International Journal of Mechatronics, Electrical and Computer Technology (IJMEC)
ISSN: 2305-0543 (Online), ISSN: 2411-6173 (Print)
Vol. 11 (42), Oct. 2021, pp. 5074-5084

IEEE
Nigeria Consultants' Network (CN)

A Survey of Security Threats in Distributed Operating System

Syed Muhammad Waqas, Sumra Khan, Arbaz Ahmed
Department of Computer Science, Bahria University
Karachi, Pakistan

***Abstract*—Over the last years, the security into software systems especially in the distributed system becomes complex day by day. The secure and trusted environment is a considerably important subject to address. Different services and resources in the distributed system have to be secure at different levels, for this reason, we have analysed in detail the flaws of the distributed systems, all the security threats, situations where the system at risk faces, and the best possible solutions to secure the distributed system. Globus security mechanism is discussed in detail well as how the authentication can be done and how do we achieve message confidentiality and integrity. Every idea that radiates all sorts of solutions to this matter is verified and well-studied. It provides the proper knowledge to help one understand the meaning of a secure system, the security policies, and the security mechanism.**

Keywords— Distributed operating systems, security, secure channels, threat, DDoS, fabrication

I. INTRODUCTION

The consistency of security tactics preserved by distributed systems is a significant threat [1]. Authentication, authorization, encryption, system protection are a few of the essential elements contained by the distributed system [2, 3]. Fundamentally, a distributed operating system is OS software for gathering different autonomous organized just as recognized computational nodes. Different positions are finished by different CPUs. Essentially, a distributed operating system addresses an expansion of the OS utilized in networks that aids more significant data exchange and blends of the system across the networks [4, 5]. The distributed system comprises different layers in the logical organization as shown in figure 1.

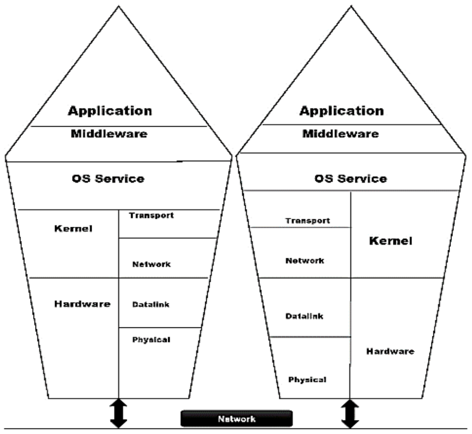

Figure 1: Different layers of Logical organization of distributed systems

In the beginning stage, the system of the security environment was reliant upon a single authority structure, notwithstanding, presently the improvement has been made concerning each activity, trained professional, and gathering with shared obligations [6]. The fundamental assaults on distributed systems are snooping (getting access towards confidential Intel), disguising (draw guesses about the personality of clients), and message tempering (destroying or editing data), replying, and rejection of the administration. The reliability of the distributed system is significant in various environments [7]. The interest for security in the distributed operating systems is developing step by step with the appearance of current innovation. Notwithstanding, but if the assailant has actual interaction with the proposed system, it gets furious to secure the framework concerned [6]. Different fundamental components of safety have appeared in Figure 2.

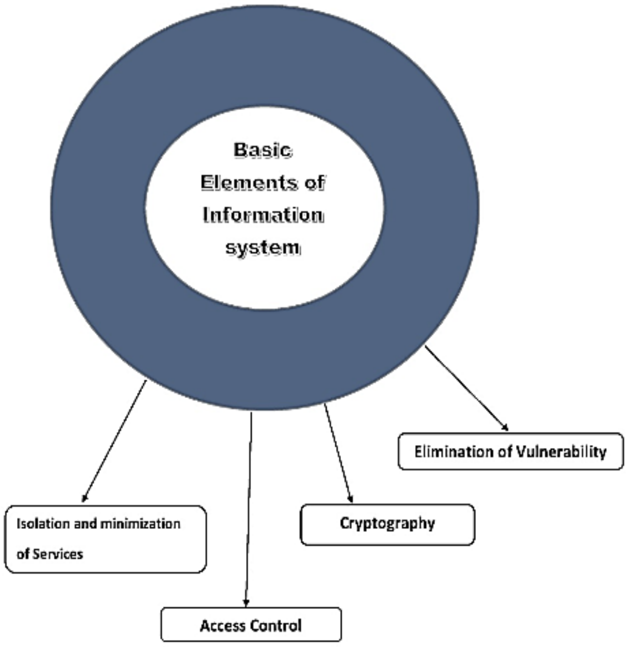
Basic Elements of Information system
Elimination of Vulnerability
Isolation and minimization of Services
Cryptography
Access Control

Figure 2: Essential components of data system security

Before discussing the variables affecting distributed system security, a framework for a distributed system is proposed and utilized as a structure for later analysis[9]. As we move forward connected to the world of computers, we realize that they are becoming increasingly distributive as we focus on the geographical aspect[10]. The purpose of distributed systems has long been admitted to be to connect and collaborate between different academic-like communities. Enterprises

Article History:
Received Date: Jul. 12, 2021, Accepted Date: Aug. 11, 2021, Available Online: Oct. 01, 2021

have considered extending the collaboration and data sharing belonging to varying businesses among enormous other cooperation entities that will fulfill the need and afterward utilize circulated assets and processing [11]. The distributed systems hold a common ground and goal to entail the interactive activities between various distinctive independent entities[3]. I simpler terms, distributed systems are where the CPUs do not work as a part of a single machine. To its users, it is displayed as any other ordinary centralized operative system. From the beginning of its existence, security has been an issue bearing the most important, that if not handled with exaggerated care, might harm the enterprises and the user communities massively [12-14].
Because of these scenarios, this paper aims to explain the concept behind security issues and the preventative measures taken against them in distributed systems.

This paper revives in Section 2 by presenting a brief Literature review. In Section 3, the Material and method of recent works are presented which are related to secure the distributed system. In Section 4, a detailed discussion of design issues and design requirements for the distributed system are discussed, and in Section 5, a detailed summary of attacks have been discussed that affect the distributed systems in one way or the other. In Section 6, the secure channel mechanism for a distributed system is discussed, different security approaches and their comparative study are discussed in Section 7and finally the conclusion is drawn in section 8.

II. RELATED WORKS

In [1], the author aimed for researching the security of distributed cluster, Grid, Database Systems, and Distributed storage using the technique of Grid authentication method, CIAA Threat model, multilevel secure database system which has benefited him in terms of improvement in the security of distributed resources, distributed data, and grid computing. In [15] author went on to research on Secure framework for ATMs in 2017 using the mechanism of SFAMSS Framework having the benefits to ensure confidentially, non-repudiation and integrity. In [7] the author researched Review security issues in distributed systems using the mechanism of Path authentication technique, which has the advantages of ensuring a secure grid environment. In [9] author has made researches on the Evaluation of Reliability patterns by adopting the method of Reliability pattern approach and is beneficial in terms of system designer and developer. In [8], research on Safeguarding security and protection in distributed systems in 2011 using the mechanism of a nonexclusive structure for three-factor validation and has benefited in terms of Affordable because of smart card application due to its efficient design. In 1994, using the technique of distributed management system architecture, Morris Sloman [16] had researched on isolating administration strategy from robotized administrators, which has the advantages of Automated distributed systems can deal by the automated manager. Bhupendra Singh Thakur, Sapna Chaudhary, in [17] researched on Detection of Content sniffing attacks using the algorithm of automatic file rendering and has its advantages of Secure the programs against content sniffing attacks. In 2017, using the algorithm of Shannon entropy and Granular computing[17] research on Finding potential features of Dos attack which has benefited in terms of time required for detecting Dos attack is reduced. In [18] author has researched on Enhancement in security and scalability of distributed systems using the technique of Enhancing Kerberos framework using Public-key cryptography which is good to achieve fully distributed authentication. Research on Secure communication in distributed systems has done by Tyron Standing [19] using the mechanism of Identity-Based Encryption in 2003 which is favorable for Secure, efficient, authenticated communication in a distributed systems.

Author and Title	**Year**	**Research Aim**	**Model / Algorithm / methods**	**advantage**
Morris Sloman	1994	Separating management policy from automated managers	distributed management system architecture	Automated distributed systems can deal by an automated manager
Marvin A. Sirbu, John Chung-I Chuang	1997	Enhancement in security and scalability of distributed systems	Enhancing Kerberos framework using Public-key cryptography	To achieve fully distributed authentication
Tyron Stading	2003	Secure communication in distributed systems	Identity-Based Encryption	Secure, efficient, authenticated communication in the distributed system.
Mohamed Firdhous	2011	security of Distributed clusters, Grid, Database Systems, and Distributed storage	Grid authentication method, CIAA Threat model, multilevel secure database system	Improve the security of distributed resources, distributed data, and grid computing
Xinyi HUANG Yang Xiang Ashley Chonka Jianying Zhou Robert H. DENG	2011	Preserving security and privacy in distributed systems	A generic framework for three-factor authentication	Affordable because of smart card application due to its efficient design
Vijay Prakash, Manuj Darbari	2012	Review on security issues in the distributed system	Path authentication technique	Ensuring a secure grid environment
Ingrid A. Buckley, Ph.D., and Eduardo B. Fernandez	2012	Evaluation of Reliability patterns	Reliability pattern approach	Useful for system designers and developers
Bhupendra Singh Thakur, Sapna Chaudhary	2013	Detection of a Content sniffing attack	automatic file rendering	Secure the programs against content sniffing attack
Stephen Specht, Ruby Lee	2013		Taxonomy of DDoS Countermeasures	Prevent systems from attacking DDoS attack
ZEINAB GHAFARI ,TAHA ARIAN AND MORTEZA ANALOUI	2017	Secure framework for ATMs	SFAMSS Framework	Ensures confidentially, non-repudiation and integrity

III. Materials and Methods

SECURITY

A. Security Threats, Policies, and Mechanism

Security Threats:

There are four types of security threads provided by the distributed system against security threats. Interception: An unauthorized user endeavors to access assistance or information. For example, we are replicating information, sniffing passwords.

Interruption: Services or data become blocked off, unusable, or demolished, for instance, denial - of - service attacks, wiping out of data.

Modification: Unauthorized persons access the data as well as change the data or meddling with assistance so it no longer holds quickly to its subtleties. For instance, it is obstructing and changing conveyed data, modifying a program so it subtly logs the exercises of its client.

Fabrication: an unauthorized user inserted a fake message into the network. For example, we have included a passage to a secret word data set, replaying recently sent messages.

Security Policies:

This figures out what is secure for the framework or association, or substance. It essentially alludes to the limitations on the attributes of the individuals and regulations forced upon the foes by different procedures. So, a security policy exercises the components in a structure allowed to take and which ones are denied [20].

DISTRIBUTED SYSTEM 'S SECURITY MECHANISM

A distributed system's security mechanism is envisioned for forestalling or recuperating from a security assault. A security administration essentially utilizes at least one security instrument. Generally, a security administration improves the security of the information preparing frameworks [21, 22].

- Security instruments maintain security courses of action.
- Huge security instruments.

– Encryption: changes data into something an assailant can't grasp.

– Validation: checks the declared character of a part.
– Authorization: grants components to simply get to those resources that they are equipped for access.

– Auditing: logs which clients got to what and what bearing.

The internet server running on a grouped framework. Giving mechanisms to secure the framework against:

- External assaults
- Internal assaults
- Detection
- Reaction

IV. Design Issue

Heterogeneity: Heterogeneity is applied to the organization, PC equipment, working framework, and execution of various designers. A critical segment of the heterogeneous dispersed framework customer worker climate is middleware. Middleware is a bunch of administrations that empowers applications and end-client to connect across a heterogeneous disseminated framework [23].

Openness: The straightforwardness of the dispersed framework is settled basically by how much new asset-sharing associations can be made open to the clients. Accessible designs are depicted by how their key interfaces are appropriated. It depends upon a uniform correspondence section and scattered interface for enlistment to shared assets. It will, as a rule, be made from heterogeneous equipment and programming [23].

Scalability: The adaptability of the framework ought to stay effective even with a critical expansion in the number of clients and assets associated [23].

Security: The security of a data framework has three parts confidentiality, honesty, and accessibility. Encryption secures shared assets, maintains delicate data mysteries when communicated [23].

Failure Handling: When a few issues happen in equipment and the product program, it might deliver erroneous outcomes, or they may stop before they have finished the proposed calculation, so restorative measures ought to execute to deal with this case[23].

Disappointment taking care of is troublesome in circulated frameworks because the disappointment is incomplete, i.e., a few segments come up short while others keep on working.

Concurrency: There is a likelihood that few customers will endeavour to get to a common asset simultaneously. Different clients make demands on similar assets, i.e., read, compose, and update. Every asset should be protected in a simultaneous climate. Any article that addresses a common asset in a conveyed framework should guarantee that it works effectively in a simultaneous climate [23].

Transparency: Transparency guarantees that the appropriate framework ought to be seen as a solitary substance by clients or the application software engineers as opposed to the assortment of independent frameworks, which are coordinating [23]. The client ought to be uninformed of where the administrations are found and the moving from a neighbourhood machine to a distant one ought to be straightforward.

A. REQUIREMENTS FOR DISTRIBUTED SYSTEM DESIGN

Execution problems Responsiveness: Intelligent applications need a quick and predictable reaction. At the specific the reaction is gotten is settled not just by the server and network burden and execution, yet furthermore by the deferrals in all the item portions included, i.e., the OS, the middleware organizations, (for instance, far away distant strategy conjuring like naming) and the application code itself offering the help.

Throughput: This is the rate at which computational work is done (number of customers updated each second) and is impacted by the planning speeds and at customers and workers and data move rates.

Balancing computational loads: Intensely loaded servers it is important to utilize a few servers to host solitary assistance and to offload work (for example an applet on account of a web server [24-26] to the customer where plausible. Cycles in a distributed system (instance customer side and server-side cycles) cooperate by passing messages, bringing about correspondence (message passing [27, 28], and coordination (synchronization and requesting of exercises[29]) among measures. Each interaction has its state. The two critical elements influencing measure collaboration in distributed systems, for example, Communication execution [30] is regularly a restricting trademark and no single worldwide thought of time since timekeepers on various PCs will in general float.

There are three methodologies for insurance against security threats.

-Security in opposition to invalid operations
-Security in opposition to unauthorized invocations
-Security in opposition to unauthorized users

V. Different types of Attacks that affect Distributed system

Vulnerability: It demonstrates a deficiency in the framework that empowers an assaulting specialist to make unseemly malignant conduct[31].
Threat: A danger is something pointed toward hurting the framework.
Compromise: It alludes to the effect of the weak assault.
Exploit: It implies software misuses the weakness/powerlessness of a framework.
Payload: This alludes to executing the activities pre-arranged as the point of the concerned assault.
Rootkit: It alludes to a bunch of projects that shrouds the existence of the aggressor concerned.
Malware: This is the nonexclusive name for pernicious projects.

- Virus: It suggests a code that multiplies automatically by attaching its relating code to the whole activity.
- Backdoor: It suggests a strange piece of code that engages unapproved access.
- Trojan: It shows a good code including an undocumented similarly as the secret influence on others.
- Logic/postponed bomb: It implies when a specific condition is satisfied then a piece of code executes.
- Worm: It suggests a code that induces automatically successfully through looking at the network reasonably.
- Bacteria: It suggests a code that can copy itself for draining the system's resources locally.

External Attacks:

The different sorts of outer assaults that can happen are outlined in Figure 4.

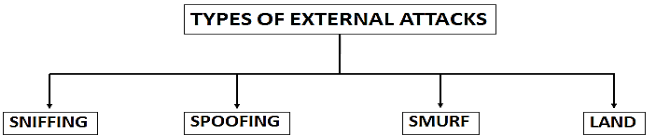

Figure 4 different types of outer assaults

Sniffing attack:
Sniffing is an interaction of checking and catching all information parcels going through a given organization. Sniffers are used by the network/structure head of an organization to screen and investigate network traffic. Aggressors use sniffers to catch information parcels containing delicate data like passwords, account data, and so forth.

Spoofing:
Spoofing is the point at which an aggressor imitates an approved gadget or client to take information, spread malware, or sidestep access control frameworks. There are various sorts of Spoofing, with three of the most well-known being: IP address parodying - Attacker sends packets over the organization from a bogus IP address.

Smurf Attack:
A Smurf Attack is a denial-of-service (DoS) attack that incorporates sending ICMP reverberation demands (ping) traffic to the transmission address of switches and different network devices in huge PC networks with a spoofed source address (the location of the ideal DoS target)[17].
On the off chance that the first solicitation (to a device in a vast network) is communicated to a particularly huge number of machines, the subsequent assault can be exceptionally compelling. After 1999, regardless, most switches don't propel parcels delivered off their transmission addresses. This makes the likelihood of a viable colossal extension Smurf Attack truly low. [17].

Landing:
It is described as the wonder of duping the person in question while in correspondence with them.
Many assaults on machines and cycles go with specific kinds of assaults.

Information Theft:
This includes the way toward assuming control over the vital data from different machines.
Lately, there has been a considerable proportion of information concerning burglaries, for instance, Visa number burglary, ATM satirizing, electronic money robbery, data set burglary, etc.

Denial-of-Service (DoS):
A DoS attack alludes to the protection that wins at whatever attacker starts activities that keep the authentic clients from

gaining admittance to focused PCs viable or some other organization assets[32].
Normally, such assaults flood the servers, frameworks, or networks with the traffic to overpower the casualty assets to make it rushed or incomprehensible for the approved clients to get to it[33].

At whatever point a doubt emerges for a DoS attack, the associations or ventures call their ISP for verification that whether the inferable from a DoS attack or then again because of something different. A while later, the ISP helps with moderating the attack by choking the malicious traffic by utilizing the load balancers to decrease attacks. The good judgment of DoS affirmation can be analyzed through interference expectation systems, interference distinguishing proof structures, and so forth additionally, in coursed working systems, the affiliation-related gadgets nearby the PC are dirtied by malware[34, 35]. The different sorts of DoS attacks have appeared in Figure 5.

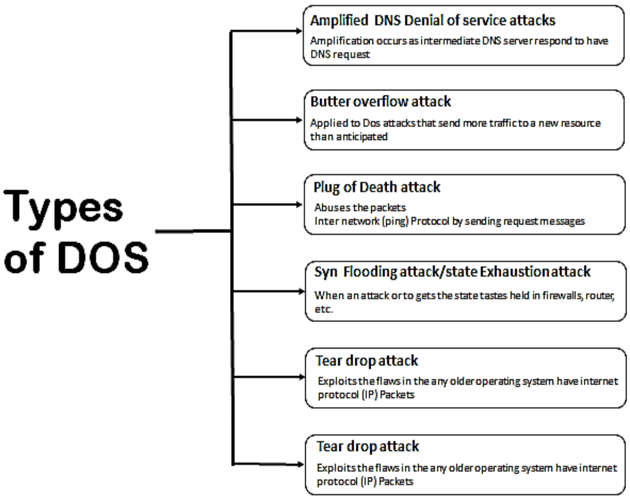
Types of DOS
Amplified DNS Denial of service attacks
Amplification occurs as intermediate DNS server respond to have DNS request
Butter overflow attack
Applied to Dos attacks that send more traffic to a new resource than anticipated
Plug of Death attack
Abuses the packets
Inter network (ping) Protocol by sending request messages
Syn Flooding attack/state Exhaustion attack
When an attack or to gets the state tastes held in firewalls, router, etc.
Tear drop attack
Exploits the flaws in the any older operating system have internet protocol (IP) Packets
Tear drop attack
Exploits the flaws in the any older operating system have internet protocol (IP) Packets

Figure 5 Types of DoS attacks security

VI. SECURE CHANNELS:

A. Authentication

The one significant security threat is authorization. It is a system that shows if a massive activity is allowed. Same as other asset sharing structures, matrix figuring frameworks need asset explicit and explicit approval. Secure Channel-based authentication is a sort of verification that upholds the protected exchange of validation information. It is utilized in blend with Cronto pictures or QR codes to exchange the Secure Channel messages. This verification process requires the utilization of Digipass licenses activated using multi-device licensing (MDL)[8]. The working of the Secure Channel-based authentication is shown in Figure 6.

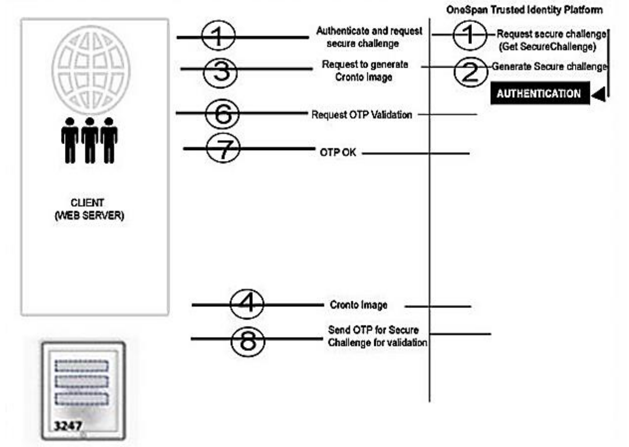
OneSpan Trusted Identity Platform
CLIENT (WEB SERVER)
1
Authenticate and request secure challenge
3
Request to generate Cronto Image
6
Request OTP Validation
7
OTP OK
4
Cronto Image
8
Send OTP for Secure Challenge for validation
1
Request secure challenge (Get SecureChallenge)
2
Generate Secure challenge
AUTHENTICATION
3247

Figure 6 Secure Channel-based authentication

The authorization system is divided into 2 categories in the grid computing system, VO (virtual organization). The first one is considered a level system, and the second one is a resource level system. VO framework has a unified approval system that gives credits for the administrators to gain admittance to the assets. other than that, resource level structures are decentralized and permitted the customers to put their hands on the buys dependent upon the credits showed up by the heads [8, 36].

VO level system:
VO, a dynamic group of individuals or groups of firms, elaborate the terms and conditions (business goals and procedures) for sharing funds. VO caliber grid computing organization is a centralized authority for the whole VO. Structures are made huge if the VO is accessible there, which includes sets of customers and various resource providers (RP) who are the owners of the assets for being worked by the heads of the VO. On the other side whenever a customer wants to get to the particular resources asserted by RP, they have an accreditation from the approval framework, which lets the administrators guarantee the explicit right.

Resource Level System:

Other than a centralized authorization system, decentralized systems have implemented the decisive step to make authorization to get access to the set of assets. Asset suppliers offer offices to the local gatherings. This interaction is completed to acquire the trust relations of local communities. On the other side, an end client wants to get their hands on the assets; they create their accreditations that have acquired unmistakable strategy attestations. The asset supplier has to concede or deny the solicitation for admittance to the support. The end clients introduce the certifications to the resources to gain admittance to it. In this sort of structure, the resources need to hold over the last position to supporting or keeping the system from getting end clients.

Message Integrity and Confidentiality
Message Integrity:

Large scale distributed computing system has specific concern towards data integrity such as the grid whose soul production is the outcome of the computation. If data integrity ought to be maintained, then the system must be resistive towards the aggressor attacks. The security mechanism is dependent on two categories, transport-level security and message-level security[6, 37].

- Transport Level Security: The network connections on the transport layer is encoded by TLS and SSL. Asymmetrical cryptography has been used in TSL and SSL for the vital exchange; symmetrical has been used for message authentication codes for message integrity and privacy integrity. For the security of the communication between the client and the server, Globus Toolkit 4.0 (GT4) uses the SSL/TLS protocol over HTTP is used. As shown in Figure 7.

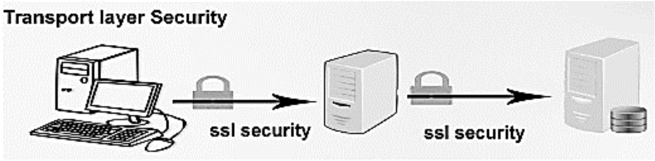

Figure 7 Transport Level Security

- Message Level Security: operates at the upper level and uses the web services based on WS- Security, WS-Secure Conversation, etc which are the standard protocols. These standard protocols propose to establish plus use specific context and SOAP messages (Simple Object Access Protocol). Initially, a secure framework is created between a client and a server. If the secure framework is established, then the following messages are signed utilizing the XML-signature standard. XML- signature works with a symmetrical key to sign messages, which is also the reason for its fast operations, but additional round trips are also required to maintain connections. This procedure works properly for several interactions. GSI operates the system to give security on a per-message basis, i.e., there is no pre-existing situation between the receiver and sender to an individual message. As shown in Figure 8.

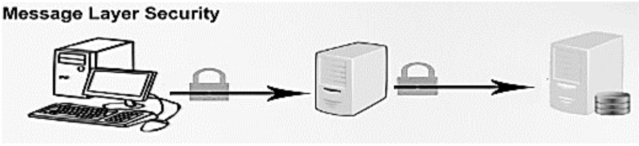

Figure 8 Message Level Security

Confidentiality:

There are two special encryption techniques known as symmetrical and asymmetrical (public) used for making secure grids:

- Symmetrical encryption: single secret key is shared to perform to encrypt as well as decrypt information. To make sure that the data is only revealed between two users (the one who sends the message and the one who receives the message); the key should only be given to the two users who are sender and receiver. Regarding performance, this form of encryption dominates asymmetrical encryption but should be handled more carefully with additional administrative care of the shared key[37]. Some examples of symmetrical key protocols include Data Encryption Standard (DES), Rivest Cipher 6 (RC6), and Advanced Encryption Standard (AES). The exchange security relies upon symmetrical critical protection. Suppose an aggressor captures the symmetrical key; he will read the ciphertext and create a new one[18]. As shown in Figure 9.

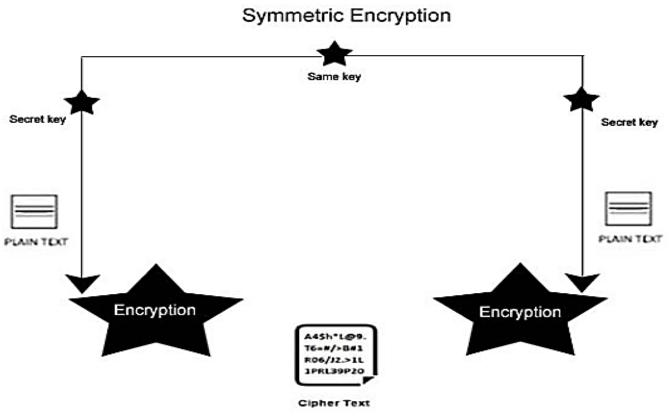

Figure 9 Symmetric Encryption

- Asymmetric Key Encryption: This produces public key as well as private key pairs dependent on crypto graphical secure mathematical methods. Suppose a message is encrypted with the public to only be decrypted with a private key in comparison. Public access is visible to everyone. The symmetrical key has created the computation that beginnings by discovering two incredibly enormous apparent numbers. Even if the public is distributed extensively, it is impossible for the pcs to calculate the private key from the public key.

The security fact tells that it is tough to surpass hundreds of digits. Security is improved through this mathematical algorithm, but a very long encryption time is required, specifically for the data in access amount. Public key encryption is mainly utilized to send symmetrical encryption keys between the two gatherings, and further encryption is performed utilizing symmetrical keys [18]. As shown in Figure 10.

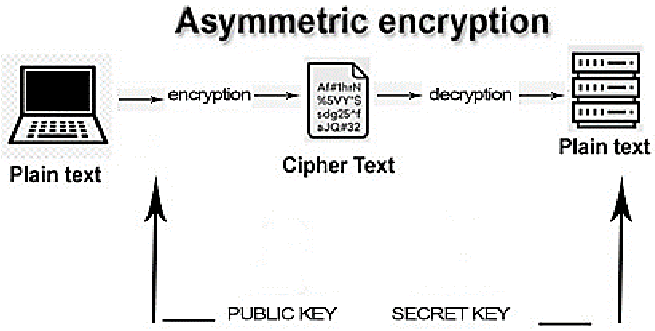

Figure 10 Asymmetric Encryption

SECURE GROUP COMMUNICATION

Secure groups can be elaborated as:

- Members whose authentication and trust are promised are permitted to involve.

- Group messages are kept confidential, integrated, and guaranteed.

- Perfect Forward Secrecy (PFS): group keys cannot be revealed by compromising long-term secrets.

- Forward Confidentiality: previous volunteers cannot achieve keys utilized in the future (FCY). The requirement duo that the present member cannot have keys utilized previously is called Backward Confidentiality (BCY)[19]. In support of FCY, every time a member joins or leaves, the group keys should always be changed. There might be a high value. Hence, attempts should be made to put FCY at ease without tearing security in both Ensemble and the DVPN system[38].

With the help of the Access Control List (ACL), members' trust policies are elaborated. Other than the above 3 requirements, another requirement allows members to change their ACLs [30] dynamically.

If the four requirements are elaborated in motivation, suppose there is a meeting of military staff with the full support of civilian advisors. While the security for the meeting is low, they put low-security information out to the advisors. In the past, the gathering is entitled characterized, regular citizens, leave the room, and the tactical staff keeps on completing the community with the utilization of high-security data. While the civilians were still in the room, high-security information was not revealed[37].

GLOBUS SECURITY ARCHITECTURE

This policy and the manner that security instruments provide in distributed systems to implement such types of strategies are greatest settled by assuming a model. Allow us to talk about the security policy required for the Globus wide-region framework [3]. Essentially, Globus is a framework that upholds massive scope distributed computation where several hosts, records, and different assets are simultaneously employed for doing the computation. These conditions are additionally referred to as computational frameworks[39].

The security plan for Globus incorporates accompanying assertions:

The environment comprises various administrative domains.

Local operations: It addresses the activities that are led uniquely inside a solitary space. These are simply exposed security policies of a local domain.

Global operations: it addresses the tasks about few domains that want the alarmed initiator to be acknowledged in each field any place the activity is being led.

Activities between substances in particular domains need joint verification.

Global authentication is placed on a position of local authentication.

Controlling admittance to the assets is predominantly only exposed to local security.

Clients can appoint the privilege to the processes.

Certifications can be divided between measures in the same domain.

There are many administrative domains, but local security is present on it is each part. It is additionally perceived that local policies can't be changed since the field participates in Globus. Therefore, guarantee in Globus precludes itself from working, which can hamper a few areas applicable to this issue. Besides, Globus accepts that local tasks to a domain are considered just to the concerned domain's security policy. The Globus security strategy implies that different solicitations for activities can be started either locally or universally. The initiator can be a client or cycle following up in a client's interest and privately known inside every domain [40].

When a client or a cycle following up for a client gets verified, it gets fundamental to confirm the specific access rights regarding assets. For instance, a client wishing to refresh a document will initially be validated; a short time later, it tends to be confirmed whether the concerned client is essentially allowed to refresh the record. The Globus security strategy portrays that the access control decisions are outlined locally inside the domain of the location of the accessed resource. Besides, Globus centers around security dangers implying different disciplines. In particular, the security strategy exhibits the portrayal of a client in any distant domain, just as the distribution of assets from a far-off domain to a client or his agent. The architecture of the Globus security strategy is as demonstrated in Figure 11.

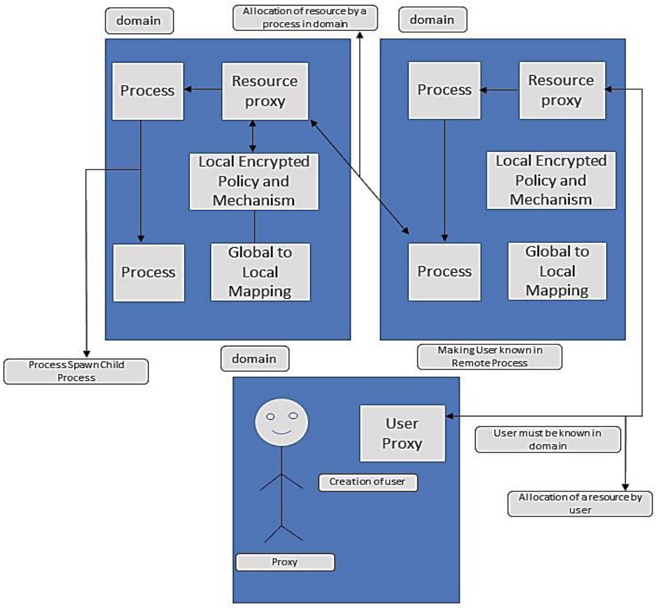
domain
Allocation of resource by a process in domain
domain
Process
Resource proxy
Process
Resource proxy
Local Encrypted Policy and Mechanism
Local Encrypted Policy and Mechanism
Process
Global to Local Mapping
Process
Global to Local Mapping
Process Spawn Child Process
domain
Making User known in Remote Process
User Proxy
User must be known in domain
Creation of user
Allocation of a resource by user
Proxy

Figure 11 Architecture of global security policy.

Distribution of Security Mechanism

The reliance existing among administrations concerning trust brings about the thought of a Trusted Computing Base (TCB). A TCB addresses a bunch of all security instruments in a disseminated PC framework that is vital for guaranteeing a security strategy needed to be trusted[29, 41]. The more modest the TCB is, the better it will be. Besides, TCB in a distributed system can consolidate the neighborhood working frameworks at a few hosts. A document worker in a disseminated record framework may be accepted on the few assurance components managed by the local operating system[6, 42]. Besides, middleware-based distributed systems need to confide in the current local operating system. If no trust exists, part of the usefulness of the local operating system must be joined into the distributed system itself[31].

VII. Different Security Approaches in Distributed Systems

Different sorts of safety approaches are utilized to make a safe distributed system. The few important approaches, which are trust-based, authentication-based, cryptography techniques based and access control-based.

Authentication Based Security

The authentication procedure is proposed in [38]. On-request way revelation algorithm is suggested to empower domains to protection in the cooperation environment. A transport scheme to access of substances in appropriated distributed systems has been proposed in [29]. Heterogeneously dispersed frameworks are profoundly pertinent in different applications, as electronic exchange handling frameworks, stock statement update system which needed an integration of authentication, integrity, and confidentiality. systematic security-driven planning engineering is introduced in [39]. This strategy has been proposed for DAG (Direct Acyclic Graph). The methodology powerfully gauges the trust of every node. The verification of the remote client is a significant exploration region in the distributed systems. A three-factor-based validation approach is discussed in [8]. In this, two-factor validation has been stretched out to three-factor verification; it guarantees customer security proficiency in disseminated frameworks. The three components used to foster this methodology are, password, smart card, and biometrics. In [43], different parts of the security in distributed systems have been given including, user authentication using passwords and digital certificates and confidentiality in information transmission. The job of authentication servers in distributed computing systems has been examined in [2]. The primary plan issue is the cryptographic calculations, synchronization, and measure of trust. A got secret phrase-based verification with a believed outsider is created in [2]. The methodology depends on a notable authentication protocol, called Kerberos.

Trust-Based Security Approaches

It is created for different application [44] ,alike to P2P framework. This model provide significant part for securing the framework of distributed application. An extended D-S theory-based trust model (ExDSTM) is created in [11]. Other D-S hypothesis models are proposed in [42, 45, 46]. A dynamic and context-sensitive trust-based security component has been created in [13]. Hazard the executives has been coordinated into security by utilizing a trust model in [47]. Method represents that hazard the board can be applied to amplify the use of the appropriated framework.

Access Control Based Security

In the most essential sense, access control in data security is tied in with figuring out who gains admittance to what stuff (documents, catalogs, applications, and so on) For instance, in the event that I access our organization's record worker, I can see reports identified with showcasing. Somebody in our Finance office, then again, would have the option to audit monetary reports. Yet, somebody outer to the organization would not have the option to get to any of these things.

On the other hand, objects could be assets that you need to shield from unapproved access, use, or revelation. What's more, the subject is the client (or gathering of clients or even non-individual substances like applications or administrations) that the entrance controls apply to. Thus, access controls (in a more specialized sense) are the devices, arrangements, models, and instruments that empower you to allow or confine admittance to your association's advanced or actual assets. This incorporates everything from confining or allowing admittance to explicit documents and information bases to IT frameworks and actual areas.

Essentially, these sorts of physical and consistent limitations keep unauthorized people from doing things they shouldn't with your touchy frameworks or information. Moreover, they likewise help to forestall accidental openness or divulgence of delicate things.

Cryptography Based Approaches

A structure of safety in a distributed framework fundamentally representing a gadget level framework handle is introduced in [6]. Public key cryptography, software agents, and XML binding innovations are designed for this methodology. The improvement of protected distributed framework utilizes different methodologies, similar to Public Key Infrastructure (PKI) and Role-Based Access Control (RBAC). In [40], the RBAC approach is utilized to foster verification dependent on Public Key Certificates (PKC).

Policy-Based Approaches

The policy of system security component is created in [20]. This structure gives particular security arrangements and autonomous of the hidden framework. This structure depends on space explicit language for implementation, verification, and specification of distributed security strategies.

The real coordination of safety approaches in distributed framework is talked about in [48]. So, The approaches of security are physically arranged and consequently authorized to the distributed framework.

Pattern-Based Security

Different sorts of safety designs for distributed system security are gotten in [9]. Different sorts of example-based security systems are very much examined and their development and fittingness are assessed.

Quorum Based Security Systems

Quorum systems are profoundly pertinent for tackling the issue of information consistency in distributed fault-tolerant systems in [49], an Intrusion-Tolerance Quorum System [ITOS] of half breed time model dependent on Trust Timely Computing Base (TTCB) is introduced. A job-based admittance control model has been created in [48]. The Role Ordering (RO) schedulers are presented alongside simultaneousness control dependent on the meaning of jobs relegated to the exchanges.

Other Security-Based Approaches

A mobile agent-based security framework is introduced in [48]. This framework check and examines the strength of safety and different dangers. This framework is to identify unlawful practices and retaliate in interruption with countermeasures is called self-protection. A procedure for assessing, implementing, and evaluating oneself ensured framework has been proposed in [50]. The proficient coordinated effort among security and protection for disseminated framework security has been talked about in [51]. The plan of distributed security frameworks can be advanced. A hereditary algorithm is utilized for this reason in [52]. A security heterogeneity approach for booking models in the appropriated framework is developed in [53]. A novel heuristics scheduling algorithm is introduced, which endeavors to boost the likelihood that all undertakings are running with no danger related to the assault. In [54] XtremWeb design has been talked about which comprises of figuring working in huge scope distributed system. The architecture of the system and parallel programming paradigms are talked about well overall. A proposition for secure exchange in a mobile system dependent on the delegate object model in [55]. It centers around the difficult issue of appropriated nature in present-day PC frameworks. The RAIN innovation is examined in [56], which is an examination coordinated effort among Caltech and NASA-JPL on circulated processing. A few verifications of idea applications are created: like an exceptionally accessible web worker, video worker conveyed check-pointing framework. A legitimate Information Flow (LIF) scheduler is introduced in [57]to synchronize transactions to forestall illicit data streams.

COMPARATIVE ANALYSIS OF THE SECURITY OF DISTRIBUTED SYSTEM

Many security approaches are discussed in [7] [58][36] to make distributed environment secure. These are authentication Based Security, Pattern-Based Security, Policy-Based Approaches, Trust-Based Security, Quorum Based Security Systems, and other security technique [7, 58, 59]

SNO	category	Focus	reference
		Authentication technique based on the path	[38]
		Scheduling architecture for security	[39]
		Client authentication based on remote	[8]
		digital certificates, password, and confidentiality	[43]
		Cryptography approach in the authentication of servers	[2, 6, 40]
		Blockchain-based approach	[59]
		challenge-response based RFID protocol	[58]
2	Policy-Based security	Modular security policies	[20, 8]
		Risk management P2P system context	[47]
		P2p system	[44]
		Extended D-S theory-based model	[11,42, 45, 46]
		Context-Sensitive trust model	[42]
4	Quorum based security	Distributed false tolerance	[49]
		Security pattern for distributed system	[9]
		Mobile agent-based system	[60]
		Generic Algorithm based	[52]
		X-Torn web architecture	[54]
		RAIN Technology	[56]
		LIF scheduler	[57]

VIII. CONCLUSIONS AND FUTURE SCOPE

Today's computing infrastructure that has a threat environment is highly exposed because of the widespread adoption of distributed computing architectures. In this survey paper, we surveyed background solutions that were designed to secure the distributed system. The security challenges in the distributed system require further study. Different researchers from industry and organization as well as from academia provided possible solutions to these security challenges in the previously published study**.** It is our belief, that through closing the gaps identified in this survey paper, a complete solution that is capable of securing the distributed systems can be finally achieved. Authentication, access control, cryptographic techniques, quorum-based systems, trust-based models, etc. are many developments towards the generation of secure and trusted distributed systems. The detailed review is presented in this survey provides the distributed security issues requirements, identified threats, and known vulnerabilities.

References

[1] M. Firdhous, "Implementation of security in distributed systems-a comparative study," *arXiv preprint arXiv:1211.2032,* 2012.

[2] P. Chatterjee, E. R. Kumar, C. Mamatha, and M. G. Kumar, "SECURITY IMPLEMENTATION IN DISTRIBUTED SYSTEMS-ATM," *International Journal of Mechanical Engineering and Technology (IJMET),* vol. 8, pp. 680-683, 2017.

[3] Y. Bai, "On distributed system security," in *2008 International Conference on Security Technology*, 2008, pp. 54-57.

[4] P. K. Sinha, *Distributed operating systems: concepts and design*: PHI Learning Pvt. Ltd., 1998.

[5] A. S. Tanenbaum and M. Van Steen, *Distributed systems: principles and paradigms*: Prentice-hall, 2007.

[6] Y. Xu, L. Korba, L. Wang, Q. Hao, W. Shen, and S. Lang, "A security framework for collaborative distributed system control at the device-level," in *IEEE International Conference on Industrial Informatics, 2003. INDIN 2003. Proceedings.*, 2003, pp. 192-198.

[7] V. Prakash and M. Darbari, "A Review on Security Issues in Distributed Systems," *International Journal of Scientific & Engineering Research,* vol. 3, p. 1ISSN, 2012.

[8] X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R. H. Deng, "A generic framework for three-factor authentication: Preserving security and privacy in distributed systems," *IEEE Transactions on Parallel and Distributed Systems,* vol. 22, pp. 1390-1397, 2010.

[9] A. V. Uzunov, E. B. Fernandez, and K. Falkner, "Securing distributed systems using patterns: A survey," *Computers & Security,* vol. 31, pp. 681-703, 2012.

[10] K. Nuredini, "Security Issues in Distributed Systems-A survey," in *1st International Symposium on Computing in Informatics and Mathematics*, 2013.

[11] L. Jiang, J. Xu, K. Zhang, and H. Zhang, "A new evidential trust model for open distributed systems," *Expert Systems with applications,* vol. 39, pp. 3772-3782, 2012.

[12] O. Demir and B. Khan, "Quantifying distributed system stability through simulation: A case study of an agent-based system for flow reconstruction of ddos attacks," in *2010 International Conference on Intelligent Systems, Modelling and Simulation*, 2010, pp. 312-317.

[13] Y. Ding, F. Liu, and B. Tang, "Context-sensitive trust computing in distributed environments," *Knowledge-Based Systems,* vol. 28, pp. 105-114, 2012.

[14] H. Koshutanski, "A Survey on distributed access control systems for web business processes," *IJ Network Security,* vol. 9, pp. 61-69, 2009.

[15] Z. Ghafari, T. Arian, and M. Analoui, "SFAMSS: a secure framework for atm machines via secret sharing," *arXiv preprint arXiv:1505.03078,* 2015.

[16] M. Sloman, J. Magee, K. Twidle, and J. Kramer, "An architecture for managing distributed systems," in *1993 4th Workshop on Future Trends of Distributed Computing Systems*, 1993, pp. 40-46.

[17] B. S. Thakur and S. Chaudhary, "Content sniffing attack detection in client and server side: A survey," *International Journal of Advanced Computer Research,* vol. 3, p. 7, 2013.

[18] M. A. Sirbu and J.-I. Chuang, "Distributed authentication in Kerberos using public key cryptography," in *Proceedings of SNDSS'97: Internet Society 1997 Symposium on Network and Distributed System Security*, 1997, pp. 134-141.

[19] T. Stading, "Secure communication in a distributed system using identity based encryption," in *CCGrid 2003. 3rd IEEE/ACM International Symposium on Cluster Computing and the Grid, 2003. Proceedings.*, 2003, pp. 414-420.

[20] H. Hamdi and M. Mosbah, "A DSL Framework for Policy-Based Security of Distributed Systems," in *2009 Third IEEE International Conference on Secure Software Integration and Reliability Improvement*, 2009, pp. 150-158.

[21] M. Sloman, "Policy driven management for distributed systems," *Journal of network and Systems Management,* vol. 2, pp. 333-360, 1994.

[22] W. T.-M. Yao, "Fidelis: A policy-driven trust management framework," in *International Conference on Trust Management*, 2003, pp. 301-317.

[23] H. Tillwick and M. S. Olivier, "A Layered Security Architecture: Design Issues," in *Proceedings of the Fourth Annual Information Security South Africa Conference (ISSA2004)*, 2004.

[24] J. Domingo-Ferrer and J. M. Mateo-Sanz, "Practical data-oriented microaggregation for statistical disclosure control," *IEEE Transactions on Knowledge and data Engineering,* vol. 14, pp. 189-201, 2002.

[25] P. Samarati, "Protecting respondents identities in microdata release," *IEEE transactions on Knowledge and Data Engineering,* vol. 13, pp. 1010-1027, 2001.

[26] W. Qi, J. Song, and Y.-b. Bao, "Near-uniform range partition approach for increased partitioning in large database," in *2010 2nd IEEE International Conference on Information Management and Engineering*, 2010, pp. 101-106.

[27] S. Vijayarani and M. P. Jothi, "Partitioning clustering algorithms for data stream outlier detection," *International Journal of Innovative Research in Computer and Communication Engineering,* vol. 2, pp. 3975-3981, 2014.

[28] D. Toshniwal, "Clustering techniques for streaming data-a survey," in *2013 3rd IEEE international advance computing conference (IACC)*, 2013, pp. 951-956.

[29] S. Pallickara, J. Ekanayake, and G. Fox, "A scalable approach for the secure and authorized tracking of the availability of entities in distributed systems," in *2007 IEEE International Parallel and Distributed Processing Symposium*, 2007, pp. 1-10.

[30] M. Sawant, K. Kinage, P. Pilankar, and N. Chaudhari, "Database partitioning: a review paper," *International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN,* pp. 2278-3075, 2013.

[31] S. B. B. Priyadarshini, A. B. Bagjadab, and B. K. Mishra, "Security in Distributed Operating System: A Comprehensive Study," *Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies,* pp. 221-230, 2019.

[32] S. Khan, A. Gani, A. W. A. Wahab, and P. K. Singh, "Feature selection of denial-of-service attacks using entropy and granular computing," *Arabian Journal for Science and Engineering,* vol. 43, pp. 499-508, 2018.

[33] S. Specht and R. Lee, "Taxonomies of distributed denial of service networks, attacks, tools and countermeasures," *CEL2003-03, Princeton University, Princeton, NJ, USA,* 2003.

[34] T. Peng, C. Leckie, and K. Ramamohanarao, "Detecting distributed denial of service attacks using source IP address monitoring," in *In Proceedings of the Third International IFIP-TC6 Networking Conference (Networking 2004*, 2002.

[35] D.-N. Le, V. N. Van, and T. T. T. Giang, "A New Private Security Policy Approach for DDoS Attack Defense in NGNs," in *Information Systems Design and Intelligent Applications*, ed: Springer, 2016, pp. 1-10.

[36] B. C. Neuman, "Proxy-based authorization and accounting for distributed systems," in *[1993] Proceedings. The 13th International Conference on Distributed Computing Systems*, 1993, pp. 283-291.

[37] M. He, A. Hu, and H. Qiu, "Research on Secure Key Techniques of Trustworthy Distributed System," in *2009 International Conference on Computer Engineering and Technology*, 2009, pp. 172-176.

[38] M. Shehab, A. Ghafoor, and E. Bertino, "Secure collaboration in a mediator-free distributed environment," *IEEE transactions on parallel and distributed systems,* vol. 19, pp. 1338-1351, 2008.

[39] T. Xiaoyong, K. Li, Z. Zeng, and B. Veeravalli, "A novel security-driven scheduling algorithm for precedence-constrained tasks in heterogeneous distributed systems," *IEEE Transactions on computers,* vol. 60, pp. 1017-1029, 2010.

[40] W. Chang-Ji, W. Jian-Ping, and D. Hai-Xin, "Using attribute certificate to design role-based access control," in *Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies*, 2003, pp. 216-218.

[41] W. Stallings, *Cryptography and network security, 4/E*: Pearson Education India, 2006.

[42] B. Yu and M. P. Singh, "An evidential model of distributed reputation management," in *Proceedings of the first international joint conference on Autonomous Agents and Multiagent Systems: Part 1*, 2002, pp. 294-301.

[43] P. A. F. Vitti, D. R. dos Santos, C. B. Westphall, C. M. Westphall, and K. M. M. Vieira, "Current issues in cloud computing security and management," *SECURWARE,* vol. 2014, p. 47, 2014.

[44] K. S. Ramana, A. Chari, and N. Kasiviswanth, "A survey on trust management for mobile ad hoc networks," *International Journal of Network Security & Its Applications,* vol. 2, pp. 75-85, 2010.

[45] L. D. Huang, G. Xue, X. L. He, and H. L. Zhuang, "A trust model based on evidence theory for P2P systems," in *Applied Mechanics and Materials*, 2010, pp. 99-104.

[46] J. Wang and H.-J. Sun, "A new evidential trust model for open communities," *Computer Standards & Interfaces,* vol. 31, pp. 994-1001, 2009.

[47] C. Lin and V. Varadharajan, "Trust based risk management for distributed system security-a new approach," in *First International Conference on Availability, Reliability and Security (ARES'06)*, 2006, pp. 8 pp.-13.

[48] P. Rai and P. Singh, "An overview of different database security approaches for distributed environment," *IJISET-International Journal of Innovative Science, Engineering & Technology,* vol. 2.

[49] H. Zhou, X. Meng, L. Zhang, and X. Qiao, "Quorum systems for intrusion-tolerance based on trusted timely computing base," *Journal of Systems Engineering and Electronics,* vol. 21, pp. 168-174, 2010.

[50] N. De Palma, D. Hagimont, F. Boyer, and L. Broto, "Self-protection s*Distributed Systems,* vol. 23, pp. 330-336, 2011.

[51] S. S. Yau, P. A. Bonatti, D. Feng, and B. Thuraisingham, "Security and privacy in collaborative distributed systems," in *29th Annual International Computer Software and Applications Conference (COMPSAC'05)*, 2005, p. 267 Vol. 2.

[52] P. Bykovyy, Y. Pigovsky, V. Kochan, A. Sachenko, G. Markowsky, and S. Aksoy, "Genetic algorithm implementation for distributed security systems optimization," in *2008 IEEE International Conference on Computational Intelligence for Measurement Systems and Applications*, 2008, pp. 120-124.

[53] T. Xie and X. Qin, "Performance evaluation of a new scheduling algorithm for distributed systems with security heterogeneity," *Journal of Parallel and Distributed Computing,* vol. 67, pp. 1067-1081, 2007.

[54] F. Cappello, S. Djilali, G. Fedak, T. Herault, F. Magniette, V. Néri, *et al.*, "Computing on large-scale distributed systems: XtremWeb architecture, programming models, security, tests and convergence with grid," *Future generation computer systems,* vol. 21, pp. 417-437, 2005.

[55] N. Shenbagavadivu and S. U. Savithri, "Enhanced Information Security in Distributed Mobile System Based on Delegate Object Model," *Procedia Engineering,* vol. 30, pp. 774-781, 2012.

[56] V. Bohossian, C. C. Fan, P. S. LeMahieu, M. D. Riedel, L. Xu, and J. Bruck, "Computing in the RAIN: A reliable array of independent nodes," *IEEE Transactions on Parallel and Distributed Systems,* vol. 12, pp. 99-114, 2001.

[57] T. Enokido and M. Takizawa, "A Legal Information flow (LIF) scheduler for distributed systems," in *2007 International Conference on Parallel and Distributed Systems*, 2007, pp. 1-8.

[58] K. Rhee, J. Kwak, S. Kim, and D. Won, "Challenge-response based RFID authentication protocol for distributed database environment," in *International Conference on Security in Pervasive Computing*, 2005, pp. 70-84.

[59] S. Shetty, C. A. Kamhoua, and L. L. Njilla, *Blockchain for distributed systems security*: John Wiley & Sons, 2019.

[60] O. T. Arogundade, T. E. Abioye, and M. Sanjay, "An ontological approach to threats pattern collection and classification: a preliminary study to security management," *International Journal of Electronic Security and Digital Forensics,* vol. 12, pp. 323-335, 2020.