and adaptability.

The current computer system has to be expanded further in terms of computation and response time because of its limited architecture and lack of end-to-end processing power. The utilization of online learning, edge computing, processing-in-memory, and other novel computing support technologies can enhance the real-time performance of a computer system through intelligent computing. The convergence of location processing and perception with computation is one example of how emerging technologies have emerged as potential research areas.

The deep integration of the triple space results in a higher diversity of computing jobs, greater complexity and challenge in task solutions, and an increase in unstructured computing scenarios and data. The modeling, analysis, and adaptive processing of unstructured data are therefore made possible by the new computer paradigm. Transparency computing is achieved by an intelligent and automated strategy that combines understanding, breakdown, solution, and resource allocation for tasks.

In order to manage a variety of tasks, including cooperative evolution and hardware and software refactoring, intelligent computing looks into novel computing techniques. With several levels of granularity, the new system arranges computer resources and configures hardware while intelligent processes are running. Using intelligent technologies, such as flexible software and hardware design, flexible algorithm and model collaboration, and adaptive data and resource allocation, the new mechanism will build an automatic computing system with autonomous learning and evolutionary iteration.

Human-computer interaction, swarm intelligence, and human-in-loop are examples of emerging synergistic computing systems that blend human sensing and cognitive power with computer operation and storage capabilities. Such innovative structures efficiently increase the senses and reasoning capacities of computers. Machines can efficiently and accurately collect data from the physical world at very high speeds thanks to a range of sensors. However, they are not able to carry out complex activities and analyse the data on their own. Notably, humans are able to communicate with machines in human–computer interactions, study the physical world at a higher level, and comprehend the laws of the physical universe.

- **The paradigm of computing for intelligence**.

By creating new frameworks, techniques, integrations, architectures, and systems, the computing for intelligence paradigm aims to raise the bar for intelligence while delivering ubiquitous, transparent, automatic, real-time, and secure computing services. Complicating matters, hardware architectural heterogeneity and complexity limit improvements in processing power and service quality.

Memory processing, heterogeneous integration, and wide-area collaboration are all included in the computing framework's innovative non-von Neumann structure. Furthermore, high processing power demands are catered for in the design of the specialized hardware building blocks. The system sensing, scheduling, and management of computing resources, together with the chip's processing structure, are optimized. Integrating hardware and successfully increasing intellectual processing capacity becomes more difficult when taking into account the variety of intelligent devices, the discretization of computing resources, and the complexity of network connections.

Investigating the low-power properties of biological materials using state-of-the-art computer techniques like Biocomputing and xeromorphic computing offers a fresh approach to increasing energy efficiency in limited spaces. The human brain is far more energy-efficient than any artificial intelligence (AI), requiring only 20 W of power to learn. Intelligent computing has the potential to significantly improve computing efficiency and reduce energy usage by developing new computer hardware and software and studying the computational techniques used by biological and human brains.

Intelligent computing facilitates human-machine integration and efficient collaboration by improving machine intelligence, sensing capabilities, and emergency response. Intelligent computing utilizes the whole connectivity of people, machines, and objects to build a thoroughly integrated computing system. When human-machine interactions are coordinated, supported, and enhanced, humans can gain from more comprehensive, precise, and thoughtful intelligent services.

Timely services for users and edge terminal nodes cannot be provided by the conventional cluster-centered computing architecture. In order to successfully integrate terminal computing resources, cloud computing, edge computing, and supercomputing, novel distributed computing architectures are being built. These include end-to-end cloud and wide-area collaboration. The centralization issue is resolved by intelligent job breakdown, paving the way for the development of efficient and widely-used computer services.

A setting where physical computing, information computing, and human contact are combined may increase the surfaces available for malicious attack, increasing the system's susceptibility. Concerns regarding privacy and data security are also brought up by the massive volume of diversified data. Using locally developed safe mechanisms and dependable computing processes, a new intelligent computing system that is dependable and secure is built to address these issues. It guarantees the confidentiality and precision of the identity, data, processing, and outcome.

8. COMPUTING FOR INTELLIGENCE:

Due in significant part to the constant increase in processing capacity, AI breakthroughs are emerging on a daily basis [12]. The largest model released in 2020 needed six million times the processing power of the ground-breaking 2012 model that popularized deep learning. Open AI researchers have come to the conclusion that this rapid rising cannot be sustained indefinitely after drawing attention to this tendency and making an effort to measure its rate of rise in 2018. As it happens, the impending slowdown might already be in motion.

Researchers from Open AI conducted a study in 2018 to monitor the expansion of the biggest models in terms of processing power [13]. They found two trends with the rapid growth of computing resources, using the amount of computation required to train some of the most well-known AI models in the history of AI research. Historically, novel concepts or ground-breaking theories have propelled AI's quick evolution. In an attempt to accomplish the same task, the most recent state-of-the-art models frequently rely exclusively on larger neural networks and more potent processing systems than those previously employed.

According to their analysis, before 2012, the computational power needed to create a novel model increased roughly in tandem with Moore's law—the well-known finding that a single microchip's computational capability doubles every two years. When AlexNet, an image identification system, was launched in 2012, it sparked renewed interest in deep learning techniques, even though they had been the main driver behind most AI breakthroughs over the past ten years. As shown in Fig. 1, the introduction of Alex Net caused a sharp rise in the computing requirements of top models, which doubled every 3.4 months between 2012 and 2018.

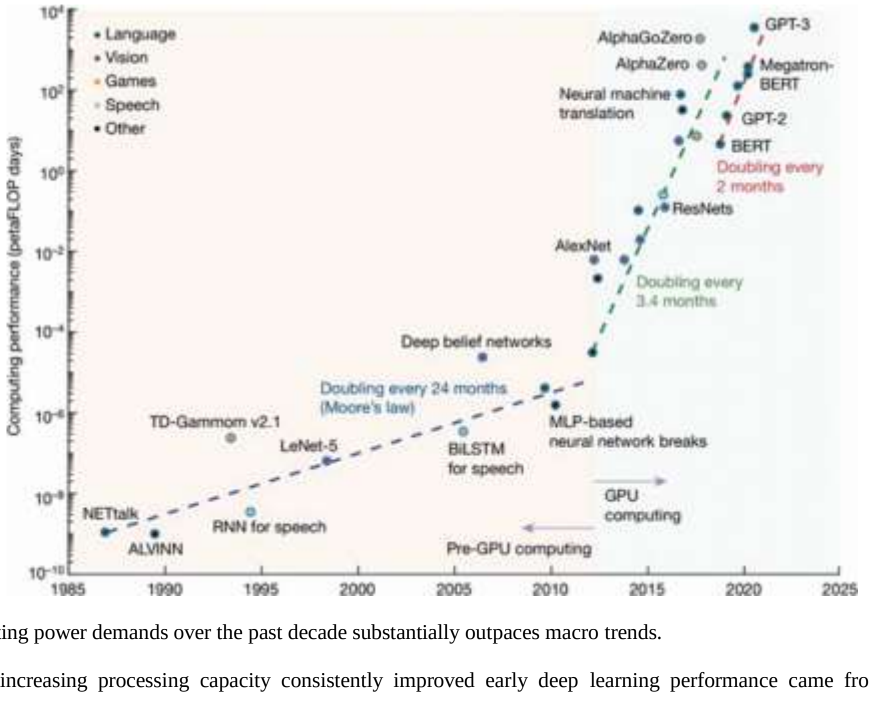

Fig. 1. Growth in computing power demands over the past decade substantially outpaces macro trends.

The first evidence that increasing processing capacity consistently improved early deep learning performance came from early work on photo categorization. However, attention turned to other fields as processing power grew and image recognition algorithms started to outperform humans in several tasks [13]. Reward learning approaches were used to build massive AI models in the middle of the 2010s that could play games like Atari or Go Then the transformer architecture emerged, reintroducing language obligations as a priority. A popular AI model in recent years is the word generator GPT-3 from Open AI.

Processing requirements remained high even with advancements in algorithms and architectures that allowed for more learning with fewer computations. For Alex Net through GPT-3, there is a 3.4-month doubling period in compute requirements. As a result, processing power is beginning to limit intelligent computing. At the same time, energy efficiency of AI/ML platforms will become increasingly important to reduce computation costs.

The goal of distributed machine learning (DML) technique development is to lessen the processing burden on a single server, allowing for scalable computations [14]. Federated learning (FL) is a sort of distributed machine learning (DML) that shows great promise for distributed learning while preserving data privacy at the servers. It also eliminates the overhead of having a large volume of data sent from several locations to a central server. Intelligent computer systems of the future will require a variety of DML paradigms, after all.

9. CONCLUSION:

The fourth phase of human growth is currently beginning, and we are making the crucial shift from the information society to the intelligent society's human-physics-information integration. Computing technologies are changing in this transition in ways that are disruptive and even transformational. The path of computing in the future is thought to be intelligent computing, which includes both intelligence-oriented and intelligence-empowered computing. In today's smart society, it will enable large-scale and complicated computational tasks by offering ubiquitous, efficient, secure, autonomous, dependable, and transparent computing services.

The present study offers a thorough examination of intelligent computing, encompassing its theoretical underpinnings, the technological amalgamation of intelligence and computing, significant applications, obstacles, and prospective avenues. Our goal is to encourage future theoretical and technological advancements in intelligent computing by offering this evaluation as a useful resource for scholars and practitioners.

REFERENCES:

1. X. Yang, X. Yu, H. Huang and H. Zhu, "Energy efficiency based joint computation offloading and resource allocation in multi-access MEC systems", IEEE Access, vol. 7, pp. 117054-117062, 2019..

2. X. Wang, Y. Ji, J. Zhang, L. Bai and M. Zhang, "Low-latency oriented network planning for MEC-enabled WDM-PON based fiber-wireless access networks", IEEE Access.

3. B. Shi, J. Yang, Z. Huang and P. Hui, "Offloading guidelines for augmented reality applications on wearable devices", Proc. ACM Int. Conf. Multimedia, pp. 1271-1274, 2015.

4. Z. Xiang, F. Gabriel, E. Urbano, G. T. Nguyen, M. Reisslein and F. H. P. Fitzek, "Reducing latency in virtual machines: Enabling tactile Internet for human-machine co-working", IEEE J. Sel. Areas Commun., vol. 37, pp. 1098-1116, May 2019

5. G. P. Fettweis, "The tactile Internet: Applications and challenges", IEEE Veh. Technol. Mag., vol. 9, no. 1, pp. 64-70, Mar. 2014.

6. M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A survey on enabling technologies protocols and applications", IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347-2376, 4th Quart. 2015

7. H. Shariatmadari, R. Ratasuk, S. Iraji, A. Laya, T. Taleb, R. Jäntti, et al., "Machine-type communications: Current status and future perspectives toward 5G systems", IEEE Commun. Mag., vol. 53, no. 9, pp. 10-17, Sep. 2015.

8. G. Zhu et al., "Toward an Intelligent Edge: Wireless Communication Meets Machine Learning", *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 19-25, Jan. 2020.

9. M. Yahuza et al., "Systematic Review on Security and Privacy Requirements in Edge Computing: State of the Art and Future Research Opportunities", *IEEE Access*, vol. 6, pp. 18,209-37, 2018.

10. S. Al amro, D. A. Elizondo, A. Solanas, A. Martnez-Balleste et al., "Evolutionary computation in computer security and forensics: An overview." in Computational Intelligence for Privacy and Security, Berlin Heidelberg:Springer-Verlag, pp. 25-34, 2012.

11. J. Zhang, B. Chen, Y. Zhao, X. Cheng and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues", *IEEE Access*, vol. 6, pp. 18209-18237, 2018.

12. Krizhevsky A, Sutskever I, Hinton GE. "Imagenet classification with deep convolutional neural networks". Commun ACM. 2017

13. Khan LU, Saad W, Han Z, Hossain E, Hong CS. "Federated learning for internet of things: Recent advances, taxonomy, and open challenges". *IEEE Commun Surv Tutor* 2021

14. Hu S, Chen X, Ni W, Hossain E, Wang X. "Distributed machine learning for wireless communication networks: Techniques, architectures, and applications". *IEEE Commun Surv Tutor*. 2021