Mobile Agents in the Medical Care Domain

Subjects: Computer Science, Interdisciplinary Applications

Contributor: Pradeep Kumar, Kakoli Banerjee, Niraj Singhal, Ajay Kumar, Sita Rani, Raman Kumar, Cioca Adriana Lavinia

A mobile agent is a software application that moves naturally among hosts in a uniform and non-uniform environment; it starts with one host and then moves onto the next in order to divide data between clients. The mobile paradigm is utilized in a wide assortment of medical care applications such as the medical information of a patient, the recovery of clinical information, the incorporation of information pertaining to their wellbeing, dynamic help, telemedicine, obtaining clinical data, patient administration, and so on. The accompanying security issues have grown in tandem with the complexity and improvements in mobile agent technologies. As mobile agents work in an insecure environment, their security is a top priority when communicating and exchanging data and information. Data integrity, data confidentiality and authentication, on-repudiation, denial of service, and access control, are all key security concerns with mobile agent migration.

Keywords: mobile agent migration ; security ; privacy ; healthcare

1. Introduction

Mobile agents [1] are innovations that originated in two distinct disciplines. The first discipline concerns artificial intelligence, and the idea that an intelligent agent is created [2]. The second discipline concerns distributive computing, wherein a mobile agent is created via code mobility. A legitimate definition for mobile agents, regarding the two referenced disciplines, is that they are smart programming substances that can pause and resume their tasks automatically, on various platforms, in order to complete assigned tasks [3]. A relocating mobile agent undertakes a process that is independent; it can navigate its way through, and adapt to, a heterogeneous environment, moving from platform to platform, and interfacing with different mobile agents. Mobile agents automatically [4] decide where and when to migrate, and they may execute their task at anytime, or they may suspend the execution of that task altogether, move to another host, and proceed with executing the task on that host instead. Characteristics of mobile agents are:

- Mobility: Mobile agents can freeze an operation on one platform and continue with the operation on another (i.e., inside a different region. This is often referred to as agent migration) [5].
- Individualism: Each mobile agent is guided by a program that is especially written to achieve at least one goal. The operations of mobile agents are entirely governed by this code, with no direct intervention from other groups.
- Reactivity: Mobile agents respond to environmental changes in order to accomplish their objectives.
- Proactivity: Mobile agents change their current circumstances and they take a few attempts to accomplish their objectives.
- Sociability refers to a mobile agent’s ability to interact with other mobile agents. This is important because some agents are only made aware of their present situation via communication with other agents.

1.1. Protection of Mobile Agents

A prime concern is the security of mobile agents [6]. The manner in which mobile agents work is shown in **Figure 1**. The security of mobile agents can be threatened via different dangerous assaults. Several types of attacks, including denial of service (DOS), masquerading, specialist and host cracking, renunciation, eavesdropping, information and data manipulation, and so on, are possible due to the mobile agents’ dynamic behavior.

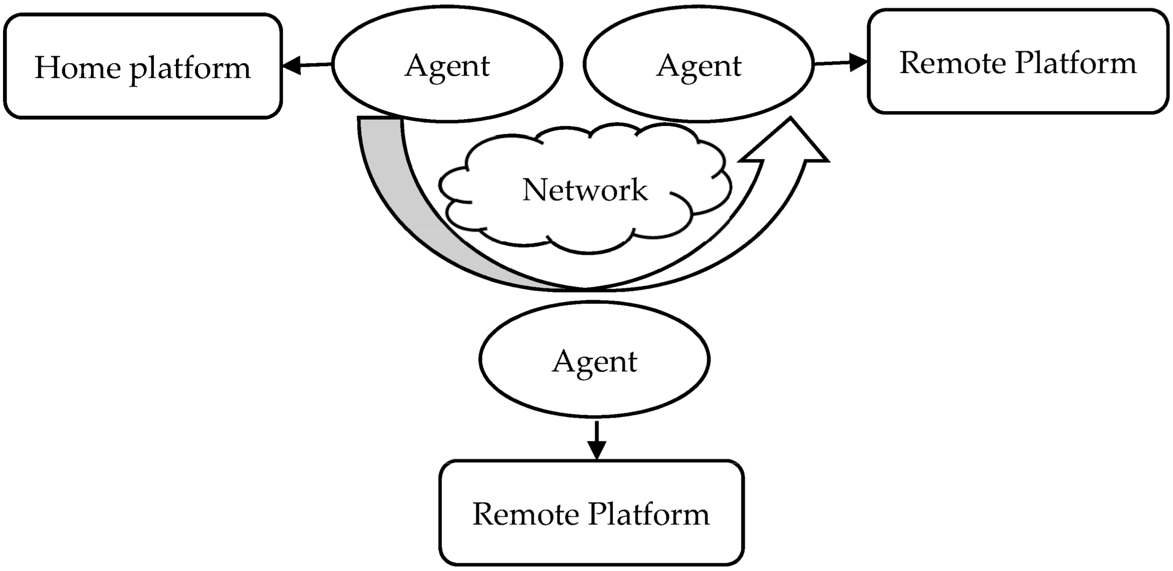

Figure 1. Main security threats to mobile agent technology.

Mobile agent technology suffers from security threats [7], which are divided into four main categories:

- Assault from agents on platforms;
- Agent-to-Agent Assaults;
- Assault from platforms on agents;
- Additional Assault to Agent Platform.

The challenges when implementing mobile agents include security risks [8], protection of hosts from malevolent specialists, protection of agents from noxious hosts, efficiency, flexibility, mobility, and standardization.

1.2. Mobile Agent Life-Cycle

The life-cycle of [9] the mobile agents (displayed in **Figure 2**) guarantees that they can adjust the climate (i.e., either at home or in an unfamiliar climate). They can switch between one hub and another, and they can hone in on their last result.

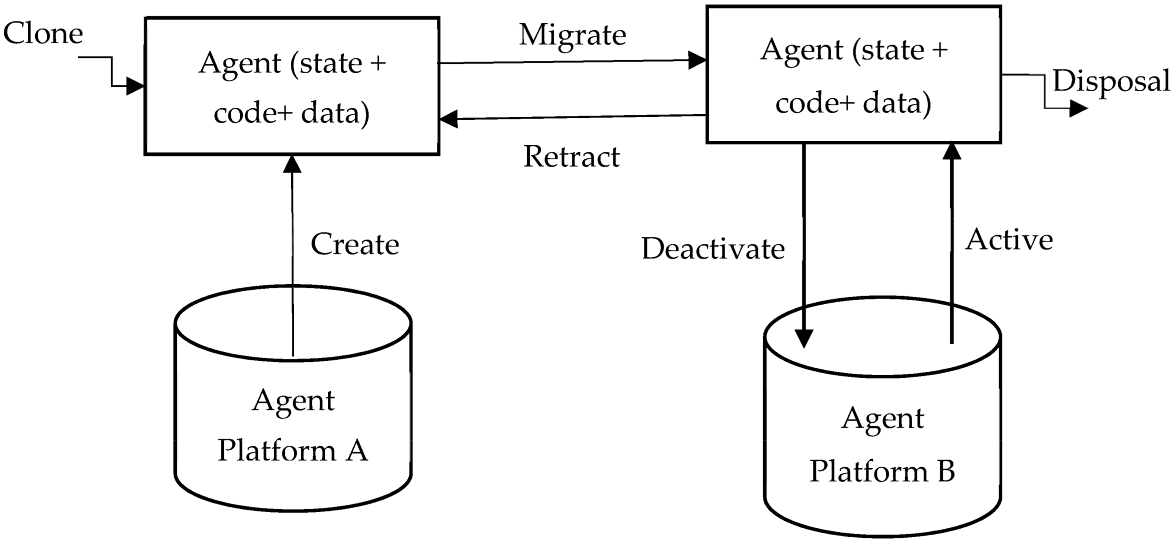

Figure 2. Mobile agent life-cycle [10].

- Creation: A new mobile agent is made, and the conditions of the mobile agent are initiated.
- Cloning: A specialist copy is made, and the present status of the first is duplicated in order to create cloning agents.
- Dispatch: A mobile agent moves to another host.

- Deactivation: The state of a mobile agent is saved in the repositories when it is in standby mode.

- Activation: The state of a deactivated mobile agent is restored from the repositories and applied to the lifetime mobile agent.

- Retraction: A mobile agent can converse with another agent and the stage.

- Disposal: The life-cycle of a mobile agent ends.

- Communication: Interactions between mobile agents and platforms.

2. Utilization of Mobile Agents in the Medical Care Domain

Mobile agents are used in a variety of medical-related activities [11], such as obtaining clinical information on executives, clinical data recovery, integrating information pertaining to a patient's wellbeing, obtaining general clinical information, and so on. The use of mobile agents in the medical care sector ensures medical data integration [12] by combining information from different medical data sources, as shown in **Figure 3**.

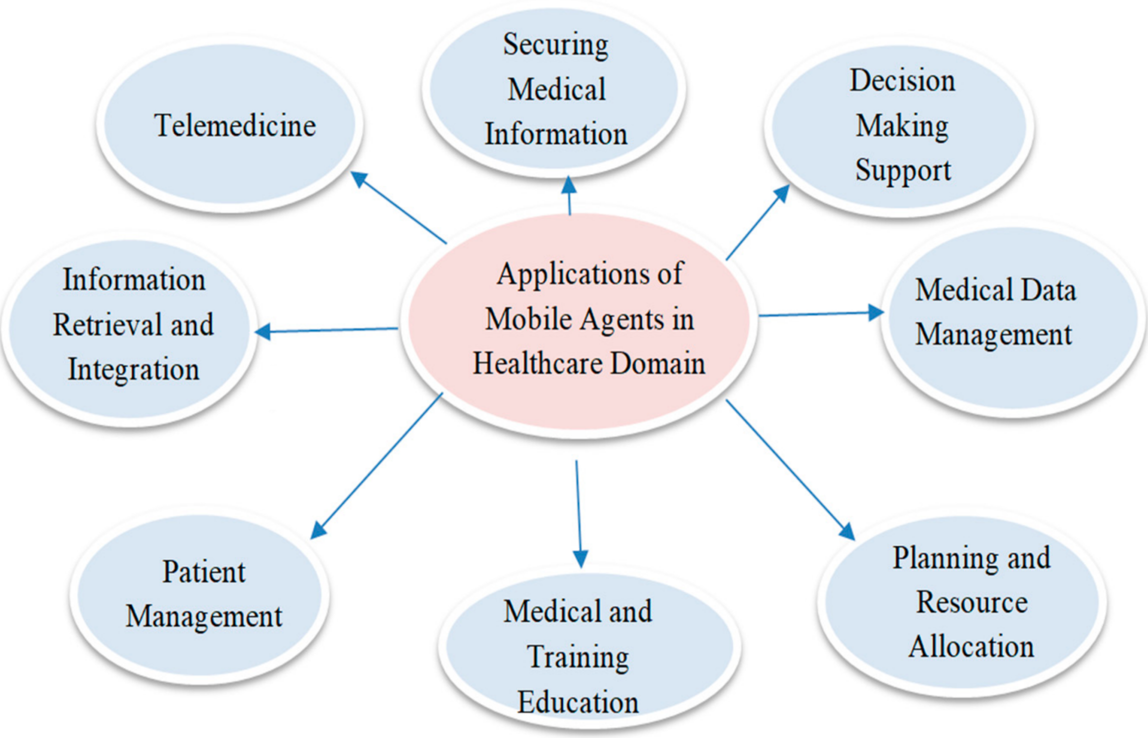
Securing Medical Information
Telemedicine
Decision Making Support
Information Retrieval and Integration
Applications of Mobile Agents in Healthcare Domain
Medical Data Management
Patient Management
Planning and Resource Allocation
Medical and Training Education

Figure 3. Applications of mobile agents in the healthcare domain.

- Health Data Management: Acquiring, analyzing, and protecting medical information [13].

- Information Retrieval: Retrieving medical information from heterogeneous databases.

- Decision-Making Support: Assisting healthcare workers with procedures, including treatments and diagnostics.

- Telemedicine: Systems focused on remotely monitoring the situation with patients, thus allowing for a wide range of assessments.

- Securing Medical Information: Approaches to working, bearing in mind the wellbeing and security of patient information.

Figure 4 and **Figure 5** represent the real-time application of mobile agents in healthcare.

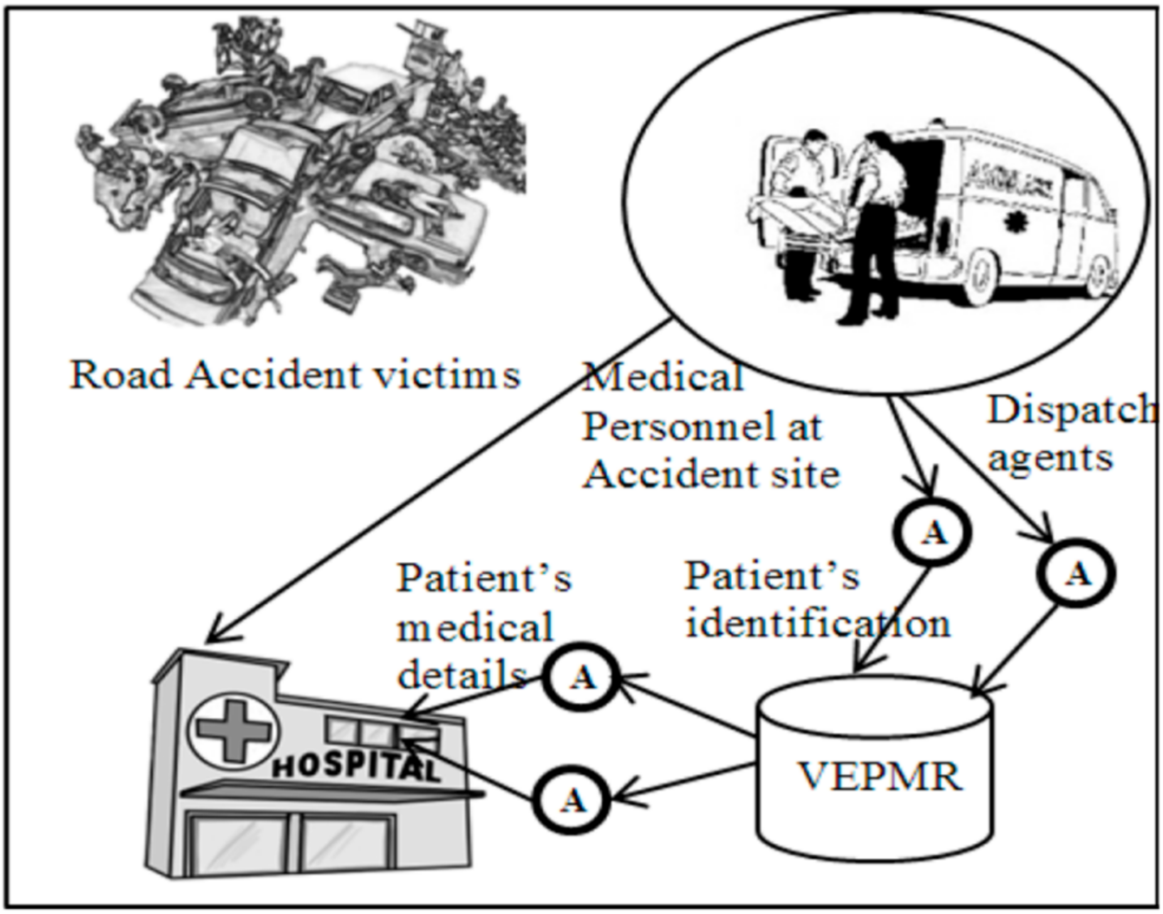

Figure 4. Application of a mobile agent in a road accident.

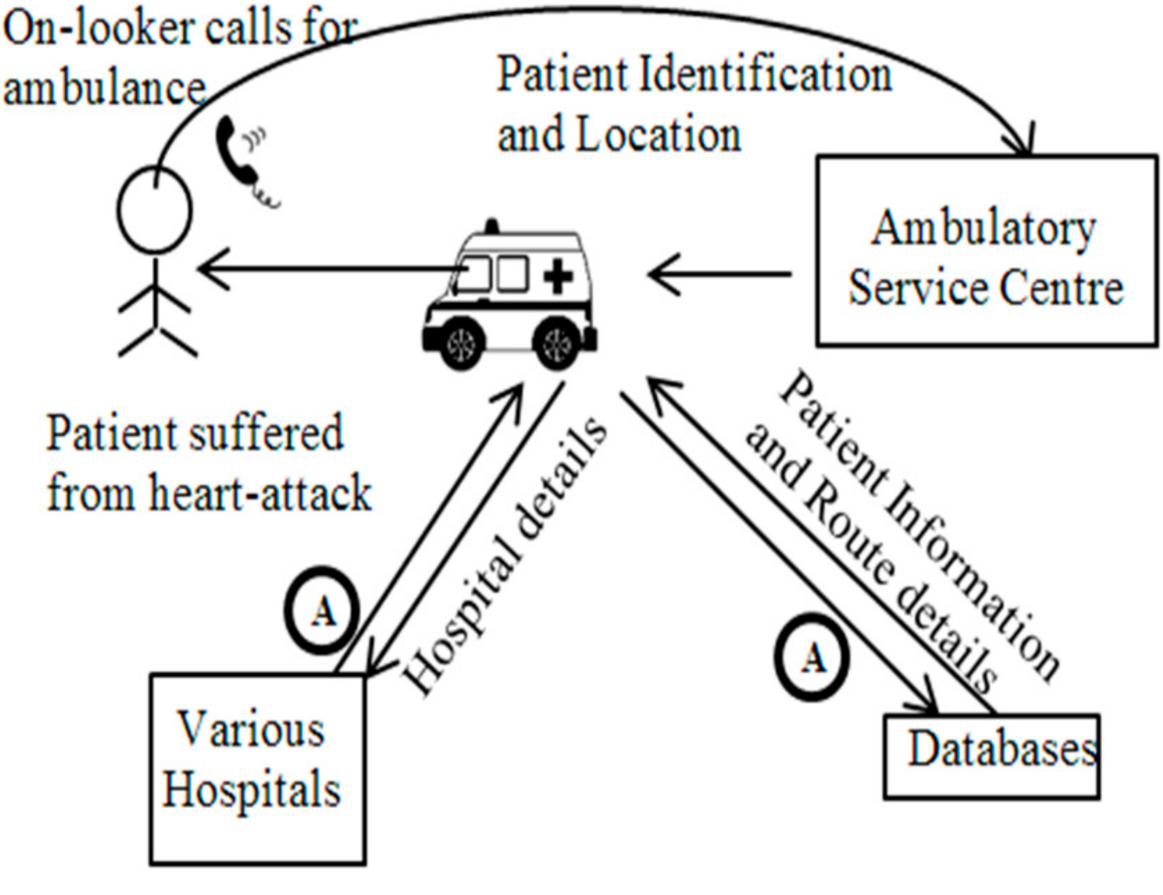
On-looker calls for ambulance
Patient Identification and Location
Ambulatory Service Centre
Patient suffered from heart-attack
Hospital details
Patient Information and Route details
A
A
Various Hospitals
Databases

Figure 5. Application of a mobile agent in an emergency.

Requirement of Security

Security is a pressing issue for mobile agents [14] as they migrate from user to user. Security parameters are shown in **Figure 6**.

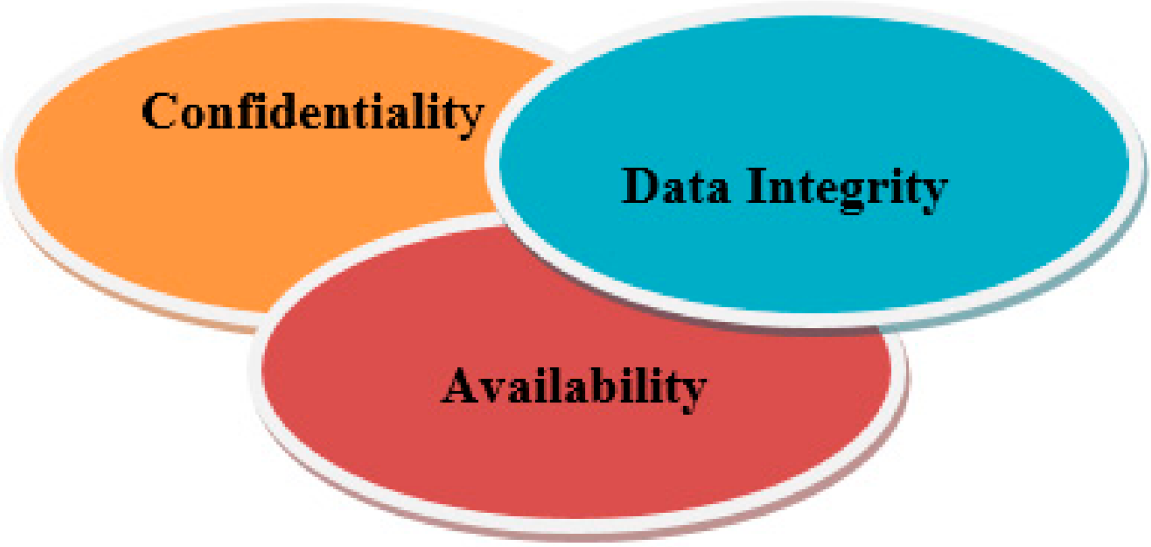

Figure 6. Security parameter.

- Confidentiality: Security of information and data (state + data + code) [6] among platforms and agents.
- Data integrity: Data and information [15] should not be interfered with by a third party.
- Availability: Data and information requested by the platform or agents should be easily accessible.

3. Verifiable, Secure Mobile Agent Migration in Healthcare Systems Using a Polynomial-Based Threshold Secret Sharing Scheme with a Blowfish Algorithm

Liu et al. [8] proposed a model based on the fusion of a virtual integrated clinical database system with the mobile agent paradigm. Mobile agents help send information between different medical clinics, and the proposed model was utilized to incorporate information from different clinical data frameworks. This model was seen as having exceptionally favourable uses for the following reasons: patient information was regularly, and immediately, obtained by the medical clinics, saving a great deal of time [4]; needless patient trials did not occur in some clinics, which saved time for crises; and it guaranteed secure and productive information sharing.

The framework was executed as follows:

- A patient arrived at the hospital, and the medical faculty requested the patient’s vital clinical records via a VI (Visualized Interface).
- A MAS (Mobile Agent Scheduler) [16] dispatched portable specialists to outside organizations and emergency clinics, in order to solicit and assemble data. When the portable specialist arrived at the outside organization, it finished the check assessment initiated by the MAS of the outside establishment, accumulated data from the outside foundation’s CIS (Clinical-information Index Storage), and it continued its journey to the organization.
- After visiting all of the required institutions, the mobile agents returned to the organization at which they were assigned. The list items were saved in the CIS and displayed via the VI, which allowed the specialists to make better decisions.

Burstein et al. [17] presented a design that consolidated the mobile agents’ ideas, and considered how they could dynamically help in the medical care crisis space. This paper explicitly demonstrates how to utilize mobile agents in order to help disorganized administrations. First, a crisis circumstance is considered, wherein a moderately aged man experiences cardiovascular failure. The onlookers promptly call for an emergency vehicle, noting the area and nature of the problem, any recognizable identification on the patient, and so forth. When on route to the site of the incident, paramedics dispatch pair of mobile agents. First, the mobile agents travel to the medical clinics close to the site of the incident in order to understand whether accessible specialists, attendants, beds, or offices will be required. The second mobile agent recovers the patient’s clinical history, as well as the attributes of the chosen emergency clinic. This ensures that when the paramedics arrive at the crisis site, their onboard terminal in the rescue vehicle now mirrors the nearby clinics’ terminals, which are ordered from the most to least helpful, in accordance with the situation.

Additionally, the paper noted how subtle clinical information pertaining to the patient, and subtle information concerning the local environment, are accessible. When heading to the chosen emergency clinic, a message is conveyed to the related emergency clinic specialist. When the rescue vehicle arrives at the medical clinic, this data lets the trauma center and health worker know how to plan for the appearance of a patient. This paper concludes by arguing that mobile agents are helpful in situations in which the accuracy of information is critical for a successful decision.

Orgun [18] focuses on a scenario wherein patients change medical clinics and have numerous episodes in different medical services offices, thus prompting patient-related data to be divided into different frameworks. The authors suggested an electronic medical agent model that uses various participating versatile specialists in order to effectively access, translate, learn, and take advantage of the data that is available on different wellbeing frameworks. This multi-agent framework, with a metaphysical component that is dependent on HL7, works with the accumulation of patient data across an entire medical service association. The electronic medical mgent model comprises different agents from different servers, including a merchant agent and a cosmology server. A server for agents provides an interface for the information. Applications are set up on the electronic medical agent model network, and they are composed of the aforementioned information in various configurations, with various field names, and the data is able to be compared with that of a similar patient. An agent merchant monitors every one of the agents in the framework at a random time, in addition to the library of the numerous partaking applications and datasets in the medical services association.

Chaouch et al. [19] analyzed mobile agent-based structures DiabMAS (Diabetes Multi-Agent System) for the remote clinical assessment of diabetic patients. The argument for deploying mobile agents is to reduce traffic by assigning agents to locations where activities can be completed and message transmissions are closed, thus reducing network stress. Here, the key idea is to screen and assure patients, thus diminishing costs with regard to the advancement of patient diseases, and furthermore, creating a movement that provides a moderate degree of satisfaction.

Hsu [20] focused on telemedicine, and they alluded to an application that couples the innovation of PC technology and correspondence with clinical advantages. It will be available in different forms: tele-education, tele-conference, tele-medical procedures, and tele-observing. Here, the principal impetus behind this project is to design a protected specialist that can implement telemedicine-based pair-to-pair organizing. The design of a pair-to-pair network based on the JXTA convention utilizes two models of telemedicine administration: unsurprising and erratic administrations. When a mobile agent holding patient data begins its journey by starting on one spot, before moving onto the next through the web, it tends to be assaulted by malevolent agents; therefore, the design utilizes a two-layer security component in order to answer agent-based telemedicine administrations for mobile agents. Security necessities require the design to be: non-renounceable, private, dependable, and consistent.

Pouyan [21] describes a three-layer agent-based paradigm for e-health care that consists of collecting, evaluating, controlling, and eventually conducting patient-related services via the internet in real-time. Patients, healthcare clinics, and the central hospital comprise the three tiers. Physicians, nurses, trainers, and representatives can be from any sector to form a dynamic virtual team. All of these actors are mobile agents. A specific agent that represents a patient’s description, circumstances, and health, assigns the patient to a specific member of healthcare staff. Some medication data is entered into a database in accordance with the to the responsibilities allocated to each member of healthcare staff. The diagnostics group sends the request to the central institution in order to obtain data from the data system.

Benachenhou [22] examined the utilization of mobile specialist innovations in terms of their ability to correspond between various distant areas. This is a particularly pertinent consideration for when a crisis happens, particularly in mass setback occurrences when a large number of casualties need clinical consideration. This paper examines the utilization of mobile agents for the quicker and exact recovery of information, when legitimate medical care hardware or the examination of clinical data is beyond the realm of possibility. The author gives a description of a crisis wherein a group of individuals is affected by eye contamination. The paper showed that scanning for, and enquiring into, expert care for every single case set aside time.

Indeed, the paper showed that if every one of the specialists was assumed to reach out to experts by sending them the medical profiles of every single patient, tumult and blockage will unquestionably ensue, thus ensuring that not even one of them will receive help; however, if it is assumed that the experts contact every single patient, the correspondence traffic will be decreased, though, it will still take a great deal of time. The paper indicated that affected individuals will visit nearby medical service communities. Nearby clinical official investigations will receive data from patients that will be stored in the neighborhood framework. A unique clinical office will dispatch a specialist, or several specialists, to all servers in order to observe the aftereffects of essential tests on affected eyes. These officials will receive answers to their information requests.

Biswas [23] considered straight (t, n) secret sharing plans, and they noticed some of its benefits. The proposed (t, n) edge plot depended on Shamir's SS scheme. The paper gives an itemized security investigation of every one of the three periods of the SS scheme, including the specific offer being made, secret key reproduction, and mystery key approval. In any case, two, rather than one, irregular polynomial plans for producing two offers for each member are utilized. In this plan, one polynomial is utilized to divide confidentiality between t or more members, and the other is utilized to approve the mystery key and to discover cheating, assuming that it happens. The plan does not utilize any stolen work that has been discovered; in any case, the coefficients of the two polynomials are connected, and thus, the offers made by them are connected. The plan utilizes two arbitrary polynomials, with one normal coefficient between them. For offers made as a result of cheating, both the polynomials are altered, and thus, (t-1) effective cheating methods carried out by deceptive members can be rendered unimportant. Hence, this plan is useful as it does not involve other conditions to discover cheating, and it includes additional calculations to check such conditions.

Ahmed El-Yahyaoui [24] introduced an encryption plot, wherein the clamor is steady and does not rely upon the homomorphic assessment of ciphertexts. The homomorphy of the plan is derived from basic lattice tasks (expansion and increase). In a cloud environment, the operating period of the cryptography aims for enhancement action, and it logs a request for a few milliseconds. The author proposed a novel homomorphic cryptography scheme that is indisputable. It consists of a symmetric, commotion-free, probabilistic encryption with a non-commutative ring quaternionic cipher text space. The proposed encryption has a viable application in terms of its ability to offer sound calculations, in an environment of scrambled information, during distributed computation; this can be applied to the protection of a large amount of information. It is an efficient and practical scheme, the safety of which hinges on resolving an over-characterized set of quadratic multidimensional polynomial requirements in a non-commutative ring. The two key aspects of the strategy are homomorphy and confidence. The proposed approach allows a remote, unreliable, networked computing system to conduct sophisticated computations over scrambled data while allowing the customer to verify the accuracy of their rethought actions throughout the decryption process.

Alexeis Garcia-Perez [25] notes the fact that as countries transition into a post-industrial world, where understanding the economy is characterized by radical innovations in the information technology area, the digital transformation of the health industry is crucial. In order to sustain sectoral growth and to fortify against its fragility by deploying the newest technologies, their use in the health and care ecosystem must be managed properly in terms of cyberresilience.

Patel [26] explored the principle objective of dissecting the presentation of these calculations using documents that had either a little or a large amount of information. The runtime and amount of storage used by these computations during the operation are factors to consider. The experimental results and graphic research show which computation is the most suitable for small and large datasets. Scientific outcomes portray the more reasonable calculation for time and memory imperative frameworks. Velibor Božić [27] underlines the difficulty of managing health risks. IT, usernames, and passwords are insufficient to describe manager risk assessment competencies. The incorporation of risk mitigation into medicine must be planned as a program with a multimodal team as the sector is significantly larger and more complicated.

References

1. Tardo, J.; Valente, L. Mobile agent security and Telescript. In COMPCON'96. Technologies for the Information Superhighway Digest of Papers; IEEE: Piscataway, NJ, USA, 2002; pp. 58–63.
2. Narad, M.S.K. Group Authentication Using Back-propagation Neural Network. Int. J. Adv. Res. Comput. Commun. Eng. 2017, 6, 272–278.
3. Yao, M. A Security Architecture for Protecting Dynamic Components of Mobile Agents. Doctoral Dissertation, Queensland University of Technology, Brisbane City, QLD, Australia, 2004.
4. Chen, T.-L.; Chung, Y.-F.; Lin, F.Y.S. Deployment of Secure Mobile Agents for Medical Information Systems. J. Med. Syst. 2011, 36, 2493–2503.
5. Esparza, O.; Soriano, M.; Muñoz, J.L.; Forné, J. A protocol for detecting malicious hosts based on limiting the execution time of mobile agents. In Proceedings of the Eighth IEEE Symposium on Computers and Communications. ISCC 2003, Kemer-Antalya Turkey, 3 July 2003.
6. Al-Jaljouli, R.; Abawajy, J.H. Secure Mobile Agent-based E-Negotiation for On-Line Trading. In Proceedings of the 2007 IEEE International Symposium on Signal Processing and Information Technology, Giza, Egypt, 15–18 December 2007; pp. 610–615.
7. Jansen, W. Countermeasures for mobile agent security. Comput. Commun. 2000, 23, 1667–1676.

8. Bagga, P.; Hans, R. Applications of Mobile Agents in Healthcare Domain: A Literature Survey. Int. J. Grid Distrib. Comput. 2015, 8, 55–72.
9. Cavalcante, R.C.; Bittencourt, I.I.; da Silva, A.P.; Silva, M.; Costa, E.; Santos, R. A survey of security in multi-agent systems. Expert Syst. Appl. 2012, 39, 4835–4846.
10. Kumar, P.; Singhal, N.; Singh, S. Anonymous Scheme for Secure Mobile Agent Migration Using Mignotte's Sequence and Back Propagation Artificial Neural Networks. Int. J. Comput. Inf. Syst. Ind. Manag. Appl. 2021, 13, 192–199.
11. Santos-Pereira, C.; Augusto, A.B.; Cruz-Correia, R.; Correia, M.E. A secure RBAC mobile agent access control model for healthcare institutions. In Proceedings of the 26th IEEE International Symposium on Computer-Based Medical Systems, Porto, Portugal, 20–22 June 2013; pp. 349–354.
12. Vieira-Marques, P.M.; Robles, S.; Cucurull, J.; Cruz-Correia, R.J.; Navarro, G.; Marti, R.; Navarro-Arribas, G. Secure Integration of Distributed Medical Data Using Mobile Agents. IEEE Intell. Syst. 2006, 21, 47–54.
13. Fortino, G.; Trunfio, P. Internet of Things Based on Smart Objects; Springer: Berlin/Heidelberg, Germany, 2014.
14. Kumar, P.; Vatsa, A.K. Novel Security Architecture and Mechanism for Identity based Information Retrieval System in MANET. Int. J. Mob. Adhoc Netw. 2011, 1, 397–404.
15. van der Haak, M.; Wolff, A.; Brandner, R.; Drings, P.; Wannenmacher, M.; Wetter, T. Data security and protection in cross-institutional electronic patient records. Int. J. Med. Inform. 2003, 70, 117–130.
16. Fong, C.-H.; Parr, G.; Morrow, P. Security Schemes for a Mobile Agent Based Network and System Management Framework. J. Netw. Syst. Manag. 2010, 19, 230–256.
17. Burstein, F.; Zaslavsky, A.; Arora, N. Context-aware mobile agents for decision-making support in healthcare emergency applications. In International Workshop on Context Modeling and Decision Support: 05/07/2005-05/07/2005; CEUR Workshop Proceedings: Vienna, Austria, 2005; Volume 144.
18. Orgun, B.; Vu, J. HL7 ontology and mobile agents for interoperability in heterogeneous medical information systems. Comput. Biol. Med. 2006, 36, 817–836.
19. Chaouch, Z.; Tamali, M. A Mobile Agent-Based Technique for Medical Monitoring (Supports of Patients with Diabetes). Int. J. Comput. Model. Algorithms Med. 2014, 4, 17–32.
20. Hsu, W.-S.; Pan, J.-I. Secure Mobile Agent for Telemedicine Based on P2P Networks. J. Med. Syst. 2013, 37, 9947.
21. Pouyan, A.A.; Ekrami, S.; Taban, M. A Distributed E-health Model Using Mobile Agents. In Proceedings of the Seventh International Conference on Autonomic and Autonomous Systems, Venice/Mestre, Italy, 22–27 May 2011; pp. 7–12. Available online: http://www.thinkmind.org/index.php?view=article&articleid=icas_2011_1_20_20065 (accessed on 15 August 2021).
22. Benachenhou, L.; Pierre, S. Protection of a mobile agent with a reference clone. Comput. Commun. 2006, 29, 268–278.
23. Biswas, A.K.; Dasgupta, M. Two polynomials based (t, n) threshold secret sharing scheme with cheating detection. Cryptologia 2020, 44, 357–370.
24. El-Yahyaoui, A.; EL Kettani, M.D.E.-C. A Verifiable Fully Homomorphic Encryption Scheme for Cloud Computing Security. Technologies 2019, 7, 21.
25. Garcia-Perez, A.; Cegarra-Navarro, J.G.; Sallos, M.P.; Martinez-Caro, E.; Chinnaswamy, A. Resilience in healthcare systems: Cyber security and digital transformation. Technovation 2022.
26. Patel, K. Performance analysis of AES, DES and Blowfish cryptographic algorithms on small and large data files. Int. J. Inf. Technol. 2019, 11, 813–819.
27. Demster, B. Managing Information and Security in Healthcare; Bloomsbury Publishing: London, UK, 2013.

Retrieved from https://encyclopedia.pub/entry/history/show/84303