International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 06 | Jun 2026 www.irjet.net p-ISSN: 2395-0072

# Security and Privacy under Umbrella of Cyber security: Integration with Location Based Services, Software Agents, and Deep Learning

**Nawaf Abdullah Alrayes**

*College of Computing, Fahad Bin Sultan University, AIMD Lab, KSA, Tabuk*

---

**Abstract -** *This paper presents an overview of cyber security and privacy issues in modern connected environments, with special focus on location-based services, software agents, and deep learning applications in the medical sector. It first explains cyber security as a core requirement for protecting digital systems, networks, software, and data from unauthorized access, disruption, damage, and theft. The paper also discusses the importance of cyber security functions such as identification, protection, detection, response, and recovery. In addition, it highlights privacy protection in location-based services, where repeated and accurate location data may reveal sensitive personal information, user behavior, and movement patterns. Several privacy-preserving methods are discussed, including obfuscation, anonymity, dummy locations, and differential privacy. Furthermore, the paper introduces agent-based systems as flexible and distributed software solutions that support cooperation, adaptability, and intelligent decision-making, while also emphasizing their security challenges. The role of deep learning in the medical sector is also reviewed, particularly in medical image processing and diagnosis. Finally, the paper explains that the integration of cyber security, privacy protection, agent-based systems, and deep learning requires responsible design, secure data handling, and continuous protection mechanisms to ensure trust, safety, and reliability.*

**Key Words: Cyber security, CIA Triad, Location-Based Services, Privacy Protection, Agent-Based Systems, Deep Learning, Medical Sector, Artificial Intelligence.**

## 1. INTRODUCTION

### 1.1 Cyber security and the CIA Triad

### What cyber security means

Cyber security is the practice of protecting digital systems, networks, software, and data from unauthorized access, disruption, damage, or theft. In simple terms, it is what helps modern digital life run safely. Today, governments, hospitals, businesses, and universities all depend on connected technologies, so cyber security is no longer just a technical issue. It has become a practical requirement for protecting information, keeping services available, and maintaining trust in digital systems [1].

The CIA Triad is one of the most important models used to explain the main goals of cyber security. It consists of Confidentiality, Integrity, and Availability. Confidentiality means ensuring that information is accessed only by authorized users, usually through passwords, encryption, authentication, and access control. Integrity means protecting data from unauthorized modification, so that information remains accurate, complete, and trustworthy. Availability means ensuring that systems, services, and data remain accessible whenever authorized users need them. Together, these three principles form the foundation of cyber security because they help organizations protect sensitive data, maintain reliable services, and reduce the impact of cyber threats.

In practice, cyber security also depends on a continuous process that includes identifying risks, protecting systems, detecting suspicious activities, responding to incidents, and recovering after attacks. This shows that cyber security is not only about preventing cyber-attacks, but also about preparing organizations to manage threats before, during, and after incidents. Strong cyber security therefore requires technical tools, clear policies, regular updates, staff awareness, and continuous monitoring.

### Why it matters

Cyber security matters because the effects of an attack go far beyond computers. A cyber-attack can interrupt essential services, expose personal data, damage an institution's reputation, and lead to serious financial loss. In highly connected environments, one weakness can affect many other systems. This is why cyber security should be understood not only as an IT concern, but also as an issue of governance, planning, and risk management [1].

### Main cyber security functions

A useful way to understand cyber security is through its main functions: identify, protect, detect, respond, and recover. First, organizations need to identify important assets, risks, and responsibilities. Then they must protect systems through access control, data security, and maintenance. After that comes detection, which involves monitoring for suspicious behavior and possible incidents. If an attack occurs, the organization must respond quickly and clearly, and finally recover services while improving future readiness. This step-by-step view shows that cyber security is not only about preventing attacks, but also

about being prepared before, during, and after them [1]. As shown in Fig. 1, cyber security is commonly organized into five main functions: identify, protect, detect, respond, and recover.

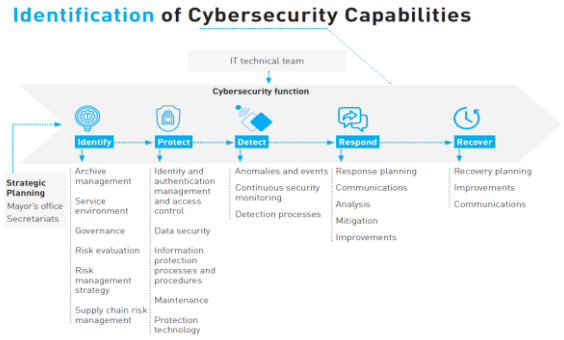


**Fig -1***:* Main cyber security capabilities, from identifying risks to recovery after incidents [1].

### A practical view

In real life, many cyber incidents happen because of simple weaknesses such as poor passwords, outdated software, weak access control, or low user awareness. So, strong cyber security is not based only on advanced tools. It also depends on routine good practice, staff training, and clear policies. In that sense, cyber security is not just a technical shield; it is a habit of responsible digital behavior [1].

## 2. PRIVACY PROTECTION IN LOCATION-BASED SERVICES

### What location-based services are:

Location-Based Services, or LBS, are services that use the location of a device to provide useful information or assistance. Common examples include navigation apps, nearby restaurant search, weather updates, emergency help, and friend-finder services. These services are popular because they are convenient and often highly accurate. Bettini explains that LBS can generally be grouped into personal services and social network services, depending on whether the location is mainly shared with the provider or also with other users [2].

### Why privacy is a concern

The privacy problem appears because location data can reveal much more than a person's current position. Over time, it may show where someone lives, works, shops, travels, or whom they meet. Bettini defines a privacy threat as a situation in which an unauthorized entity can connect a person's identity with private information. This means that a location history can reveal habits, routines, and even sensitive personal details. The risk becomes even greater when many location points are collected and analyzed together instead of being viewed separately [2].

### Who can threaten privacy

Privacy risks in LBS do not come from only one source. The service provider itself may become a risk if it uses data in unexpected ways. An outside attacker may try to intercept or steal the information. In some social-location systems, even other users may become privacy threats. Bettini also shows that the precision of location data and the frequency of requests are very important, because highly precise and repeated data make re-identification much easier [2].

### How privacy can be protected

Several methods have been proposed to reduce these risks. One common approach is to lower the precision of the shared location instead of sending the exact position. Other methods include anonymity techniques, obfuscation, dummy locations, and differential privacy approaches such as geo-in distinguishability, where controlled noise is added to protect the real position. However, stronger privacy often reduces service accuracy, so privacy protection in LBS is usually a balance between safety and utility rather than a perfect solution [2]. As shown in Fig. 2, privacy protection in location-based services can be achieved by transforming actual location records into obfuscated location records before they are sent to the service provider.

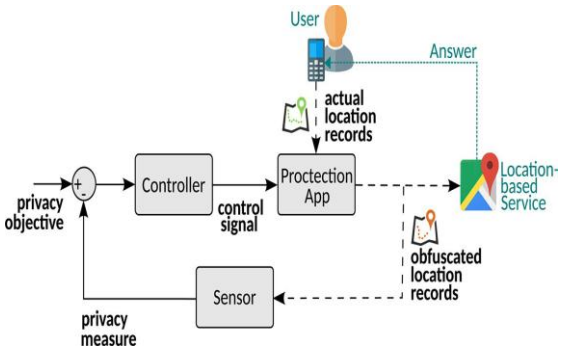


**Fig -2:** A privacy-protection model for location-based services using location obfuscation.

## 3. AGENT-BASED SYSTEMS

### Basic idea

Agent-based systems are software systems made up of autonomous agents that interact with one another and with their environment. Each agent has a role, makes decisions, and performs actions that contribute to a larger system goal. This approach is especially useful when the problem is distributed, dynamic, or difficult to manage from one central controller. Both classical and recent work show that agent-based systems are well suited to complex problems where communication, cooperation, and adaptability are important [3], [4].

### Why they are useful

The main strength of agent-based systems is that they reflect how many real-world systems actually work. Applications such as traffic control, healthcare support, logistics, and autonomous environments involve many entities acting at the same time. Instead of forcing everything into one rigid program, agent-based design allows each part of the system to operate with some independence while still cooperating with the others. This often makes the overall system more flexible, scalable, and responsive to change [3], [4].

### How they are designed

A classical design method is the UML-based process proposed by Cossentino and colleagues. In this method, use-case diagrams help identify agents and their roles, class diagrams describe their structure, and sequence or activity diagrams explain behavior and communication. An important idea in this process is iteration: agent structure and agent behavior are refined together until the system requirements are properly implemented. This makes agent-based design a structured engineering process rather than an informal idea [3].

### A modern direction

A more recent development is the integration of AI and machine learning into agent-based systems. Abu Maria and AlKhatib propose an AI-Driven Agent-Based System Development Framework in which AI and ML are incorporated into the full lifecycle of the system. This allows agents to learn from data, adapt to changing conditions, and improve decision-making. At the same time, the paper notes that challenges still remain, including complexity, the need for good-quality data, and the lack of unified standards [4]. As shown in Fig. 3, an agent-based system works through continuous interaction between the agent and its environment, where actions produce new states and feedback.

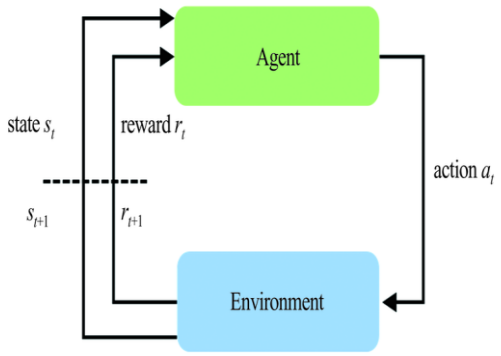


**Fig -3:** Basic interaction loop between an agent and its environment in an agent-based system.

## 4. DEEP LEARNING IN THE MEDICAL SECTOR

### Why deep learning matters in medicine

Deep learning has become one of the most influential technologies in the medical sector because it can learn useful patterns from large and complex datasets. In healthcare, these datasets may include medical images, pathology slides, biosignals, and clinical records. One of the strongest areas of progress has been medical imaging, where deep learning is now widely studied for classification, detection, segmentation, and decision support. This is why the selected figure fits the topic very well, especially if the section focuses on image-based medical applications [5], [6].

### Main applications

Deep learning has shown value in many medical tasks, including diabetic retinopathy detection, tumor analysis, lung nodule classification, thyroid diagnosis, fetal localization, and other imaging-based applications. Its main advantage is that it can identify subtle visual patterns that may be difficult to capture through traditional methods. At the same time, the literature shows that these systems are most helpful when they support clinicians rather than replace them, especially in tasks involving screening, triage, and image interpretation [5], [6].

### Challenges and responsibility

Even though deep learning is powerful, strong performance in research does not automatically mean safe use in real healthcare settings. The WHO guidance on AI for health stresses that safety, transparency, accountability, and human oversight are essential. In addition, medical AI systems can suffer from bias if training data are limited or unbalanced, which may affect fairness and reliability across patient groups. So the key issue is not only building accurate models, but also making sure they are ethical, well-evaluated, and used responsibly [7].

### Real-world use

Deep learning is already part of the broader regulatory conversation around AI-enabled medical devices. The FDA notes that AI-enabled medical devices are an active and growing area of oversight, which shows that this technology is moving from research into real clinical use. Even so, clinical deployment still requires careful validation, regulation, and monitoring. For that reason, the future of deep learning in medicine is promising, but its success depends on combining technical progress with safe and responsible practice [8]. As shown in Fig. 4, deep learning has been applied to a wide range of medical imaging tasks, including diabetic retinopathy detection, brain tumor detection, lung nodule classification, and thyroid diagnosis.

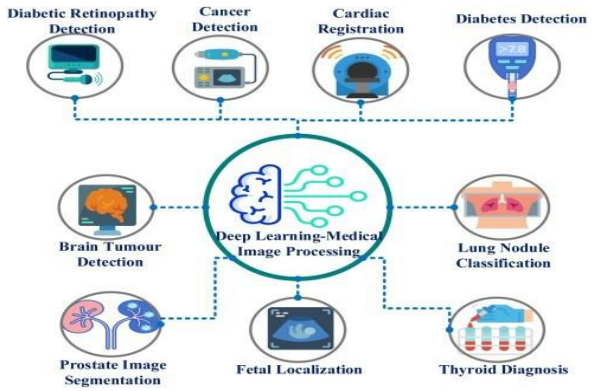


**Fig -4:** Examples of deep learning applications in medical image processing and diagnosis.

## 5. ISSUES OF INTEGRATION

In regarding to integration with location based services, agents can be integrated to enable users to search for nearest points of interests. However, privacy of users can be attached, by external intruders, especially if they have experience in applying advanced attacks such as location homogeneity and semantic location attacks as well as query analyzing attacks [9, 10, 11, 12, 13]. In addition, power consumption of mobile device battery comes to the top when trying to ensure high level of privacy as well as low complexity of privacy protection method to ensure continuity of using location based services applications [14]. Moving towards agents, they can be attacked by destination machines to change the code of the mission carried by the agent, the parameters of the tip of the mobile agent, or the results of the executed task carried by the agent. Actually, many works studied the security of agents [15, 16, 17]. In case of not taking into consideration such issue, systems are failed.

Moreover, when integrating of systems that ensure privacy protection in IoT-based infrastructures, big data, using data mining methods, and security of web applications must be taken into account [18, 19]. Otherwise, much vulnerability will be arisen.

As a special case in medical sector, using deep learning is ranked on the top during the COVID-19 years [20]. This means that ensuring good training with security of training data set and other datasets used to develop diagnostic systems [21, 22] must be considered to gain trust of users in medical companies (private of governmental).

## 6. CONCLUSIONS

Cyber security, privacy protection, software-agent security, and deep learning are strongly connected in modern digital systems. Cyber security is essential because digital services now support many critical sectors, including education, healthcare, transportation, business, and public services. Any weakness in these systems may lead to data leakage, service disruption, financial loss, and reduced user trust. Privacy protection is also highly important in location-based services because users' location records can reveal private habits, daily routines, and sensitive personal information. Agent-based systems provide useful solutions for distributed and dynamic environments, but they must be protected against attacks that may modify their code, data, parameters, or mission results. Deep learning offers strong benefits in the medical sector, especially for diagnosis and image analysis, but it also requires secure datasets, ethical use, transparency, validation, and human oversight. Therefore, successful integration of these technologies depends not only on technical performance, but also on secure design, privacy-aware processing, governance, and continuous monitoring. Overall, responsible cyber security practices are necessary to ensure safe, trusted, and reliable digital transformation.

## ACKNOWLEDGEMENT

The author take help of ChatGPT to present illustrative figures as well as for proof reading. However, the basic scientific content is presented by the author.

## REFERENCES

1) L. Cotino and M. Sánchez, A Cyber security Guide for Smart Cities. Inter-American Development Bank, 2021.

2) C. Bettini, "Privacy Protection in Location-Based Services: A Survey," in Handbook of Mobile Data Privacy. Springer, 2018.

3) M. Cossentino, A. Chella, and U. Lo Faso, "Designing agent-based systems with UML."

4) K. Abu Maria and A. A. AlKhatib, "Bridging the Gap: AI-Driven Agent-Based Systems in Modern Software Engineering," Journal of Information Systems Engineering and Management, vol. 10, 2025.

5) Esteva, A., Chou, K., Yeung, S. et al. Deep learning-enabled medical computer vision. npj Digit. Med. 4, 5 (2021). https://doi.org/10.1038/s41746-020-00376-2

6) Aggarwal, Ravi, Viknesh Sounderajah, Guy Martin, Daniel SW Ting, Alan Karthikesalingam, Dominic King, Hutan Ashrafian, and Ara Darzi. "Diagnostic accuracy of deep learning in medical imaging: a systematic review and meta-analysis." NPJ digital medicine 4, no. 1 (2021): 65.

7) World Health Organization, Ethics and Governance of Artificial Intelligence for Health, 2021. (World Health Organization)

8) U.S. Food and Drug Administration, “Artificial Intelligence-Enabled Medical Devices,” 2025. (U.S. Food and Drug Administration)

9) Mohamad Shady Alrahhal, Maher Khemakhem and Kamal Jambi, "A Survey on Privacy of Location-Based Services: Classification, Inference Attacks, and Challenges," Journal of Theoretical and Applied Information Technology, vol. 95, no. 24, 2017.

10) Mohamad Shady Alrahhal, Maher Khemakhem and Kamal Jambi, "Agent-Based System for Efficient kNN Query Processing with Comprehensive Privacy Protection," International Journal of Advanced Computer Science and Applications, vol. 9, no. 1, 2018.

11) Mohamad Shady Alrahhal, Muhammad Usman Ashraf, Adnan Abesen and Sabah Arif, "AES-Route Server Model for Location Based Services in Road Networks," International Journal of Advanced Computer Science and Applications, vol. 8, no. 8, 2017.

12) Hosam Alrahhal et al., "A symbiotic relationship based leader approach for privacy protection in location based services," ISPRS International Journal of Geo-Information, vol. 9, no. 6, p. 408, 2020.

13) Abdullah S. Alyousef, Karthik Srinivasan, Mohamad Shady Alrahhal, Majdah Alshammari and Mousa Al-Akhras, "Preserving Location Privacy in the IoT against Advanced Attacks using Deep Learning," International Journal of Advanced Computer Science and Applications, vol. 13, no. 1, 2022.

14) Mohamad Shady Alrahhal, Maher Khemekhem and Kamal Jambi, "Achieving load balancing between privacy protection level and power consumption in location based services," International Research Journal of Engineering and Technology, vol. 5, no. 3, pp. 619-625, 2018.

15) Bandar Alluhaybi, Mohamad Shady Alrahhal, Ahmed Alzhrani and Vijey Thayananthan, "A Survey: Agent-based Software Technology Under the Eyes of Cyber Security, Security Controls, Attacks and Challenges," International Journal of Advanced Computer Science and Applications, vol. 10, no. 8, 2019.

16) Bandar Alluhaybi, Mohamad Shady Alrahhal, Ahmed Alzhrani and Vijey Thayananthan, "Dummy-based approach for protecting mobile agents against malicious destination machines," IEEE Access, vol. 8, pp. 129320-129337, 2020.

17) Bandar Alluhaybi, Mohamad Shady Alrahhal, Ahmed Alzhrani and Vijey Thayananthan, "Achieving self-protection and self-communication features for security of agent-based systems," 2020.

18) Majed Abdullah Albarrk and Mohamad Shady Alrahhal, "Web Applications Security: More Collaboration," 2020.

19) Mohamad Shady Alrahhal and Adnan Abi Sen, "Data mining, big data, and artificial intelligence: An overview, challenges, and research questions," 2018.

20) Mohamad Shady Alrahhal and Majed Abdullah Albarrk, "A Survey of the COVID-19 Epidemic Through the Eyes of Artificial Intelligence and Deep Learning: Challenges and Research Questions," 2020.

21) Mona Alfifi, Mohamad Shady Alrahhal, Samir Bataineh and Mohammad Mezher, "Enhanced Artificial Intelligence System for Diagnosing and Predicting Breast Cancer using Deep Learning," International Journal of Advanced Computer Science and Applications, vol. 11, no. 7, 2020.

22) Mohamad Shady Alrahhal and Eftkhar Alqhtani, "Deep learning-based system for detection of lung cancer using fusion of features," International Journal of Computer Science and Mobile Computing, vol. 10, no. 2, pp. 57-67, 2021.