International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7033
***Article Received**: 01 April 2023 **Revised:** 25 May 2023 **Accepted:** 06 June 2023*

A Secured Multi Agent Architecture for Grid Computing

R Sivasubramanian[1], N Malarvizhi[2]
[1]Research Scholar,
Vel Tech Rangarajan Dr Sagunthala R&D Institite of Science and Technology
Chennai, India
sivar2000@gmail.com
[2]Professor, Department of Computer Science and Engineering
Vel Tech Rangarajan Dr Sagunthala R&D Institite of Science and Technology
Chennai, India
drnmalarvizhi@veltech.edu.in

Abstract—Grid computing provides big possibilities like resource sharing, resource virtualization, and capacity planning since diverse resources that are geographically dispersed are virtualized as a single entity. The associated security concerns are one of the key obstacles preventing grid computing from being broadly adopted and used. Users in a grid are concerned about the security of their assets and the privacy of their data. A host's security in terms of its data or virtual servers may be jeopardised when it interacts with a grid. By providing multilateral security, i.e., security for both the Grid client and the Grid supplier, our building design expands the degree of assurance that can be placed on the accuracy of a Grid calculation and the assurance of client-provided resources. We discuss the issue of ensuring security and present the multi-agent security construction analysis. The paper outlines a multi-agent strategy for protecting the grid environment's resources. The strategy is put forth to address the grid computing industry's growing, serious security issue. The paper defines a multi-agent security architecture that integrates the capabilities of agents with the Grid Security Infrastructure's basic security mechanism (GSI). A security Master agent and a few security task execution agents make up the strategy.

Keywords-Multi-agent, Security, Architecture, Grid computing.

I. INTRODUCTION

Grid offers infrastructure for creating, maintaining, and managing inter systems that offer safe coordinated access to computing data and services, as well as dynamic, autonomous, and domain-independent access on demand. The basic goal of the grid is to provide a means for users to use the geographically dispersed tools available to them to solve problems. A grid system is necessary to combine heterogeneous resources with varied quality and quantity. However, a high proportion of connected, dynamic, and altered processing resources make up the grid environment. As a result, there could risks particular computation, memory, and communication methods. The security of matrix figuring has become the bottleneck in commercial and scientific computation. We must use a variety of health strategies, like distinguishing evidence, confirmation, approved control, protected correspondence, reviews, and records, to make the lattice registering environment safe. This paper is organized as follows. Section II includes the prior research on grid security requirements, and its inadequacies. Section IV describes multi agents architecture, their benefits, and how they may be integrated with grid to address grid security challenges. Section III states the architecture requirements for grid security. V addresses themulti-agent architecture for grid security that has been proposed. Conclusion and further work is noted in Section VI.

II. THE GRID ENVIRONMENT SECURITY ISSUES & PREVIOUS WORK

In the literature, "systems and applications that integrate and manage resources and services spread across many control domains" [1] are deemed to be the idea of grid computing. Foster and Kesselman [2] define a grid as a system that complies with three distinct criteria: it organises resources that are not controlled centrally, it employs general-purpose, open-standard protocols and interfaces, and it provides nontrivial quality of service. [3] "Coordinated resource sharing and issue solving in dynamic, multi-institution virtual organisations" is how you should define grid computing. Utilizing cooperative synergies, such as resource owners sharing unused disc space and processor time with users to solve difficult problems that their own personal resources could not address, the grid is capable of functioning more efficiently and cheaply [4]. Computational grids, data grids, and service grids are the three primary categories of computer grids currently in use. Each

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7033
***Article Received**: 01 April 2023 **Revised:** 25 May 2023 **Accepted:** 06 June 2023*

has its own set of weaknesses, particularly in the security sector.

TABLE I TYPES OF GRID COMPUTING

Grid Type	Security Issues
Computational Grid	Program with infinite loop can be used to down the nodes of the grid, decrease the functionality
Data Grid	Users can overwrite data of the users if they exceed their available space limit which corrupt the other data
Service Grid	Users can use the service grid to launch denial of the service attack against another site

Grid computing security can be divided into three main domains, including hazards with design, networking, and administration [5]. Any secure grid environment must use techniques to protect resource protection, secure communication, data encryption, authentication, and authorisation [6]. A user submits a job to the grid, and the job is received by the gatekeeper or entry point of the grid system. At that time, there should be systems in place to authenticate the user. There is a need to provide confidentiality and integrity when the work is submitted to the grid so that no one may view the contents of the information conveyed or modify the contents. Finally, there should be systems in place for delegation and single sign-on. The problem of managing the security of users and resources arises in the context of the grid environment's diversified and geographically dispersed resources and vast variety of users, each with specific demands and aspirations for the grid system. Three major kinds of grid security problems may be identified: management-related problems, infrastructure-related problems, and architecture-related problems[7]. In this article, we will focus on architecture-related problems.Abbreviations and Acronyms.

A. Grid security architecture Previous work

The Globus Security Model is the most extensively used grid security design [8]. One of the most popular grid computing software toolkits available today is the Globus Toolkit (GT) [9]. The essential security functions of authentication, access control, integrity, privacy and non-repudiation, single sign-on, and interoperability are all covered by the Globus method to modelling grid security. It is employed to generate Grid applications and systems. Grid Security Infrastructure (GSI) was created in order to address security concerns and unify grid security efforts [10]. The Open Grid Services Architecture (OGSA), which is built on Web services concepts and technology, is the most significant grid computing architecture. With the help of MyProxy [11], a credential repository created to address the issue of saving credentials on local hosts by transporting credentials between locations, a user is now able to log in to the grid from any place and solve the credential storage problem.

The HIPernet [12] and Anti-Doping [13] designs are two more security systems. While Anti-Doping is a method for ensuring the integrity of data sent across grid computing infrastructures by preventing data alteration or corruption during transmission, HIPernet is a technology that offers a solution for secure distributed computing.

The following elements are all included in the Grid security model [14 and 15]: Components specific to an application

- Secure Communication
- Translation of Credentials and identities
- Enforcement of Access Controls
- Audit and non-repudiation

Components Rules and Policies

- Identity/Credential Mapping
- Authorization
- Privacy
- Service/end-point

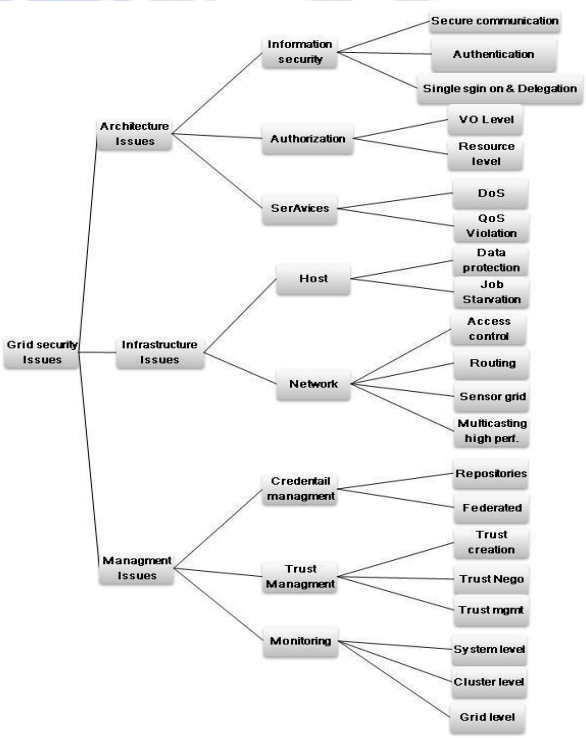

Figure 1.The grid security issues

B. Issues with earlier Grid Security architectures

1) *Onerous security management:* The administrator of the Grid system must be well-versed in the entire Grid system. In

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7033
***Article Received**: 01 April 2023 **Revised:** 25 May 2023 **Accepted:** 06 June 2023*

scientific collaborations, anything is possible. These grid deployments have a somewhat small and constrained range and scope. The extent and scope of grid deployments in industrial and commercial contexts are unpredictable. Security requirements are subject to dynamic change at any time. It is challenging for the Grid system administrator to be aware in global security.

2) Demand for and scarcity of dynamic features: Once grid system managers have deployed the security configuration, it hardly ever has to be modified during runtime. The environment is uncertain and subject to change at any time due to the grid installations' continually changing scope. As a result, the grid system's ability to be changed is lowered by the absence of dynamic features.

3) Inadequate cooperation and interactions: Each cooperation and interaction participant needs to learn about the other's security requirements and policies and strive to come to an agreement on a corporate security strategy. While neither party can obtain a corporate security plan, such as mutually distinct properties for credentials, it often takes undue human involvement to resolve. Additionally, it causes the grid system's extensibility to decrease. The operators' framework is presented in response to these shortcomings of the GSI as shown above.

III ARCHITECTURE REQUIREMENTS FOR GRID SECURITY

The Grid security design is based on the security requirements. The following elements are included in the high level grid security requirements: [14 and 16].

1) Authentication: Providing interfaces for various authentication mechanisms to be plugged in as well ways to distinguish the mechanism being used.

2) Authorization: Ability to manage access to grid components based on authorization rules.

3. Delegation: Providing methods that enable the delegation of access rights from requesters to services, while guaranteeing that the access rights transferred are limited to the tasks intended to be carried out within the bounds of policy.

4) Message integrity: Ensuring that all illegal updates to the message's contents or content may be recognised by the recipient. When future access to grid resources is sought, single login refers to relieving an authorised entity from the need for re-authentication for a predetermined amount of time while taking into account numerous security domains and identity mappings.

5) Protection of the confidentiality: The message's content and underlying transport, also communications between OGSA-compliant components using either store-and-forward or point-to-point techniques.

6) Privacy: Enabling a establishment and enforcement of privacy policies by both the service requester and the service provider.

7) Policy exchange: enabling security context negotiations based on security policy information between service requesters and service providers Lifetime and renewal of credentials: Possibility of updating requester credentials if a grid application operation takes longer to finish than a delegated credential's lifecycle.

8) Secure logging: Creating a basis for auditing and no repudiation so that all services can time stamp and log different sorts of information without interruption or interference of threat agents.

9) Assurance: Providing means to qualify the security assurance level that can be expected of a hosting environment. The level of security assurance reveals the different security services setting offers. On considering whether to install a service in the environment, this information is helpful.

10) Manageability: This aim to reveal numerous identity management, policy management, and other security service management challenges. To enable a cross-domain grid computing environment, a firewall must be traversed without sacrificing local firewall policy control.

11) Securing the OGSA infrastructure: This applies to securing essential OGSA components. Three categories can be used to categorise the security issues that arise in a grid setting [14].

1) Integration with already-in-use technology and systems

2) Compatibility with various "hosting environments."

IV MULTI AGENTS

"An agent is an entity that operates autonomously on behalf of others, conducts its actions with a certain degree of proactivity and reactivity, and demonstrates a certain degree of the crucial characteristics of learning, cooperation, and mobility. [17]. A specialist is a self-sufficient proactive substance whose actions depend on its internal state. The operators' autonomy alludes to the fact that their presence is less dependent on the presence of any other thing, such as a particular asset or alternative specialists. The proactive norm for specialists gives it the potential to act without being prompted or urged to. They have such peculiarities as follows [18].

- Cooperative
- Learn

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7033
***Article Received**: 01 April 2023 **Revised:** 25 May 2023 **Accepted:** 06 June 2023*

- Autonomy
- Proactive
- Situated

N. R. Jennings [19] claims that an Agent's primary capability is autonomy. A more basic definition of an Agent is an encapsulated system that is positioned in a specific environment and has the ability to perform flexible, autonomous action within that environment to accomplish predetermined goals. An agent can also communicate and work together with other agents to complete challenging tasks. It can sometimes modify its procedures in response to specific circumstances, like changes in the environment. In general, an agent can belong to any of the following types:

- Reactive agent
- Intelligent (Cognitive) agent
- Mobile agent
- Stationary agent
- Interface agent
- Collaborative agent
- Information agent
- Hybrid agent

Collecting data from various sources, searching and filtering information, monitoring, information dissemination with a specific audience, agent-to-agent negotiation, performing parallel computations, bartering, enhancing telecommunication network services, controlling smart matter, and enhancing entertainment are all examples of agent abilities.

A. Multi agent systems

For complex, frequently spread activities, groups of agents are frequently used. The grouped agents create a multi-agent system in which they collaborate to accomplish a single objective. A multi-agent system replicates human or animal civilizations in a number of ways, particularly when it comes to interaction, teamwork, and rarely bargaining to resolve challenging issues. The following benefits may be associated with a multi-agent system [23].

1) Unmistakably identifiable substances with the decently characterized limits and interfaces and critical thinking capacities.

2) Installed in a particular environment; they receive inputs related to the state of their surroundings through sensors and keep up with nature through effectors.

3) Created to perform a specific function; they have special objectives to achieve and particular critical thinking abilities (benefits) to offer in support of such efforts.

4) Autonomous - they are in charge of both their own behaviour and internal state;and

(5) Able to exemplify flexible problem-solving behaviour in the pursuit of their design objectives; they must be proactive as well as reactive.

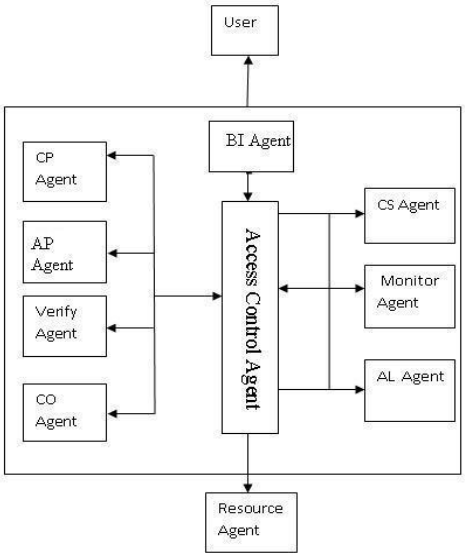

Figure 2. Secured Multi Agent Architecture

Multi-Agent Systems (MAS) - frameworks that may incorporate numerous clever operators - are turning into a procedure that empowers outline and execution of extensive frameworks in a truly secluded manner. Once receiving a specialists-oriented perspective of the world, it quickly becomes apparent that the major issues call for or incorporate multi-operators frameworks to address the issue's diffused nature, heterogeneity of loci of control, diversity of viewpoints, or competing investments. Furthermore, these operators interact to deal with the conditions that result from being set up in a typical environment or to achieve their respective aims. Additionally, a group of researchers think that the agent paradigm is the effective approach to effectively solving distributed challenges. Communication is essential in any multi-agent system since each agent is given one or more small issues to solve, further work together to solve as a team.

V. SECURED MULTI-AGENT ARCHITECTURE FOR GRID

Earlier sections it is mentioned those architectural requirements for grid security and the benefits of the usage of agents A world interface, a control unit, and a knowledge base are what InteRRaP characterises as making up an agent (KB).

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7033
***Article Received**: 01 April 2023 **Revised:** 25 May 2023 **Accepted:** 06 June 2023*

The behavior-based layer (BBL), the local planning layer (LPL), and the cooperative planning layer are the three layers that make up the control unit (CPL). These elements work together to accomplish a single goal. Our architecture's individual agents are all built with Interrap [24] operators construction modelling at their core. For grid users and resources, the proposed design offers security barriers. It can reduce the artificial security load and improve the efficiency with security tasks are executed using preferred access security. It consists of the master agent, Access Control Agent (ACA), as well as a number of agents which also carries works related to security, including Boundary interface agents (BIA), Conversation protect agents (CPA), Verification agents (VA), Approval Agents (APA), Allocation Agents (ALA), Cooperation Agents (COA), Confidential secure agents (CSA), and Monitor agents (MA). The client's intelligent interface with structural planning is the BIA. The data and security requirements of the client are obtained and parsed. The ACA is primarily in charge of modifying assignment security appeals and assigning security undertakings to errands. The others can do independent correlative security tasks.

A .Boundary Interface Agents (BIA)

GUIs are used by BIA to manage user engagement. It serves as the only user interface through which users can access the security system, and its primary duties include the following:

1) Accepts user information (through keyboard or user agents), including user identification data (username/password or certificates) in preparation for authentication.

The following are the security requirements for user jobs.

When users submit a task and try to access resources in the grid, the task requires special security requirements, such as encrypt protection. BIA describes a uniform security requirement format through check boxes based on Security Policy Base, making it easier for both users and architecture to express and parse security requirements.

Update the Security Policy Base periodically by following the changes to the grid security policy, which improves the security architecture's adaptability and extensibility.

Get the custom of special users, which is available from MA, and learn it. By adjusting the default value for the check boxes, you may give users a customized check interface while enhancing the architecture's intelligence.

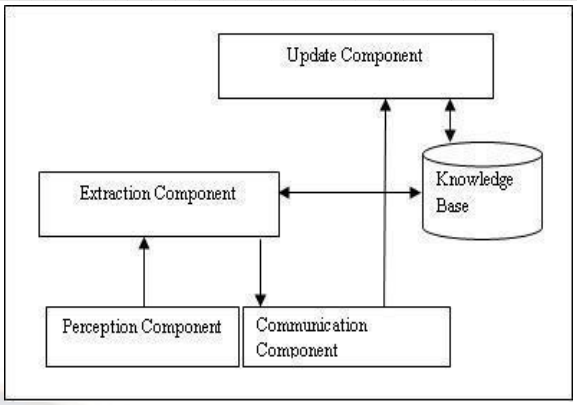

Figure 3.Architecture of Boundary Interface Agent

Figure 3 illustrates the BIA's architectural components. The primary duty of the Communication component is to communicate with ACA. Users provide information to the perception component. The Extraction component may parse the security policy based on the Knowledge Base and retrieve users' identities. The Update component updates the Security Policy Base after getting the update information. Parse policy and security policy are kept in the knowledge base.

B. Access Control Agent ACA

The primary responsibility of this specialist, who serves as the structure's timetable focal point, is to dispatch and schedule the security errands and to actualize them alongside the other security practical agents. These are its primary duties:

1) Receive user data and security specifications from BIAs, then implement job scheduling strategy;

2) Send cooperation requests to VA and APA, as well as other security functional task execution agents, and request their feedback.

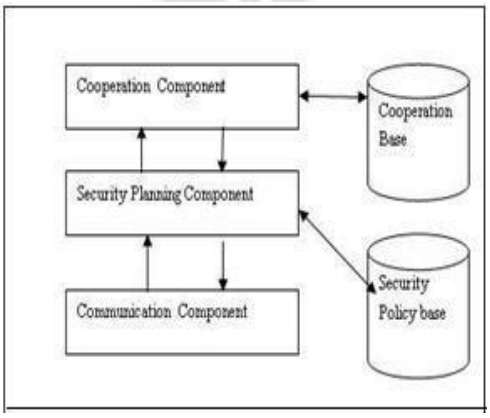

Figure 4.Architecture of Access Control Agent

The following elements constitute the ACA architecture, as depicted in Fig. 4. The agent can share information with security functional agents, including cooperation requests and feedback information, thanks to the communication component. Receiving requests for security resolution, the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7033
***Article Received**: 01 April 2023 **Revised:** 25 May 2023 **Accepted:** 06 June 2023*

Security Planning component evaluates whether to respond in accordance with the Security Policy Base, which has the applicable security policies pertaining to the grid system. The Cooperative component can then be asked to communicate with Cooperative functional agents. Through lookups of corresponding agents' information, which is stored in the Collaboration Base, the latter achieves interactions and cooperation.

C. Verification Agents VA

These representatives are the first toll-gate and are in charge of confirming a user's identity. They evaluate the input data obtained from ACA and determine whether to approve or disapprove the current user before sending the results to ACA.

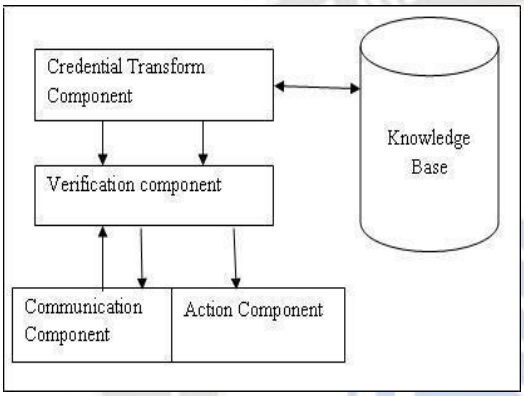

Figure 5.Architecture of Verification Agent

VA's architecture is depicted in Fig. 5. The Authentication Analysis component analyses the format of the user identity (username/password, inner-domain credential, and outer-domain credential); the Action component is responsible for invoking foundational security services offered by the Grid Security Infrastructure under the direction of the Authentication Analysis component; if the format of the credential doesn't comply with the requirements, the Grid Security Infrastructure will not be invoked.

D .Conversation Protect Agent CPA

Users and other security functional agents have their conversations protected by the Conversation Protect Agents.

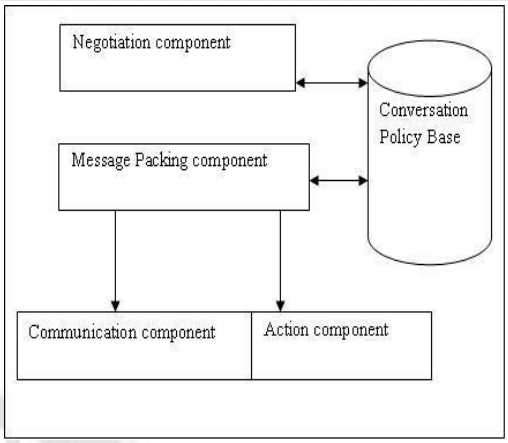

Figure 6.Architecture of Conversation Protect Agent

The following elements make up its architecture, as depicted in Fig. 6. Information interchange with the ACA is the responsibility of the communication component. With an emphasis on the Protection Policy Base, the Conversation Packing component sends pressing or encodes requests. If the shared requirements of message-ties are unpredictable, the Negotiation portion will be called upon to make an exchange off. For instance, if one requires message-level security but the other requires the use of transport-level security to improve performance. As instructed by the course of packing segment, the Action component will carry out the secure operation. Conversation protection norms are kept as in Conversation Protection Policy Base.

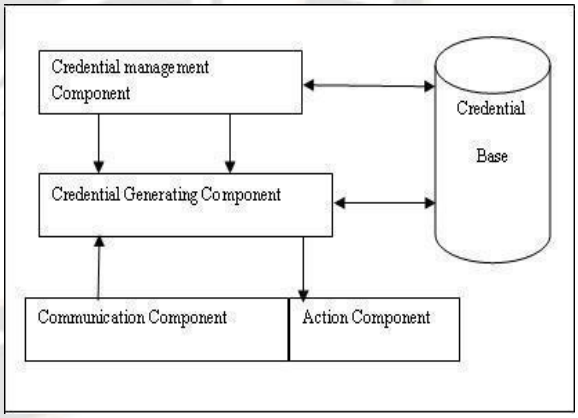

Figure 7. Architecture of Allocation Agent

E. Allocation Agent ALA

Fig. 7 shows the architecture of the allocation agent. Allocation Agents are in charge of creating proxy credentials for users and implementing single-sign-on. Four Components make up the ALA's architecture. The agent can communicate information with the ACA thanks to the communication component. In order to reduce the negative effects of being captured by an enemy, the Credential Generating component is designed to provide an appropriate short-term proxy credential and reduce its rights. The specified components have the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7033
***Article Received**: 01 April 2023 **Revised:** 25 May 2023 **Accepted:** 06 June 2023*

role to manage the accrediting process as a whole. This need is met by the Allocation Agent, who periodically checks the credentials of every client who has a job queued. (GSI provides exam-supporting question materials). When a customer's certifications are expired or are about to expire, the experts post the job in a hold status in its line and notify the client through email that their employment cannot resume until their certifications are renewed.

Delegation Agent may be improved to interact with a system like Myproxy, which combines an online credential repository with an online certificate authority to enable users to securely receive credentials when and when needed. This would minimise client hassle with managing expired accreditations. For the security tasks to be carried out, the Action component calls the appropriate GT services. Additionally, the proxy credential generating policy is kept in the credential base.

F. Confidential Secure Agent CSA

These agents primarily offer users privacy protection, including identity encryption protection, in accordance with their needs.

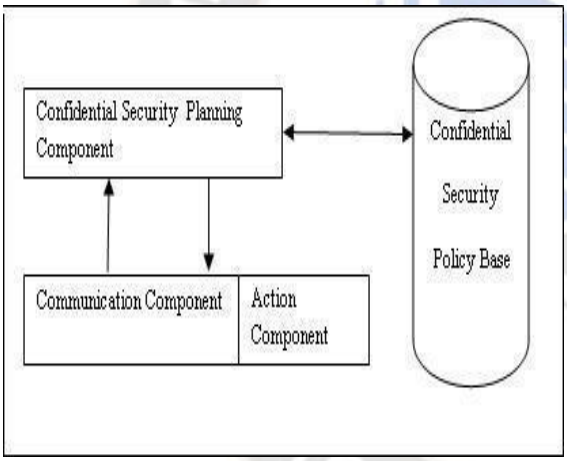

Figure 8. Architecture of Confidential Secure Agent

As seen in Fig. 8, the CSA's architecture consists of four components. The Communication Component will transfer the encrypted credential to ACA after receiving the cooperate request and credential from ACA. Based on the confidential security Policy Base, the confidential security Planning component produces a protection strategy. Implementing privacy-protecting duties is the responsibility of the Action component, while the confidential security Policy Base stores the confidential security policy and algorithm.

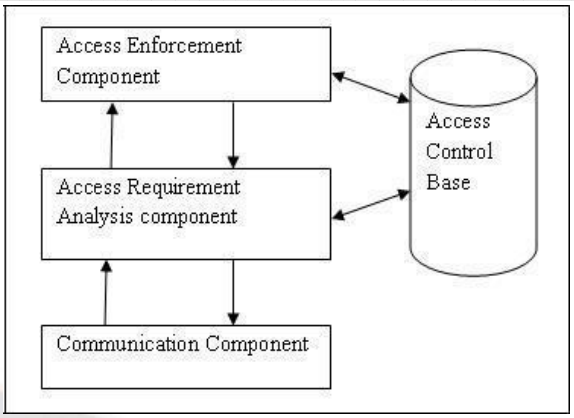

Figure 9. The Architecture of Approval Agent.

G. Approval Agent APA

The Approval Agents will implement authority tasks if a user has already successfully completed authentication. When dealing with an inner-domain user, the APA will use the ACL to carry out authority tasks; but, when dealing with an outer-domain credential, the APA will transfer the credential to the Negotiation for Cooperation agent in Figure 10 of the APA's Architecture. According to Figure 9, the Approval Agent's architecture essentially consists of four parts.

Communication with ACA, including obtaining credential and domain information, is the responsibility of the Communication component. The task's access requirements are examined by the access requirement component, then requests CAS or VOMS to obtain the necessary rights or characteristics. The set of approved operations may be sent to the Access Enforcement Component as part of a service request (push scenario) or may be retrieved by querying an Access Decision service, such as Akenti and PERMIS. Additionally, the access control policy is kept in the Access Control Base.

H. Cooperation Agent COA

Cooperation agents are used to resolve any problems that arise as a result of the differing security arrangements for the assets and assignments. They will decide which security options both artists will agree. They will identify potential security arrangements that both performers can accept.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7033
***Article Received**: 01 April 2023 **Revised:** 25 May 2023 **Accepted:** 06 June 2023*

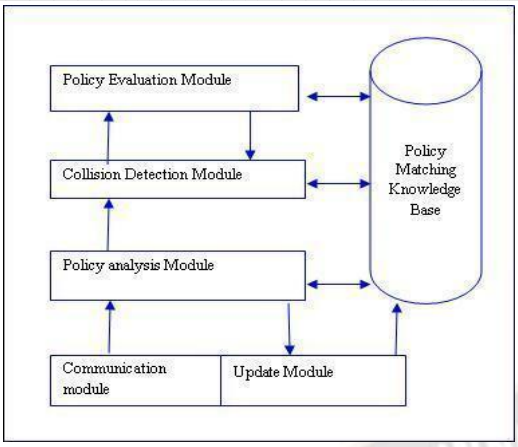

Figure 10.Architecture of Cooperation Agents

Figure 10 depicts the COA architecture. Receiving cooperation requests from ACA and security policies from resource agents is the responsibility of the communication component. Furthermore, it sends the final policy if the negotiation is completed successfully or the explanation for the failure of the negotiation. The Policy Analysis component creates a consistent policy format by combining the policies for the tasks and the resources (we can consult WS-Policy Standard). The Collision Detection component will then adhere to their security standards. We can ensure that the resources will be secure because this match will be based on the security policy for the resources. After that, it will either create the first policy file or send the collision notice to ACA. Based on the Policy Matching Knowledge Base, the Policy Evaluation component will assess the initial policy file to create the final policy file. The Policy Matching Knowledge Base is updated by the Update component. Security policy and policy matching policy are both included in the Policy Matching Knowledge Base.

I. Monitor Agents MA

The following tasks are under the purview of the Monitor Agents:

1) They will monitor the security occurrences of other security experts who are helpful in the construction modelling and log record, which can prevent risky events from occurring repeatedly. Additionally, they provide other security administration, such IDS. All we have to do is screen ACA.

2) They will analyse the behaviour of unusual clients and provide clients with encouragement, which can increase the security system's intelligence.

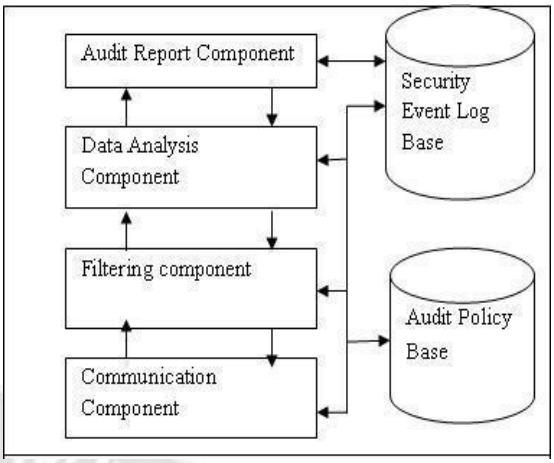

Figure 11.Architecture of Monitoring Agent

These elements make up MA's architecture, as seen in Figure 11: The Communication component tracks and logs ACA security incidents. Once the audit events have filtered, the Filtering component will extract useful data. The Filtered Audit Log will be compiled by the Data Analysis component using the Audit Policy Base to create security event mark up files, which will then be sent to the Security Event Log Database. The audit report is then produced by the Audit Report component, who outputs it in text format. Information filtering and security event analysis policies are kept in the Audit Policy Base. Scanned security event logs will be kept in the security event log database. also requires a thorough understanding network security. The essay was suggested in response to this question is formed with intelligent security frame that uses proxies. Analysis revealed that the frame made good use of its transparency and autonomy to significantly lessen the workload of both users and managers in the security sphere.

VI. CONCLUSIONS

This study presented a cooperative master-task multi-agent architecture with master agents like ACA and task agents like BIA, MA. Additionally, it resolves demanding security management, a lack of dynamic features, insufficient cooperation, and ineffective interactions. Authentication, Authorization, Delegation, Message Integrity, Confidentiality, Privacy, Policy exchange, and Secure logging are all covered by the architecture at the same time.

The vast majority of individual specialists are centred on the operator's construction and modelling based on InteRRaP, which includes responsiveness, intelligent (cognitive) interface, collaborative, and information specialists. In order to handle the growing manual security load of grid computing and its expanding use in commercial and industrial applications, multi-agent systems were created.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7033
***Article Received**: 01 April 2023 **Revised:** 25 May 2023 **Accepted:** 06 June 2023*

REFERENCES

[1] M. Humphrey, M.R. Thompson, K.R. Jackson, Security for grids, Proc. of IEEE 93 (3) (March 2005) 644–652.
[2] I. Foster, K. Kesselman, The Grid: Blueprint for a Future Computing Infrastructure (Morgan Kaufmann in Computer Architecture and Design), 1999.
[3] A.S. Grimshaw, A.S. Humphrey, A. Natrajan, A philosophical and technical comparison of Legion and Globus, IBM J. Res.Develop. 48 (2) (March 2004).
[4] R. Buyya, Grid computing information centre: frequently asked questions (FAQ),http://www.gridcomputing.com/gridfaq.html (Document view: March 28, 2006).
[5] Dr. Avinash Pawar. (2020). Development and Verification of Material Plasma Exposure Concepts. International Journal of New Practices in Management and Engineering, 9(03), 11 - 14. https://doi.org/10.17762/ijnpme.v9i03.90
[6] AnirbanChakrabarti, AnishDamodaran, ShubhashisSengupta, "Grid Computing Security: A Taxonomy," IEEE Security and Privacy, vol. 6, no. 1, pp. 44-51, Jan/Feb., 2008
[7] K. Kaneda, K. Taura, A. Yonezawa, Virtual Private Grid: A Command Shell for Utilizing Hundreds of Machines.
[8] ”GridComputingSecurity:” AnirbanChakrabarti,Springer Berlin Heidelberg New York.
[9] N. Kanaskar, U. Topaloglu, C. Bayrak, "Globus Security Model for Grid Environment", ACM SIGSOFT Software Engineering Notes, November 2005
[10] H. Bjerke, "Grid Survey", 2004. http://openlab-muinternal.
[11] Globus project, http://www.globus.
[12] Jason Novotny, Steven Tuecke, Von Welch, "An Online Credential Repository for the Grid: MyProxy," 10th IEEE International Symposium on High Performance Distributed Computing (HPDC-10 '01), 2001.
[13] J. Laganier, P. Primet, "HIPernet: A decentralized Security Infrastructure for Large Scale Grid Environments", Proceedings of the 6th IEEE/ACM International Workshop on Grid Computing, 2005.
[14] R. dos Santos, M. Aguilar, P. de Soussa, J. Soussa, R. Andrade, "Anti Doping: An Approach for Grid Integrity Verification", Proceedings of the advanced industrial conference on Telecommunications, pp. 2-7, 2005.
[15] NatarajNagaratnam, Philippe Janson, JohnDayka. Anthony Nadalin, Frank Siebenlist, Von Welch, Ian Foster, Steve Tuecke, “TheSecurity Architecture for Open Grid Services,” 2002[33]
[16] The Globus Security Team, “Globus ToolkitVersion 4 Grid Security Infrastructure: A Standards Perspective,” 2005
[17] Bart Jacob, Michael Brown, Kentaro Fukui, NiharTrivedi, “Introduction to Grid Computing,” December 2005
[18] M. Wooldridge, and N. R. Jennings. “Intelligent Agents: Theory and Practice”. In Knowledge Engineering Review, Vol. 10, No 2, 1995, pp. 115-152.
[19] H. Li, Q. Wu,"Summary on Research of Multi-agent System" JOURNAL OF TONGJI UNIVERSITY. 2003,
[20] Jennings, NR. "On Agent-based Software Engineering," Artificial Intelligence, Elsevier, 2000(177): 277-296
[21] Caroline C. Hayes. (2001) ’Agents in a Nutshell A very Brief Introduction’, IEEE Trans. KDE, Vol. 11 No1, January/February 1999
[22] Moneva, J.M. Victor R. Lesser. (1999) ‘Cooperative Multi-agent systems: A personal View of the state of the art,’ IEEE Trans. KDE, Vol. 11 No1, January/February 1999.
[23] Paul Garcia, Ian Martin, Laura López, Sigurðsson Ólafur, Matti Virtanen. Deep Learning Models for Intelligent Tutoring Systems. Kuwait Journal of Machine Learning, 2(1). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/167
[24] G. Weis. (1999) ‘Multiagent Systems, a modern approach to distributed Artificial Intelligence’, MIT press, 1999.
[25] Moneva, J.M. Victor R. Lesser. (1999) ‘Cooperative Multi-agent systems: A personal View of the state of the art,’ IEEE Trans. KDE, Vol. 11 No1, January/February 1999 :
[26] M. Wooldridge, "An Introduction to Multi-Agent Systems." Beijing:Publishing house of Electronics Industry. 2003.