ISSN No:-2456-2165

Study on Different Grid Security Issues and Challenges for Grid's Massive Real-Life Applications

Avijit Bhowmick[1], Arup Kumar Nandi[2], Goutam Sutradhar[3]
[1]Budge Budge Institute of Technology, West Bengal, India
[2]Senior Principal Scientist, CSIR-CMERI, Durgapur, West Bengal, India
[3]Director, National Institute of Technology, Manipur, India.

Abstract:- The focus of computational Grid is on collaborative resource management in real-time, distributed, virtual environments. The ever-changing nature of Grid settings raises complex security issues that call for innovative technology solutions. This paper's major purpose is to outline the prerequisites for computational grid security. The crucial problems have been identified with Grid security and explains approaches to fixing these fundamental problems. we look at some of the most persistent security concerns around the Grid and describe towards solutions currently in development to solve them. We addressed all the issues related to Grid and the work done by Globus Toolkits to ensure security. There are several types of grid systems in use today, and each type has different security demands and solutions to meet those requirements. In addition to providing an effort to identify and characterise grid security challenges for various grid configurations and security situations that are encountered by computational grid. This article presents an overview of various sorts of security vulnerabilities in computational grid & the potential directions for future research are also covered.

Keywords:- *Computational Grid, Authentication, Authorization, Security, Online Grid Security Architecture, Virtual Organization (VO).*

I. INTRODUCTION

The security of the smart computational grid is a relatively new issue, and there are constant advancements being made in this area. Most online data security is provided by the industry standard encryption method AES-128. The goal of grid computing is to increase system performance at a reduced cost via resource sharing. In accordance with the literature, a computational grid is a system where several services collaborate and share resources. Grids, as defined by Foster and Kesselman, allow for the decentralised coordination of resources, make use of a universal interface for all purposes, and guarantee nontrivial service quality.

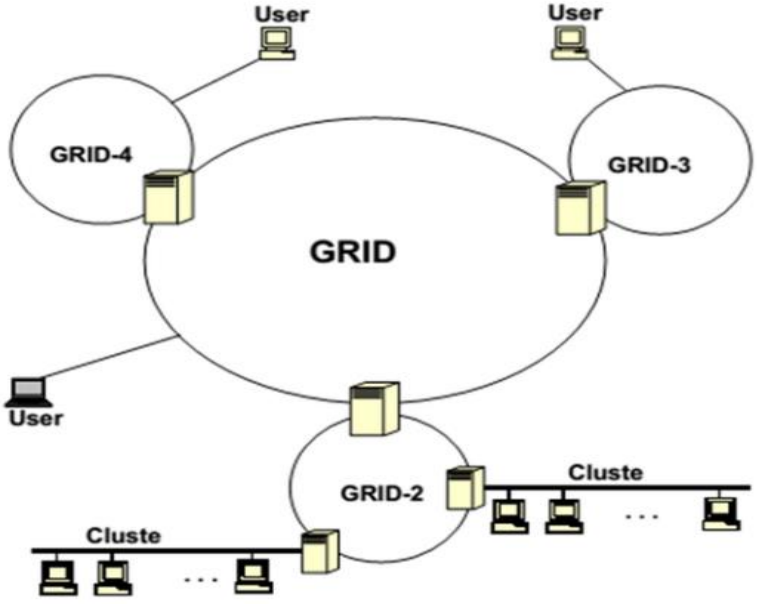

Fig.1 Grid Network Overview

Sharing resources via computational grid improves performance and reduces costs compared to having each company maintain its own "closed-box" resources, which is why this model is becoming more well-known in the field of real-life applications [1]. In their definition of a grid, Foster and Kesselman highlight three characteristics: decentralised resource coordination; employing standardized, open, all-purpose protocols and interfaces while providing service quality. Coordination of resource sharing and issue sharing in several virtual institutions is characterised by computational grid. [2]. To efficiently calculate besides processing data, grid networks aim to combine the resources of several computer

ISSN No:-2456-2165

clusters into a single, unified system. "Systems and programmes that manage resources as well as facilities distributed across a variety of control areas" is how the field of literature defines grid computing [3]. The emergence of dynamic "virtual organisations" (VOs) consisting of sets of people and their related means and facilities that have a similar goal however are not physically situated in the same physical location is a regular occurrence in Grid Computing. Security concerns arise due to the need of VOs' requirement to facilitate the integration and control of resources. Some of these issues are being addressed by the work being done in the field of grid computing, which relies not on undeviating inter-organizational belief but then on the VO as a connection between the organisations taking part in a certain community. [4].

II. SECURITY REQUIREMENTS

Authentication, reliability, no repudiation, privacy are examples of security features which are essential in grid systems and applications. Problems with identification and permissions. There is no need to modify existing local access control methods appreciations to the authentication it provides for verifying users, processes that rely on users' computation and the resources needed for the authentication processes. The following requirements are results from the characteristics of the grid environment and its uses and must be met in order to create effective security architecture.

Most of the time, the industry-standard cryptographic technique AES-128 is used to safeguard conversations and data transmissions. Grid computing is a method that allows for powerful computation [5]. Utilizing dispersed geographically scattered resources in an organised manner, grid computing seeks to maximise system performance at a lower cost. Security features like as authentication, integrity as well as access control, privacy, and also no repudiation is essential in grid systems and applications. Concerns about identification and authorization include: - It gives authentication for checking the authenticity of the user's computer and its resources. It's backwards compatible with existing local access control techniques [6]. Single Sign On: Once authenticated, A user needs the ability to obtain resources, utilise and release them, and participate in secure communications without ever needing supplementary authentication. Passwords, private keys, and other forms of authentication information need to be safeguarded. Local security regulations ought to govern who has access to what resources locally, which should be compatible with local security solutions. There is an inter domain security service that can protect local resources even if they are modified. That is, they can't employ too much encryption all at once, thus the code has to be exportable. The amount of talk that goes on at once should be kept to a minimum. Protection for confidential group chats: in any one conversation, a number of processes are coordinating their actions. There is currently no such thing as a security strategy to ensure the safety of this kind of collaboration. A security policy that protects numerous data sources using public- and private-key cryptography should be able to accommodate a variety of implementations [7].

A. Single Sign-On

After a single successful authentication, users should have unrestricted access to all system resources and be able to freely exchange information with other system users and administrators.

B. Safeguarding Credentials

Private keys, user passwords, and other data should be secured.

C. Compatibility With Regional Security Systems

The security policy for access to local resources should also be implemented locally. There is an interdomain security server that can protect local resources even if they are modified.

D. Exportability

They can't employ too much encryption all at once since the code has to be able to be exported. The amount of talk that goes on at once should be kept to a minimum.

E. Provision For Safe Group Communication

In communication numerous processes work together to carry out its functions. There is currently no such thing as a security strategy to ensure the safety of this kind of collaboration.

F. The Support of Many Implementations

Security policies built on public as well as private key cryptography have to be implemented to protect data from a variety of sources.

III. GRID SECURITY CHALLENGES

Certification, authentication, and authorization are all handled by A and B's respective corporate security systems, but these services are managed separately. The two businesses do not have any trust for one another. The case in point is a collaborative activity in which a user from under domain A1 wants to use a resource that is coped by a user from under domain B1. Numerous sources offer the third party with the control policies. A VO is a decision-maker who oversees the allocation of different heterogeneous resources. There are three fundamental responsibilities that must be in place at all times because of the dynamic nature of legislation and the introduction of new participants: Extensive array of protections: Enterprises that are part of a VO have made investments in protective systems and infrastructure. These measures are crucial to the safety of the grid. Users should be able to independently develop new services (or "resources") on the fly, without requiring the participation of system administrators. These services must collaborate with one another. The ability to give the service a name and provide rights to that name in accordance with local norms and legislation is crucial. The ability of VO to dynamically establish trust domains is crucial to ensuring that the user can effectively communicate with all system components. Trust in a VO has to be dynamically established whenever people join or depart. In order for users to cooperate with VO resources, there must be a user-driven security plan in place [8]. The majority of the time, data that may be mined resides

ISSN No:-2456-2165

on heterogeneous platforms like grids, which is why these environments are so common. For both methodical and organisational causes, it is challenging to integrate entire data. As a result, it is crucial to offer techniques, tools, and services which make it easier to mine distributed data. These skills need to be easily integrated into distributed data mining systems so that difficult issues may be solved. Modern algorithms, grid services and other IT infrastructure are required for this. We require new techniques to mine these large datasets because of the sheer amount of data they contain. Complex data types are increasing in number. To enable such data mining on a grid, new strategies, algorithms, tools, and grid services will need to be developed. While automated data mining in decentralised contexts may be beneficial, there are legitimate privacy, security, and governance concerns that must be addressed. Any grid-based data mining system worth its salt will have to account for these factors. An effective user interface hides the underlying technological complexity of the system from the user. For grid-supported workflow management, resource identification, allocation, scheduling, and user interfaces, new software as well as tools, infrastructure is required.

The third party receives the control policies from a number of different sources. An VO is a person or organisation responsible for coordinating the distribution and use of available resources. Due to the ever-changing nature of regulations and the influx of new players into the system, it is essential that three core tasks be in place at all times:

A. A number of security measures:

Organisations taking part in Virtual Organisation have made investments in infrastructure and tools to ensure security. Such procedures are important to the security of the grid.

B. Dynamic service creation:

Users must be capable to dynamically develop their own services (e.g., resources) without needing to contact an administrator. These services need to work in tandem with one another. Therefore, we need to be able to give the service a name that complies with local norms and regulations and award rights to that name.

C. Establishing trust domains:

For VO to work effectively, it is necessary to create coordination between the user and all available resources. When users join or leave a VO, these spaces must dynamically create trust. To establish new user entries and coordinate with VO resources, a user-driven security paradigm are required (Energy Assurance Daily, 2007).

IV. ISSUES WITH GRID SECURITY

Grid computing systems face many of the same challenges as we did, including those related to user privacy, data security, authentication, and authorisation. A grid system is a means for dynamically pooling resources to maximise system efficiency [9]. Three broad categories can be used to group grid security concerns; Issues with architecture, infrastructure and management.

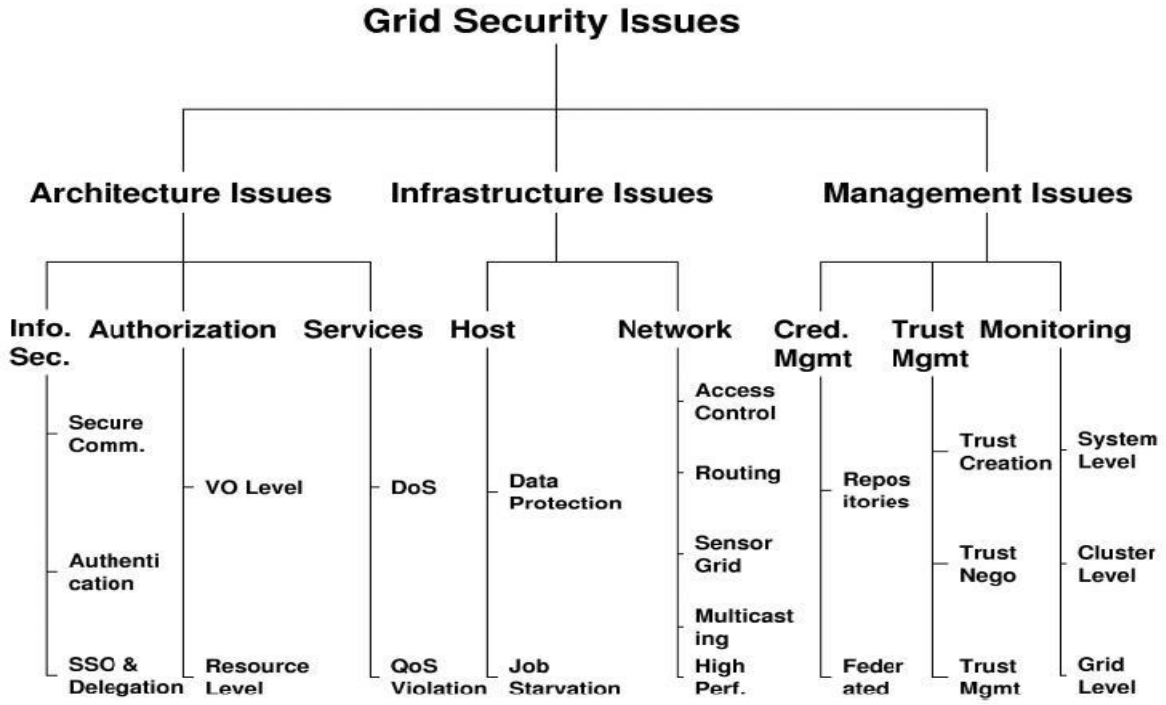

Fig.2 Security Issues of Grid[9]

A. Architecture Related Problems:

The grid's architecture is the subject of these problems. Because grid users worry about the data the grid contains, its

ISSN No:-2456-2165

confidentiality, integrity, and the validity of its users must be safeguarded [10]. Information security, authorisation, and service level security are all examples of architecture-level flaws that have the potential to throw the system into disarray. When using a grid, it's important to have permissions that are tailored to both the resources and the system itself. It's particularly useful for networks where several entities must pool their resources. There are two different kinds of authorisation systems: those that are virtual organization-level and those that are resource-level. Systems at the organisational level have a centralised authorization system that issues credentials to users in order to get access to resources, whereas systems at the resource level provide access to users on the basis of the credentials supplied by those users. There are two categories of grid service level security issues: Problems with quality-of-service violations and denial of service attacks. Forcibly violating QoS by an adversary via congestion, stalling or discarding packets, or resource hacking is at the heart of the QoS violation problem. When access to a service is restricted, DoS attacks become more severe [11]. Problems with the Grid's Infrastructure This category includes problems with the grid's infrastructure, namely its network and hosts. An individual host's concerns about its own security may make it hesitant to join the grid. Possible infrastructure-related problems include leaky data storage, a lack of available jobs, and inaccessible hosts [12]. Many different phases of implementing a grid computing infrastructure need attention to many potentially complex topics. Data management, information services as well as resource management and security are all places where these difficulties might crop up. There are two broad categories of infrastructure problems: host security problems and network security problems. Concerns concerning a host's security at the level at which it joins the grid are known as host level security problems. Data security and unemployment are two of the most pressing ancillary concerns [11].

B. Management Related Issues:

Managing the grid presents a third group of problems. Due to applications and grid frame's nature, pass administration is crucial in grid systems. Scheduling, rescheduling, monitoring, auditing, and recording are some of the several management concerns. In a pulsating grid situation, where users and nodes often enter also exit the system, managing trust is challenging. There are a number of steps involved in resource monitoring, including data collection, processing, transmission, storage, and display.

V. GRID SECURITY AREAS

In order to address the aforementioned grid security difficulties and obstacles, the following are the most common approaches:-

A. Authentication:

The authentication and authorisation of users seeking to make use of the grid's resources is where most grid security efforts are concentrated. Logging into the grid once should provide users access to all of its resources. Grids' continued success and widespread adoption depend on this single sign-on method for accessing their diverse and dispersed environments [13]. Single sign on utilising Public key infrastructure (PKI) based on X.509 certificates is increasingly used for grid middleware like Globus or gLite. PKI allows the grid to validate the user's certificate and for the user to confirm the entrance to grid using the certificate of grid, creating a trusting connection between the two parties. The middleware Globus and gLite take this basic authentication a step further by utilizing a user proxy method to assign the authorisations to the systems that either the user or the user's processes use to do computations or that store data that the user or the user's processes have requested. They grant permissions to proxy that in turn grants permissions to the processes the user initiates that need access to other systems in the grid. The proxy utilises temporary credentials that expire after a few hours rather than the user's, preventing the user's credentials from being leaked or made public. Grid file maps created on Globus and gLite are necessary for this type of user mapping. Requiring users to be a member of virtual organisations is another way to restrict access to resources in Globus and gLite (VO). Members of just certain VOs are granted access to grid infrastructure systems using this method [14].

B. Scheduling:

In grid computing, task scheduling and controlling a job's access to data is crucial, particularly when the performed process is data-intensive [15]. It is important to set aside CPU time, bandwidth, and data storage for programmes operating in grid settings. According to, distributed task scheduling boost scheduling efficiency and equips systems with portability, security and ability to distribute scheduling duty across a wide variety of computational sites in the system. This is because of the grid structure and the managed resources. Jobs on the grid might be scheduled differently depending on the gap between the required and provided security levels, which is taken into account in a new method to scheduling. Such gaps may arise as a result of mapping local user accounts to global user accounts on computing parts of grid, and must be taken into consideration during scheduling to prevent unauthorised users from altering or gaining access to critical data or calculations.

VI. SECURITY MODEL GLOBUS TOOLKIT

The two features of the Globus Toolkit Authentication as well as Authorization of serve as the de facto standard for Grid systems and applications' "core" security software. When implementing a Public Key Infrastructure (PKI), mechanism for certificate-based authentication that support single – sign on and delegation capabilities the required libraries and java classes and other tools are provided by the Globus software development kits. Tools like Grid Security Infrastructure (GSI) and Content Analysis Security (CAS) are used to keep data safe on the grid. These methods are used to symbolise safety and are used in a wide variety of grid projects. The OGSA framework is used by web security services. It is used to symbolise the process of restructuring, refining, and repacking different Grid protocols in order to make more efficient use of available resources [17]. In order to provide WSDL for interface in order to deliver Grid

services, OSGA is utilised with the Globus toolkit. For grid service discovery, OOSGA is also used as an interface. Relations among WS security mechanism as well as OSGA security mechanism and new have recently were a focus of OSGA security development.

A. Address Security techniques of GT4:

This study confirms the most pressing security concerns and addresses architectural problems. Given that, authorization, and information security, service-level security all contribute to architecture-level problems, the researcher offers a solution that combines the Authentication and GT4 model to manage these security concerns. Due to the fact that Grid is a virtual setting where different organisations can find out every one's resource, databases etc, preventing unauthorised users from doing so presents a significant challenge. The primary challenge is keeping track of who has access to what, who owns what resources, and who initiates data processing. The authentication procedure involves checking the user's credentials against a list of approved accounts stored either locally on the user's computer or on a remote server of authentication. Grid users are assigned local user accounts on the host systems, granting them permission to run the jobs and access the data they need to complete the tasks they have requested. Users create their own maps using gridmap-files in Globus and gLite. When developing services and applications for a distributed system, it is typical to run across issues that the Globus toolkit was designed to solve. The Grid Resource Allocation Management (GRAM) paradigm underpinning GT4 offers a interface based on web services for launching, observing, and controlling the running of a wide variety of computations across distributed nodes. A comprehensive security result is all time a system which integrates parts dealing by identity establishment, policy application, activity tracking, etc. to achieve predetermined objectives. Users must provide authentication information to prove their identity and get authorised access. Having established that the user is a genuine human being and that his personal details are consistent with those already stored in the database, to prevent architectural problems, the GT4 model will do the trick. GT4's security features are built on a strong foundation of industry standards, including the application of credential set-ups and procedures that deal with message encryption, delegation, and other topics at the lowest level. All participants are presumed to have X.509 public key credentials in this scenario. To provide remote access to resources, databases, etc., it is necessary for entities to verify each other's identities, setting up a safe channel for message safeguard, generate and convey proxy credentials. Mining for Common Sets on a Grid: An effective knowledge discovery process involves the transformation of data into meaningful patterns that may be used to get an in-depth understanding of a certain area. This data mining effort requires a distributed computing grid to operate well. Using a grid framework, you may access a distributed system that's capable of handling complicated processes via a simple front end. In order to implement cutting-edge distributed pattern recognition applications, Grid provides the required resources. With the authentication of users being permitted in a grid setting, mining of frequent item sets becomes safe. Take online shopping as an example, where you'll find that the most common layouts are grid-based.

VII. CONCLUSION

Since its inception, computational grid has garnered a great deal of interest as a promising path toward achieving distributed resource sharing. Accessing computational grid resources may be done using a number of different techniques, each with their own set of security criteria and ramifications aimed at users and providers of those resources This article presents an outline of security concerns related to Globus toolkit security model and authentication scheduling, and it adds to the existing body of research on grid security. The standards used by the larger Web Services community are included into GT4's security infrastructure. The Globus Toolkits Grid Security Infrastructure is designed to address the many security concerns that arise in grid computing (GSI). This advancement is used by its GSI implementation (GSI3) to improve the model of security used by earlier iterations of toolkit, since GT3 incorporates the developing Open Grid Services Architecture. Its success paves the way for a wide range of follow-up efforts. In addition, the researchers addressed the techniques based on authentication and the GT4 model to fix the difficulties at the architectural level. For the safety of grid resources, more stringent authentication mechanisms will need to be established in the future.

REFERENCES

[1]. A.R. Butt, A. Sumalatha, N.H. Kapadia, "Grid computing portals and security issues", Journal of Parallel and Distributed Computing 63 (10) (2003) 1006–1014.
[2]. I. Foster, K. Kesselman, "The Grid: Blueprint for a Future Computing Infrastructure" (Morgan Kaufmann in Computer Architecture and Design), 1999.
[3]. M. Humphrey, M.R. Thompson, K.R. Jackson, "Security for grids", Proc. of IEEE 93 (3) (March 2005) 644–652.
[4]. Ian Foster, Frank Siebenlist, Steven Tuecke, Von Welch, "Security and Certification Issues in Grid Computing" retrieved on 28th March, 2016 from https://pdfs.semanticscholar.org/115d/c00ae0551636e2c1f691849f06ae70657ced.pdf.
[5]. Neha Mishra, Ritu Yadav and Saurabh Maheshwari, "Security Issues in Grid Computing", International Journal on Computational Science & Applications (IJCSA) Vol. No.1, February 2014.
[6]. Report to NIST on Smart Grid Interoperability Standards Roadmap EPRI, June 17, 2009.
[7]. Ian Foster, Carl Kesselman & S Tuechkor (2001), "The Anatomy of Grid: Enabling Scalable Virtual Organization" retrieved on 29th March, 20016 from
[8]. Energy Assurance Daily, Sept 29,2007, US Department of Energy, Office of Electricity Delivery & Energy Reliability, Infrastructure Security & Energy Restoration Division 28th March, 2016.

[9]. A. Chakarbarti, "Taxonomy of Grid Security Issues" retrieved on 24th March, 2016 from International Journal of Scientific & Engineering Research, Volume 7, Issue 12, December-2016 ISSN 2229-5518 16 IJSER © 2016.
[10]. Globus Alliance: 2008, "GT 4.0 Reliable File Transfer (RFT) Service", March 2008.
[11]. R. Geetha & D. Ramyachitra, "Security Issues in Grid Computing", International Conference on Research Trends in Computer Technologies, Proceedings published in International Journal of Computer Applications® (IJCA) (0975 – 8887), 2013.
[12]. Anirban Chakrabarti, "Grid Computing Security (GCS)", 2008.
[13]. Muhammad Asif Habib and Michael Thomas Krieger, "Security in Grid Computing", Johannes Kepler University, A-4040 Linz, Austria, 2008.
[14]. Butler, R., Welch, V., Engert, D., Foster, I., Tuecke, S., Volmer, J., Kesselman, "C.: A NationalScale Authentication Infrastructure", Computer 33(12) 60–66, 2000.
[15]. Kim, B.J., Hong, S.J., Kim, and "Ticket-based fine-grained authorization service in the dynamic VO environment", In: SWS '04: Proceedings of the 2004 workshop on Secure web service, New York, NY, USA, ACM (2004) 29–36.
[16]. Xue, Y., Wan, W., Li, Y., Guang, J., Bai, L., Wang, Y., Ai, J, "Quantitative retrieval of geophysical parameters using satellite data", IEEE Computer 41(4) (2008) 33–40.
[17]. EGEE JRA3 team, "EGEE Global Security Architecture for web and legacy services", EU Deliverable DJRA3.3 (2005). International Journal of Scientific & Engineering Research, Volume 7, Issue 12, December-2016 ISSN 2229-5518.