WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Implicit Password Authentication System Cryptosystem Based on Cloud Security Network

[1*]A. Arthi, [2]Ms. U. Sriaishwarya

[1]Master of Computer Applications, Gnanamani College of Technology, Namakkal.
[2]Assistant Professor, Master of Computer Applications, Gnanamani College of Technology, Namakkal.
[*] Email Id: aarthiprabaharan123@gmail.com

ABSTRACT

The encryption standard provides key assumption to the analytical With the recent adoption and diffusion of the data sharing paradigm in distributed systems such as online social networks or cloud computing, there have been increasing demands and concerns for distributed data security. However, most of them are not applicable for mobile cloud since mobile devices only have limited computing resources and power. Solutions with low computational overhead are in great need for mobile cloud applications. It enables data owners to define their own access mobile cloud policies over user attributes and enforce the policies on the data to be distributed. However, the advantage comes with a major drawback which is known as a key escrow problem. The key generation center could decrypt any messages addressed to specific users by generating their private keys. Therefore, in this study, we propose a novel KP-ABE scheme for a data sharing system by exploiting the characteristic of the system architecture. The proposed scheme features the following achievements: 1) the key escrow problem could be solved by escrow-free key issuing protocol, which is constructed using the secure two-party computation between the key generation center and the data-storing center, and 2) fine-grained user revocation per each attribute could be done by proxy encryption which takes advantage of the selective attribute group key distribution on top of the ABE.3) Also third party Auditing (TPA) organize the security. The performance and security analyses indicate that the proposed scheme is efficient to securely manage the data distributed in the data sharing system..

Keywords*: Task Scheduling, Network Resource Scheduling, Cloud Computing, Dynamic Priority Sharing, Cloud Cryptography.*

1. INTRODUCTION

Cloud computing and resource scheduling over some time with real-time access to various users. There should be a good deal to achieve greater performance in a shared environment of co-operation. Task scheduling must include multiple objectives and constraints and optimal scheduling in the cloud. The class of problem is called to which the NP-hard problem and resource mapping task belong. An inevitable task scheduling problem in cloud computing to solve quality services. The user must meet the planning instructions to respect the cloud service provider position restrictions. The user constraints, such as duration, schedule constraints and meet security and budget needs.

Limiting the cloud service provider, such as maximizing resource utilization, maximizes its effectiveness and increases the number of completed jobs. Standard Optimization help gets the job done in the shortest time, with the least cost and safety. Where the user does not specify any deadline or any commercial provision, therefore, to optimize the design of the scheduling algorithm's standard map, the job should be considered in or above the resource constraints specified by the user and the cloud service provider. Traditional security issues remain in cloud computing environments. Organizations start using the Cloud. However, traditional security technologies are no longer suitable for cloud applications and data.

According to the service mode, cloud computing resources in the cloud environment are owned by multiple vendors. Due to conflicts of interest, it isn't easy to set up a unified security mechanism. Virtualization is a key factor in the success and popularity of cloud computing. Virtualization is achieved by management software. If someone violates the data protection management plan, all the exposures stored in the Cloud are exposed. The virtualization de-allocation process and resource allocation can lead to the deletion of all data with proper planning and resource management.

2. RELATED WORK

Cloud computing, plays a crucial role in improving resource utilization and improving overall performance in a novel algorithm computing cloud called Previous Finish Time with Contrast. Task Priority [1]. The process of relational task planning is an important one and a new approach to task prioritization related to the computation of an optimized payment schedule. Work priority and parental duties are planned according to copy to reduce contact costs and obtain an optimal scheduling solution [2].Cloud service providers cannot be regarded as a trusted third party of a semi-exclusive nature. Therefore, in the conventional security model, you will not be able to put together a direct framework as a cloud computing-based group that to share. This article

proposes a public cloud that can effectively use with the help of cloud servers, but without any sensitive data, a new secure group sharing framework that exposes attackers and cloud service providers [3]

The major challenge in the cloud environment there is Load-Balancing (LB). This is to ensure that no one node has not been borne too [5], which is a dynamic workload of each node. It is by ensuring a reasonable distribution of the high efficiency and the computing resources and achieve high user realized and resource utilization.

The first DLBS problem to formulate, develop a network model for a typical open stream. A set of effective heuristic scheduling algorithms balance two for data slot stream [6,7]. High data centers imbalance degree, data is flowing, will be a lot of improvement in our DLBS methods are brought to the data center [9].Group Key Management Protocol (GKMP) for cloud storage file sharing. It is recommended from the public channel and group key generation scheme based on hybrid encryption technology to face network attacks [10]. A verification scheme to prevent a shared file from collusion attack by the cloud provider and the group members [11].

A security model and protocol for a flexible audit protocol with a formal definition and main exposure has been proposed. Use the preorder traversal technology and binary tree structure, our design, and update the client's key [12,13]. In addition, to build a property of the support forward security and verification, we have developed a new certification. The security issues in cloud computing to increase it provides efficiency and reliability services. Here are two kinds of CC security, namely data security and network security. Types of attacks are common on scan ports such as network security [14], IP cheating, death ping, and packet sniffing.

Key Agreement Protocols Note that secure and efficient group data sharing plays a vital role in CC. In this study, using the Symmetric Balanced Incomplete Block (SBIB) format will be supported by multiple participants in the cloud environment [15]. Based on the design of a flexible contract, it can extend the number of participants to support the new batch of internal agreements.

3. PROPOSED METHODOLOGIES

In this proposed work, a systematic method of balancing tasks with the consumption of loads and security is addressed. The energy consumption of the cloud data center is minimized through our proposed load balancing algorithm.

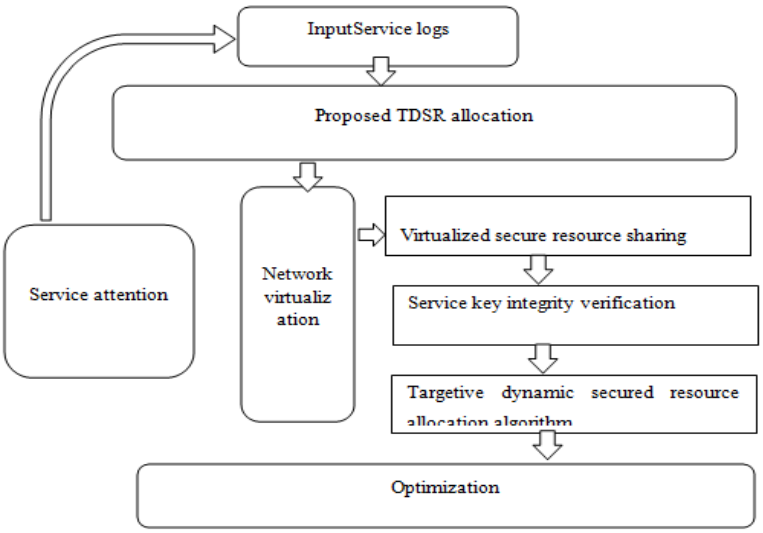

Figure 1: Proposed Architecture Diagram TDSRA

And also introduced a security model to improve the user's trust model providing in the cloud. In public key with encryption, properties are based on cryptography. Figure 1 shows the proposed architecture diagram TDSRA

3.1 Virtualized Secure Resource Sharing

This rvirtualized security analysis approaches with some requests for cloud servers submitted by all users. Region analysis was used to monitor all incoming requests on all routes and communicated to the corresponding Region of the request based on that region's

While Ri is in Region in Region List

DRT (Distributed Route Table)

If (ur_id in Ri)

Verify User security Group [r_id] = $\sum_{i=0}^{ur\_id} ur_{id} + Ri$

Verify service list (sl) =$\sum_{i=0}^{ur\_id} r_{id} + user\_Service(load)$

Else

Add Region DRT (Distributed Route Table)

Set key-value →Ri

End if

If Check DRT Statues (Active State, Down State (or) Busy)

Add DRT region and Sl

End if

The algorithm uses three separate steps; the first one is for the analysis domain, and the second domain shows the key values of the DRT, each other index assignment on the DRT (distributed routing table) Map all incoming requests, including route information active, and downstate (or busy

3.2 Service Key Integrity Verification

The end-stage requires users to create and use resources to allocate. All technologies allow users to identify and format the presentation as follows: identifies the user request policy, toxic or benign. This method is similar to a small one, with the same number of annoying user development strategies frustrating as weight and user needs. It also provides a key for the user and verifies every session connect to the cloud server.

Algorithm:

Input: Cloud Services Cs, Session Key(Sk)

Output: Resource Allocation Ra

Start

If (user request-id== true)

Generate (Sk);

Sk=$\sum_{i=1}^{ra=a} ra(a-z\&\&(0-9)*8)^2$

For each service, Si

Calculate cloud size CCS= $\frac{\text{service(si)}}{\text{Si}} \times \text{Cid(Si)} \times \text{Sd(Si)}$

End

Calculate average services CAS =$\frac{\sum_{i=1}^{\text{size(Si)}} \text{Si(CCS)}}{\text{size(Cloud)}}$

If CAS> Belief service size

Resource Allocate

Else

Return false.

If (User ReQ==Sk)

Allow CAS;

End,

Stop.

The resource allocation and relief calculation register the trust weight for each time window. In light of the resource and edge esteem, the decrease was performed. Because of believed weight, the user orders as the cloud environment

3.3 Targetive Dynamic Secured Resource Allocation Algorithm

The end-stage requires users to create and use resources to allocate. All technologies allow users to identify and format the presentation as follows: identifies the user request policy, toxic or benign. This method is similar to a small one, with the same number of annoying user development strategies frustrating as weight and user needs. It also provides a key for the user and verifies every session connect to the cloud server.

Algorithm:

Input: Cloud Services Cs, Session Key(Sk)

Output: Resource Allocation Ra

Start

If (user request-id== true)

Generate (Sk);

Sk=$\sum_{i=1}^{ra=a} ra(a-z\&\&(0-9)*8)^2$

For each service, Si

Calculate cloud size CCS= $\frac{\text{service(si)}}{\text{Si}} \times \text{Cid(Si)} \times \text{Sd(Si)}$

End

Calculate average services CAS =$\frac{\sum_{i=1}^{\text{size(Si)}} \text{Si(CCS)}}{\text{size(Cloud)}}$

If CAS> Belief service size

Resource Allocate

Else

Return false.

If (User ReQ==Sk)

Allow CAS;

End,

Stop.

The resource allocation and relief calculation register the trust weight for each time window. In light of the resource and edge esteem, the decrease was performed. Because of believed weight, the user orders as the cloud environment

4. RESULT PERFORMANCE EVALUATION

This simulation framework is developed in NS2 used to create a cloud environment. The proposed method is tested with 150users with a cloud server. The simulation details and screenshots are present below .

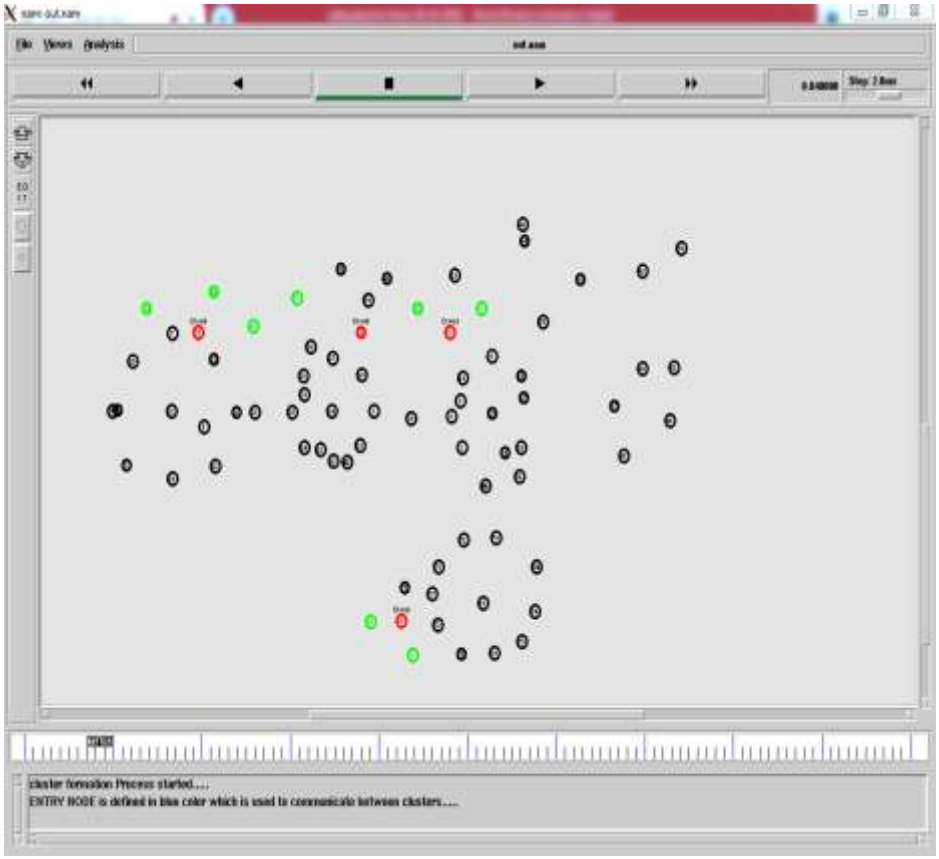

Figure 2: Scheduling Process CPU Utilization Task Process

Figure 2 describes are exploiting this task and analyzing the number of VM in each physical machine; it uses the Machines on the server. The user must first register how many Task Processes it has. Then, according to this, the Machine is made allocated.

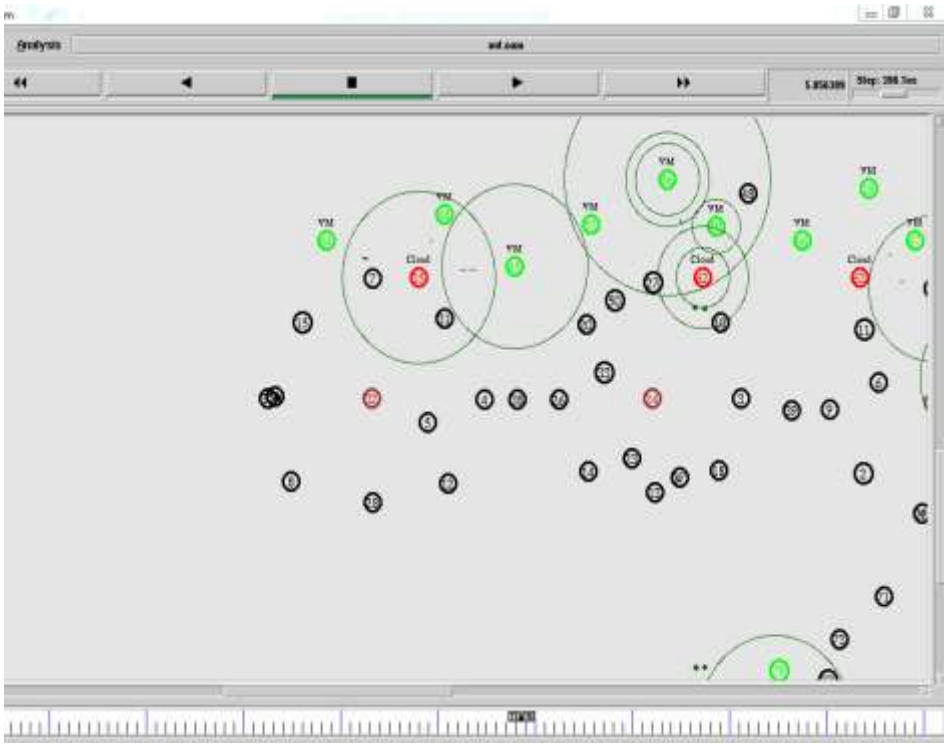

Figure 3: Resource Allocation through File Process

Figure 3, the user can use their file to do it. The user has to register their IP address, and then the user has to specify the path to which file it wants to do.

Table 1: Comparison of Service Utilization

Cloud Requests	**LBS**	**VM-Migration**	**Dynamic priority**	**TDSRA**
	Service Utilization in %			
10	90	91.2	94.2	96.1
30	89	90.5	93.2	95.5
60	87.5	89.4	89.5	95.2
90	84.1	87.1	92.4	94.8
120	83	86.7	90.5	94.5
150	81	85	90	93.4

The service availability user data pack Table 1 in one message sends another message to be Internet can some conversion of system cloud resource allocation message type of number bandwidth model.

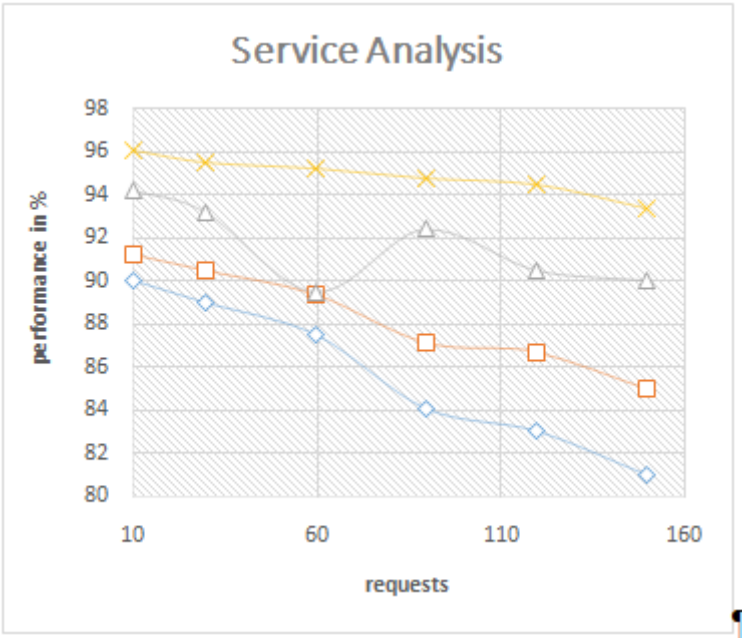

Figure 4: Cloud Service Analysis

Above Figure 4 describes the cloud service analysis; the proposed TDSRA compared with the previous approach is LBS and dynamic priority. The proposed TDSRA algorithm Cloud service analysis result is 93.4%; likewise, the existing approach results are VM-Migration algorithm cloud service analysis result is 85%, and Dynamic Priority algorithm cloud service analysis result is 90%.

As a result, the data server can retrieve more bytes of data during client requests in traffic bytes/sec.

Table 2: Comparison of the Transmission Analysis

Time in sec	**LBS**	**VM-Migration**	**Dynamic Priority**	TDSRA
	Delay in bytes			
10	2000	2800	3100	4000
30	2300	2950	3300	4500
60	2655	3000	3340	4400
90	2650	3150	3420	4700
120	2700	3205	3500	4820

Table 2 shows the comparison of transmission analysis, and the proposed TDSRA algorithm provides a transmission range is 4820 bytes for 120 sec to the client.

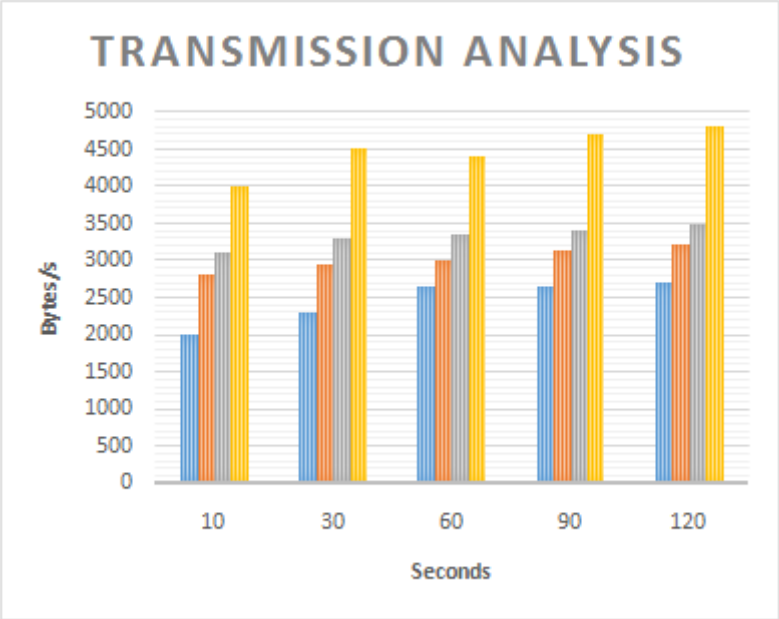

Figure 5: Data Transmission Analysis

Figure 5 is showing the data transmission as a byte displaying the graph. In this graph, the x-axis represents the bytes, and the y-axis represents a number of seconds. The proposed method TDSRA provides 4820 bytes compare to the existing method LBS, VM-Migration and dynamic priority methods, respectively 2700bytes, 3205bytes, 3500bytes.

5.CONCLUSION

Cloud server workload analysis verifies the content performance of each cloud server response. In a cloud computing workload, the server should focus on the maximum number of tasks it handles to balance the scene. Using this virtualization technology, provide the physical machine, not user security access control. Each physical machine is divided into virtual machines with different numbers of physical resources. These virtual machines are bundled with different physical resources. Executed when requesting a job scheduling task for resources allocated to a VM work. This TDSRA Method has scheduled the resource efficiently and gives more security for users. It gives better results and performance compared to the existing method.

Acknowledgement: Nil

REFERENCES

[1]. Wu, K., Lu, P., & Zhu, Z. (2016). Distributed Online Scheduling and Routing of Multicast-Oriented Tasks for Profit-Driven Cloud Computing. IEEE Communications Letters, 20(4), 684–687.

[2]. Tang, F., Yang, L. T., Tang, C., Li, J., &Guo, M. (2016). A Dynamical and Load-Balanced Flow Scheduling Approach for Big Data Centers in Clouds. IEEE Transactions on Cloud Computing, 1–1. doi:10.1109/tcc.2016.2543722

[3]. Liu, H., He, B., Liao, X., & Jin, H. (2017). Towards Declarative and Data-centric Virtual Machine Image Management in IaaS Clouds. IEEE Transactions on Cloud Computing, 1–1.

[4]. Ruan, L., Yan, Y., Guo, S., Wen, F., &Qiu, X. (2019). Priority-based residential energy management with collaborative edge and cloud computing. IEEE Transactions on Industrial Informatics, 1–1.

[5]. Xue, K., & Hong, P. (2014). A Dynamic Secure Group Sharing Framework in Public Cloud Computing. IEEE Transactions on Cloud Computing, 2(4), 459–470.

[6]. Saraswathi A.T. Kalaashri Y.R.A. and Padmavathi S. (2015), 'Dynamic resource allocation scheme in cloud computing', Procedia Computer Science, Vol. 47, pp.30-36

[7]. Jiang H. Yi J. Chen S. and Zhu X. (2016) 'A multi-objective algorithm for task scheduling and resource allocation in cloud-based disassembly', Journal of Manufacturing Systems, Vol. 41, pp. 239-255.

[8]. Mohta, R.K. Sahu and L.K. Awasthi, "Robust Data Security for Cloud while using Third Party Auditor", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, 2012

[9]. Jia Yu, KuiRen, Cong Wang, &Varadharajan, V. (2015). Enabling Cloud Storage Auditing With Key-Exposure Resistance. IEEE Transactions on Information Forensics and Security, 10(6), 1167–1179.

[10]. Tianqi Zhou, JianShen, Debiao He, Yuexin Zhang, Xingming Sun, and Yang Xiang, "Block Design-based Key Agreement for Group Data Sharing in Cloud Computing" IEEE 2017 Page No (1-15)

[11]. Juarez F. Ejarque J. and Badia R.M. (2018) 'Dynamic energy-aware scheduling for parallel task-based application in cloud computing', Future Generation Computer Systems, Vol. 78, pp. 257-271

[12]. Haratian, P., Safi-Esfahani, F., Salimian, L., &Nabiollahi, A. (2018). An Adaptive and Fuzzy Resource Management Approach in Cloud Computing. IEEE Transactions on Cloud Computing, 1–1. doi:10.1109/tcc.2017.2735406

[13]. S. More and S. Chaudhari, "Third Party Public Auditing scheme for Cloud Storage", 7th International Conference on Communication, Computing and Virtualization, Science direct, pp. 69-76, 2016.

[14]. Victor Chang, Muthu Ramachandran "Towards Achieving Data Security with the Cloud Computing Adoption Framework" 2016 IEEE Transactions on Services Computing, Volume: 9, Issue: 1, Jan.-Feb. 1 2016, pp - (138 - 151).

[15]. Juntao Chen, Quanyan Zhu "Security as a Service for Cloud-Enabled Internet of Controlled Things Under Advanced Persistent Threats: A Contract Design Approach"2017 IEEE Transactions on Information Forensics and Security, Volume: 12 , pp - (2736 - 2750).