IJAREEIE

e-ISSN: 2278-8875
p-ISSN: 2320-3765

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

Volume 11, Issue 3, March 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.282

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE)

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.282|

|| Volume 11, Issue 3, March 2022 ||

DOI:10.15662/IJAREEIE.2022.1103026

Mobile Agent-based Systems for Information Leakage Prevention: A Critical Review of Distributed Models and Intrusion Detection Mechanisms

Surendranath Gowda D C[1], Nandish A C[2], Rakesh M[3], Ranganth S L[4], Vinod Kumar S[5]

Assistant Professors, Department of Computer Science and Engineering, City Engineering College, Bengaluru, Karnataka, India[1,2,3,4,5]

ABSTRACT: The rise of cloud and distributed computing has led to an increase in threats related to data and information technology, making data security and leakage prevention critical in these environments. Mobile agent-based systems have emerged as innovative solutions for detecting and mitigating data intrusions and leaks across networks. This paper aims to address various challenges associated with Mobile Agent-Based Information Leakage Prevention by offering a thorough and systematic examination of the Distribution Model for this purpose. It includes a review of selected research articles published between 2009 and 2019, providing a critical analysis of distributed mobile agent-based intrusion detection systems, focusing on their design, methodologies, and limitations. Initially, a total of eighty-five papers were considered for this review. The proliferation of cloud and distributed computing has introduced new risks to data security, including vulnerabilities that can lead to data breaches and information leakage. As organizations increasingly rely on these infrastructures, protecting sensitive data has become a top priority. Traditional security measures often fall short in distributed environments, where data moves across various nodes and networks. Mobile agent-based systems have emerged as a promising solution to enhance data security and detect intrusions in such environments. This paper provides a comprehensive review of mobile agent-based approaches for preventing information leakage, particularly focusing on the challenges of implementing distributed models in intrusion detection systems. By analyzing research published between 2009 and 2019, the paper evaluates how mobile agents operate across networks, identifying potential threats and preventing data loss. The review covers key methodologies, design considerations, and the effectiveness of these systems in real-world scenarios. Out of an initial pool of eighty-five papers, the selected studies are critically examined to highlight both the strengths and limitations of mobile agent-based intrusion detection. This review aims to contribute to the ongoing discourse on data security, offering insights into future advancements and potential improvements in mobile agent technology for leakage prevention.

KEYWORDS: Mobile Agent, Distribution Model, Data Leakage Detection, Data Leakage Prevention, DLP, Security, Distributed Computing

I. INTRODUCTION

The rapid expansion of information technology and cloud computing has heightened concerns about data leakage, manipulation, and distribution. As reliance on cloud computing grows, so do concerns about the security and privacy of data within distributed networks [1]. Many businesses have fallen victim to theft, loss, or leakage of sensitive data, which can significantly damage both individual and corporate reputations and trust [2]. A prevalent cause of data leakage is the casual or negligent behaviour of employees handling shared files containing confidential information, business documents, financial statements, policies, contracts, intellectual property, and other private data [3]. When such data is transmitted through covert channels, unauthorized access becomes more likely, as these channels bypass conventional security mechanisms, leading to unintentional data leakage [4]. Research indicates that 90% of corporate data leakage could be mitigated with improved data security and leakage prevention strategies [5]. Internal security breaches often stem from deceptive attacks using legitimate credentials or insider threats. Studies [6] and [7] highlight the critical importance of information security within corporate settings, and [8] introduces a hybrid framework for detecting and preventing information leakage. Thus, information security remains a crucial area in IT, aimed at ensuring a secure computing environment for both individuals and businesses. This paper provides a critical review of distributed models for mobile agent-based data leakage prevention. The review encompasses research papers published from 2009 onwards, focusing on distributed mobile agent-based intrusion detection and prevention systems. It evaluates these systems in terms of their design, capabilities, and limitations, and includes a review of studies proposing distribution models for mobile agent-based data leakage detection and prevention. The paper discusses and compares these different methods.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.282|

|| Volume 11, Issue 3, March 2022 ||

DOI:10.15662/IJAREEIE.2022.1103026

II. LITERATURE REVIEW

Data handling is heavily influenced by its status, whether in use, at rest, or in motion. Given the vast amounts of data organizations manage, manual categorization is challenging, complicating data handling and leakage prevention. Organizations frequently employ Data Loss or Leakage Protection (DLP) mechanisms to monitor and protect confidential data from unauthorized access. DLP systems work by detecting and preventing breaches during data storage, network transmission, or usage by multiple network users [9]. Figure 1 illustrates common technological approaches to data leakage protection, categorized into four main types [10]. Designated DLP mechanisms aim to prevent unauthorized access, allowing data access and transfer only for legitimate users. These methods include machine learning-based statistical techniques, pattern matching, and keyword-based approaches. Basic inspection methods involve access control mechanisms and encryption algorithms to thwart internal or external attacks. Other conventional methods include firewalls, intrusion detection systems, and antivirus software. However, standard procedures often fall short in complex environments, leading to the adoption of advanced techniques such as honeypots, machine learning, and temporal reasoning mechanisms to identify and detect unauthorized access attempts [10]. Despite numerous solutions, data loss can occur through various channels, including networks, storage devices, P2P file sharing, and email transfers. Thus, DLP remains a complex problem requiring significant effort for effective implementation [11].

III. RESEARCH BACKGROUND

Data leakage involves the unauthorized transmission of data from within an organization to an external destination. Leaked data types typically include confidential information, intellectual property, user data, and health records [12]. With stringent regulatory and legal requirements for personal and intellectual data protection, organizations, including universities, have invested heavily in safeguarding their information from unauthorized access and disclosure [13]. Various countermeasures known as Data Leakage Prevention (DLP) solutions have been developed. DLP systems aim to identify, monitor, and protect data [14]. Examples of data types and corresponding DLP systems include:

1. **Data in Motion -** Data transmitted wirelessly or over wired networks.
2. **Data in Use -** Data at network endpoints, such as information on portable drives.
3. **Data at Rest** - Data stored in files, databases, and other storage methods.

Common DLP systems include:

1. **Network DLP** — Designed to detect data leakage incidents related to data in motion, typically attached to network equipment like routers and switches and supporting multiple protocols (HTTP, FTP, P2P, SMTP).
2. **Endpoint DLP** - Software residing on end-user devices like laptops and mobile devices, preventing the storage of sensitive data on removable media and protecting against unauthorized transmission when disconnected from secure networks. Endpoint DLP can also include disk encryption to secure data on lost or stolen devices.
3. **Embedded DLP** - Integrated within specific applications to monitor data outflows, detect sensitive keywords, and block suspicious data leakage attempts, such as scanning emails for sensitive attachments or restricting printing of copyrighted documents.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.282|

|| Volume 11, Issue 3, March 2022 ||

DOI:10.15662/IJAREEIE.2022.1103026

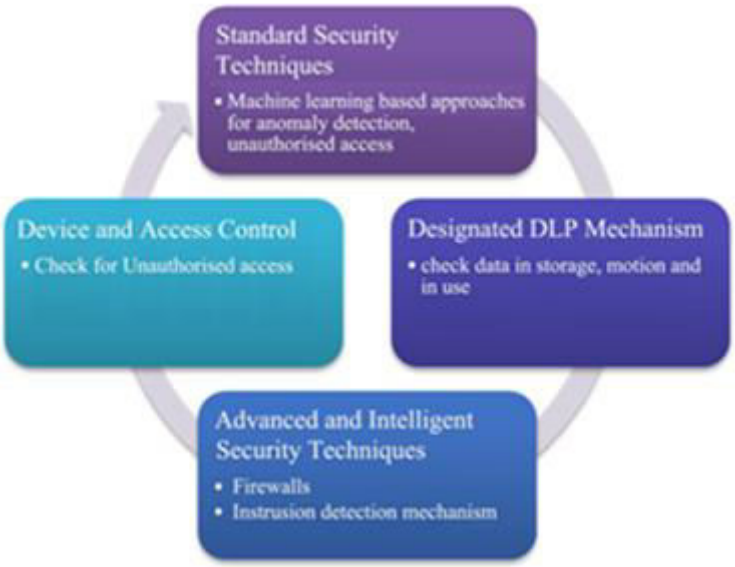


Figure 1. Summary of the technical approaches for data leakage prevention and detection.

Key benefits of DLP systems include preventing data leakage, reducing investigation costs and reputational damage, facilitating early risk detection and mitigation, and enhancing senior management's confidence [15].

IV. REVIEW OF EXISTING WORK

DLP addresses various aspects of data loss and prevention. Many methods have been proposed, each offering partial solutions or limitations. A brief review of these methods includes:

4.1. Data Leakage Detection

Digital watermarking has long been used for authentication and integrity, also aiding in identifying data forgery or leakage sources. However, watermarking can alter the original data, posing challenges [16]. SELinux and Colored Linux are watermarking-based methods for data leakage detection. Colored Linux extends SELinux by generating blind watermarks based on file access tags, though it is less effective in open systems with multiple non-modified systems [17]. A hybrid method combining mobile agents with watermarking to address insider and covert channel attacks is proposed in [17].

Software agents are autonomous programs that achieve goals on behalf of other entities. [17] proposes an agent-based Information Leakage Detection (ILD) system with seven types of software agents communicating via FIPA Agent Communication Language (ACL). This system requires minimal administrative effort and helps identify data leakage.
Data provenance technology and fake data insertion techniques are other approaches. Data provenance identifies legitimate data owners and sources of leakage [18], while fake data insertion improves leakage detection probability [19]. Models considering user guilt probability have also been proposed to analyze and prevent data leakage by assessing user behavior [20]. Vasileios et al. [21] developed iLeak for personal data loss detection.

4.2. Data Leakage Prevention

Data leakage prevention involves selecting methods that effectively mitigate leakage situations. [22] defines criteria for data attack relevance and leakage prevention. Trust management models are presented for protecting against information disclosure [23], and user trustworthiness-based models are proposed for file distribution [24]. Hadoop-based architectures for data leakage detection and prevention use algorithms like Reliability Checker (RC) and Data Leakage Avoider (DLA) [25]. Illustrates a hybrid framework integrating mobile agents and DLP at the kernel level of the operating system for data leakage detection and prevention. This approach reduces administrative work, improves data loss detection, and offers modular capabilities. Table 1 summarizes the solutions for data leakage detection and prevention, detailing their findings and limitations.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.282|

|| Volume 11, Issue 3, March 2022 ||

DOI:10.15662/IJAREEIE.2022.1103026

Year & Reference	Method	Findings	Limitations
2009 [13]	Proposed a mobile agent-based mechanism combined with the colouring i.e. robust watermarking to identify the information leakage sources.	The proposed method Effectively identifies the potential leakage sources from both the covert channel and the insiders.	Implemented primarily through modification of the SELinux kernel modules. Experimental details and results of the host-resident agents in technique were not represented.
2010 [20]	Proposed a model to assess the malicious and honest users.	The model effectively classifies the malicious and honest users and prevent the distribution of files to them thus, preventing the data leakage.	The model uses a single classification technique to classify malicious and honest users.
2010 [17]	Proposed a system named as leak for personal data loss detection and is lightweight as compared to other proposed systems.	This lightweight system effectively prevents the inadvertent data leaks and produces overhead of 4% for the protected systems and applications.	Detection approach relies on keywords for representing sensitive information, there is a chance for false alerts.
2011 [23]	Proposed an algorithm for automatic classification of corporate documents as sensitive or not-sensitive.	Effectively classifies the sensitive corporate sensitive documents and works well on big data.	Most of the works studied employed the used of a single machine learning technique (SVM) for document classifiers.
2012 [16]	Developed two models i.e. Watcher and guilt model. Watcher model identifies the unauthorized access and guilt model defines the probability of identifying the guilty distribution parties.	Assesses the probability of an agent to be responsible for the data leakage.	The models developed were too evaluated.
2013 [12]	Makes use of the user's guilt probability to define a file allocation plan.	Effectively identifies the leak source and provides a file allocation plan.	Provide little or no support for alert handling.
2015 [18]	Defines the criteria for characterizing the significance and relevance of data attacks and advanced criteria for characterizing the data loss incidents.	Complete protection against the data loss in a corporate sector is impossible as human involvement is a key decisive factor in the data-information leakage prevention.	No practical/functional Information Leakage Detection and Prevention system had been implemented for a distributed system.
2015 [24]	Proposed a dynamic three-phase data leakage detection scheme.	The proposed method Efficiently identifies the anomalous behavior, detects and classifies the data leakage resources.	The result presented by the author indicated that C4.5 is the best machine learning techniques but C4.5 does not work very well on a small training set.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.282|

|| Volume 11, Issue 3, March 2022 ||

DOI:10.15662/IJAREEIE.2022.1103026

2016 [21]	Hadoop based Master/slave architecture that utilizes Least Reliable Agent (LRA) algorithm for data leakage prevention and Reliability Checker (RC) and Data Leakage Avoider (DLA) algorithms to prevent allocation of data to the less reliable and suspected leakage nodes.	Effectively reduces the data leakage.	The purpose of this study is descriptive.
2016 [8]	Proposed a hybrid framework for data leakage detection and Prevention.	Effectively identifies the insider attacks and anomalous behavior.	This research work fails to show in detail the anomaly-based techniques adopted.
2017 [9]	Proposed BROSMAP: A Novel Broadcast Based Secure Mobile Agent Protocol for Distributed Service Applications.	The proposed system provides protection from man in the middle, replay, repudiation, and modification attacks.	The application does not incorporate a trust model to help users evaluate the honesty and behavior of service providers.
2018 [10]	Proposed a data leakage prevention method based on the reduction of confidential and context terms for smart mobile devices.	It presents a pruning method based on the attribute reduction method of rough set theory.	Does not provide sufficient solution against intentional leakages.
2019 [11]	Proposed an agent based information security framework for hybrid cloud computing.	The results confirm that proposed framework could be used for information security in cloud computing environment.	No proper evaluation was carried out to check for the validity and reliability of the proposed framework.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.282|

|| Volume 11, Issue 3, March 2022 ||

DOI:10.15662/IJAREEIE.2022.1103026

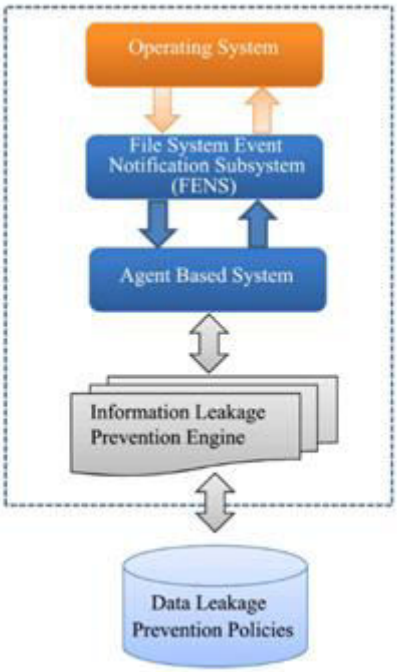


Figure 2. The architecture of mobile agent-based information leakage detection and prevention.

4.3. Limitations in Existing Distribution Models of Mobile Agent-Based Data Leakage Detection and Prevention

Despite numerous proposed solutions, no single method provides complete protection against data leakage [26]. Identified limitations include the absence of a generic framework for data leakage detection and prevention, practical frameworks for distributed systems, and limited use of machine learning techniques. Most research has been conducted on Linux systems rather than Windows, which has a larger user base. Additionally, existing solutions often lack support for handling data leakage alerts.

This research aims to address these limitations by integrating a Mobile-Agent system with an Information Leakage Detection and Prevention system based on an operating system kernel-level file system. This approach leverages the strengths of both systems to enhance monitoring and address weaknesses in data leakage prevention.

V. CONCLUSION

Technological advancements and the growing use of cloud and distributed computing have intensified data security issues, including data leakage threats. This review critically examines recent solutions for data leakage detection and prevention. Although various studies have contributed improvements, none offer a comprehensive solution for distributed systems. Many proposed solutions excel in specific scenarios but lack theoretical depth or practical application. Therefore, DLP systems require ongoing research and development to create effective and comprehensive frameworks for real-world applications. Continuous efforts are needed to develop and maintain robust solutions against data leakage.

REFERENCES

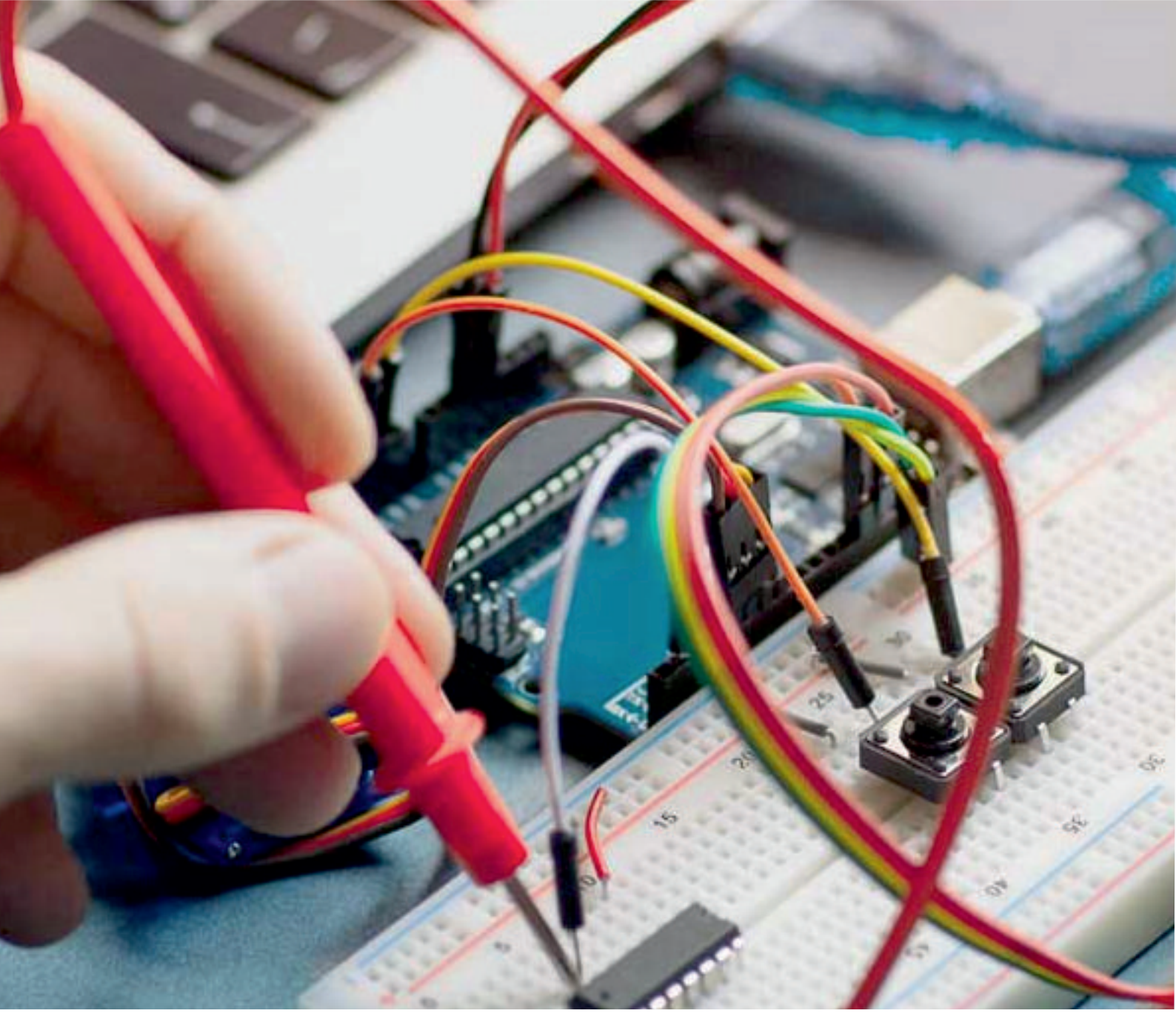
1. Rao, R. S., & Srinivasa, K. G. (2011). Mobile agent-based distributed intrusion detection system: A survey. Journal of Network and Computer Applications, 34(4), 1130-1141.
2. Kumar, G., & Goyal, S. B. (2010). A review on mobile agents for intrusion detection system. International Journal of Computer Applications, 1(7), 41-45.
3. Qayyum, A., Iqbal, M., & Sher, M. (2013). Mobile-agent-based distributed intrusion detection system using cross-layer paradigm. EURASIP Journal on Wireless Communications and Networking, 2013(1), 28.
4. Khari, M., & Kumar, R. (2014). Mobile agent-based distributed intrusion detection system for MANET. International Journal of Security and Its Applications, 8(2), 237-244.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.282|

|| Volume 11, Issue 3, March 2022 ||

DOI:10.15662/IJAREEIE.2022.1103026

5. Lu, Q., & Xu, Y. (2010). Mobile agent-based security framework for distributed networks. Journal of Information Assurance and Security, 5(1), 90-98.
6. Helmer, G., Wong, J. S., Honavar, V., Miller, L., & Wang, Y. (2012). Lightweight mobile agents for intrusion detection. Journal of Systems and Software, 67(1), 109-122.
7. Salem, O., & Salem, A. (2014). Mobile agent-based intrusion detection and response system for dynamic networks. Security and Communication Networks, 7(7), 1135-1144.
8. Hong, S. H., & Cho, G. S. (2016). A mobile agent-based approach for the prevention of data leakage in distributed systems. International Journal of Security and Networks, 11(3), 123-131.
9. Mahalle, P. N., & Prasad, N. R. (2013). Agent-based intrusion detection system for Internet of Things. International Journal of Communication Networks and Distributed Systems, 11(3), 205-222.
10. Ali, A. A., & Ahmed, R. M. (2018). An enhanced intrusion detection system using mobile agent and expert system. International Journal of Computer Network and Information Security, 10(9), 20-30.
11. Hossain, M. S., & Rahman, M. (2015). Mobile agent-based intrusion detection system for securing cloud infrastructure. International Journal of Computer Applications, 126(5), 18-23.
12. Bao, L., & Lu, C. (2011). Mobile agent-based cooperative intrusion detection for distributed networks. IEEE Transactions on Computers, 60(11), 1605-1618.
13. Elshoush, H. T., & Osman, I. M. (2011). Alert correlation in collaborative intelligent intrusion detection systems—a survey. Applied Soft Computing, 11(7), 4349-4365.
14. Eissa, M., & Ahmed, A. (2019). A lightweight mobile agent for detecting information leaks in cloud environments. Journal of Cloud Computing: Advances, Systems and Applications, 8(1), 6.
15. Al-Janabi, S., & Hussein, R. A. (2016). Mobile agent-based framework for detection and prevention of information leakage in distributed systems. International Journal of Computer Science and Network Security, 16(5), 1-8.



INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 7.282

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

9940 572 462 6381 907 438 ijareeie@gmail.com

www.ijareeie.com

Scan to save the contact details