DLINE JOURNALS

Journal of Information Security Research

Print ISSN: 0976-4143
Online ISSN: 0976-4151

JISR 2024; 15 (1)
https://doi.org/10.6025/jisr/2024/15/1/1-10

# Analysis of Cloud Services Attacks and its Solution

Farhan Nisar[1], Samad Baseer[2]
[1]Department of Computer Science Department of Computer Science Qurtaba University, Pakistan
{farhansnisar@yahoo.com}

[2]University of Engineering & Technology, Pakistan
{Drsamadbaseer@uet.edu.pk}

**ABSTRACT**

*With the development of Cloud computing applications in recent years, Cloud Computing plays a very important role in all environments for data storage, roles and services in the Cloud Computing Architectures. This is the main advantage of Cloud Computing that data can be stored in remote servers and can be accessed by the Cloud Users distantly. However, the advantages completely contain the drawbacks of data security in Clouds because of security issues, and this paper provides the proper solution. This paper presents a detailed study of cloud security attacks in cloud services in IaaS, PaaS, and SaaS components, its security issues, and how they prevent attacks.*

**Received: 18 August 2023**
**Revised: 29 November 2023**
**Accepted: 29 December 2023**


**Keywords:** Cloud, Cloud Computing, Cloud Services, Cloud Security, IaaS, PaaS, SaaS, Security Attacks And Their Solution

## 1. Introduction

*Cloud computing is used for large groups of internet working computers. These computers are personal computers or organization computers, i.e. these computers may be used for public or private purposes. For example, Microsoft hosts Microsoft Cloud, which can be publicly accessible by Microsoft users and privately accessible by its users. Cloud offers services according to the users' needs, in which they pay for resources. This framework is designed for security benefits and availability, and new opportunities are created for security purposes.*

*There are many possible attacks in the cloud computing environment, i.e. security threads from hosts, Security threads from other Virtual Machines, and Denial of service attacks. Browser attacks and many compatibility-checking problems. Cloud Computing is working against the attacker, but some extension support is enabling the attacker to damage the availability service starting from the single point entry. In research, we identify different security attacks in cloud computing environments and their prevention.*

## 2. Evolution of Cloud Services

*There are three services available in Cloud Computing*

*1) Infrastructure as a Service (IaaS)*

*2) Platform as a Service (PaaS)*

*3) Software as a Service (SaaS)*

### 1) Infrastructure as a Service (IaaS)

*In this cloud computing service, only infrastructure is available. They provide users only lease or rent services that use only storage, processing and other network resources. The IAAS model is also called storage as a service. In the IAAS environment, users can easily create, launch and terminate the connection from the server and pay for it when they need services for an hour or use it for a day.*

### 2) Platform as a Service (PaaS)

*This is the 2nd type of service which can be provided by cloud computing. They provide only a platform or tools to the users to develop their applications without using the proper software on their personal computers.*

*This service is also useful for businesses where users can create their own applications. This is very complex for users because it enables quick application according to customers' requirements. It is a next-level cloud computing service model built under the IaaS service.*

*The application for PaaS is built with different programming languages and tools that can support the current platform, i.e.,Java, Net, etc. This model includes a third party to provide the software to the users.*

### 3) Software as a Service (SaaS)

*This is the third type of cloud computing service. This type of service provides internet based service to their customers worldwide without requiring software installation and without using proper tools. The cloud service provider provides the storage capacity, platform, and software according to the business need, and the user only pays for the service. There is no need for software tools. SAAS service is also called Web-base service, and users can easily access it worldwide. There is no cost for software or developer investment or software licensing. The provider side cost is low. The customer data can be publicly stored in the cloud and easily accessible.*

## 3. Attack Associated with the IaaS Model

*In the IaaS model, maintaining security is a shared responsibility among the cloud providers. The IaaS model acquires the security issues associated with PaaS and SaaS models.The common attacks associated with the IaaS model in public cloud infrastructure are divided into the following six groups.*

*Server-based attacks are:-*

*1) Security thread sourced from host*

*2) Security thread from other Virtual machines*

*3) Denial of service attack*

*4) SLA Monitoring &and enforcing SLA Attack*

*5) On-demand billing system availability*

*6) Attack against XML and attack against web services*

*7) Man in the Middle attack*

*8) Spoofing Attack*

*9) Port Scanning*

*10) DNS security*

### 1) Security Thread Sourced from Host

*This type of security threat is in which computers are connected to other computers via a terminal and controlled computer via a Network. It is like a client-server computer. This type of attack can be done on the network because very computer is connected and chances of an attack are greater in a network.*

#### • Solution for Security Thread from Host

***i) Network Monitor***
*A network monitor can be used to view, capture and analyse network traffic in every single packet. This tool is also used to find out network problems and troubleshooting issues. Network traffic can be used to capture every session of every client in the network.*

***ii) Advance IP Scanner***
*IP scanner is a fast and easy way to scan the devices in the network. If any device is connected, like a phone, modem, USB device, etc, it alerts automatically. It offers common services like FTP, HTTP, and sharing folders on network machines, which can be scanned from time to time.*

### 2) Security Thread from Other Virtual Machines

*The virtual machine is a guest system, a host system within a virtual infrastructure. A guest operating system is installed virtually under the host operating system. If the other virtual machines are interconnected, a masquerading attack can easily done and gain secret information in the Virtual machines.*

#### • Solution for Security Thread from Virtual Machines

***i) Two Physical Networks***

• ***Data Network :*** *Monitor the Virtual Machine traffic. Physical Network is optional. We can connect all Virtual machines to the bridge network and monitor the virtual machines.*

• ***Manage Network :*** *Manage the network properly and send data from trusted persons to other virtual machines.*

***ii) Two Physical Host***

• ***Host1 :*** *Host1 is used to open its switch and two Network Interface cards:*

*The 1st NIC is connected to a data Network in which no IP can be assigned. The 2nd NIC is connected to manage the network and monitor IP traffic.*

• ***Monitoring Host :*** *It is a single Network interface card, one side connected to the management network and the other side used for host1.We can also monitor it with a unique ID.*

### 3) Denial of Service Attack

*A denial of service attack can be attempted when the attacker wants the machine and resources of the network to be unavailable to the users and disconnect the users' connection from the servers. This type of attack can be attempted on target websites, and high-load servers like bank transactions, ATM transactions, etc, are used by criminals to attempt this type of attack.*

#### • Solution for Denial of Service Attack

***i)*** *Dos attack can be detected by using traffic block tools in which they respond that caneasily detect unauthorized and authorized users.*

***ii)*** *Firewalls are used to detect to allow or deny the traffic to accessing IP and port number. If an unauthorized IP address comes, they drop all unauthorized traffic coming from hackers.*

***iii)*** *Automatic filtering mechanism detects IP filtering and WAN failure over and balancing mechanism.*

### 4) SLA Monitoring & Enforcing SLA Attack

*SLA is basically an agreement between two parties: the client and the service provider. The agreement may be between single organizations or different teams within a single organization. An internal client department in an organization can attempt this type of attack. Within an organization, if the hacker can access the customer agreement and find out the secret information from the websites, then an SLA attack can occur.*

### 5) Solution for SLA attacks (Monitoring)

*The best solution for SLA is monitoring the websites from time to time. It can show the performance matrices and alert which customer is logged in and which is logged out. It can also show the different sessions of the users and also provide the detailed blocking person who can attempt any fault when uploading and downloading in the cloud. Then, we can easily disconnect the session.*

### 6) Attack Against XML & Attack against Web Services

*XML type of attack is an attempt when the attacker wants to inject various XML tags into a SOAP (simple object access protocol) to exchange messages on the internet and modify asXML structure. XML type is mostly an attempt at restricted operation. Such modification of payment data and unauthorized admin who violated website security objectives. The attacker must know the endpoint of websites, and they find out the endpoint of the location where metadata is saved, which only knows the users.*

- **Solution for XML attack & Attack against Websites**

*The proper method for XML prevention is managing and monitoring the user when they reach the programming code. XML injection must be prevented by simply removing the single and double quotes from user input, which is a very efficient method. Many problems can occur if we cannot monitor the user. If any invalid user comes, we can easily block it, disconnect it, and kill the connection. The system should recognise the users and provide proper functions and syntax from the XML library.XML signature is also used for transactions in cloud security. It provides authentication, data integrity and support data for sign-in. An XML signature can sign in more than one type of resource. An XML signature covers encoded data, and JPG encoded data are the section of an XML file.*

### 7) Man in the Middle Attack

*This type of attack can be attempted by a hacker, who secretly obtains the information between two parties, and the parties are directly connected. This is also like a Chess Game in which hackers can know how to play the Game. It is used against many cryptographic protocols like eavesdropping, in which the hacker shows him an authorized person and communicates with the other party, believing that they are private communication.*

*When a hacker party ranges within an unencrypted Wi-Fi access point, this type of attack can put themselves as a man-in-the-middle.*

- **Solution for Man in the Middle Attack**

*Logical segmentation is used to help manage network communication and support network flows. Segmentation is a key for the Industrial automation control system network (IACS). When designing IACS, one side is 0to 2.*

### 8) Spoofing Attack

*The spoofing attack can occur when the user can connect to the network, and a hacker launches an attack on the network hosts, steals information, launches malware and controls the network. The attacker sent a False IP to connect to the network, overloading the network with multiple IP flooding addresses. ARP and DNS spoofing attack may be part of spoofing attacks.*

***i) ARP Spoofing Attack***

*The Arp spoofing attack can be attempted when the hacker sends a spoof packer IP to the local area network to link with the MAC address of the user in a network when connect to the network, and ARP spoofing attacks steal secret information.*

***ii) DNS Spoofing Attack***

*A DNS spoofing attack can happen when a hacker modifies its own server and reroutes the domain names for different IP addresses. When a user accesses an IP from a DNS server, it gives an IP, then it is controlled by the hacker, who tries to access the information and spreads viruses and malware in the system.*

**• Solution for the Spoofing, ARP & DNS Attacks**

*Spoofing attacks can be eliminated by following the rules in which networking is protected from hackers. Several steps can be followed to ensure network communication is secure.*

***i)*** *When exchanging the key between two parties, use an authentication-based mechanism*

***ii)*** *We use an access list and private addresses to secure communication.*

***iii)*** *Designing a Filtering mechanism for both sides of traffic where traffic can be in and out.*

***iv)*** *Configure your switches and routers manually; if any outside packets come it rejects them from the local area network*

***v)*** *Using an encryption session for a trusted host on your network in which the session will be securely communicated.*

**9) Port Scanning Attack**

*The port scanning is like a door in your system. Many packets can come in and out from the door. They use the different protocols on the network, e.g. UDP and TCP protocol for communication. There are 65536 different ports in the system. For example, Mail servers are using TCP port 25. When the hacker attempts an attack, they want to find out which port is open in your system. Attackers send packets and check regularly for open ports and find out which service is running on your system. Mostly, firewalls minimize the services and worry you.*

**• Solution for Port Scanning Attack**

*These types of attacks can be avoided by the use of good firewalls, and an Intrusion prevention system (IPS) mechanism is used for Port scanning. Port 80 is visible to the entire world, but it approaches limited organization. The IPS detects port scanning and shut down before them, showing a full map of the network. In Unix/Linux systems there is only a limited port is open, and port 1521 scans all TCP and UDP scans in which Solaris system is able to detect TCP vanilla and UDP scans. TCP wrapper is also used for port scanning purposes and providing administrator flexibility to permit or deny allowing services. TCP wrapper regularly checks to see the IP and authorized port. If no entry is found, it ignores the request and does not allow any Service to be utilized. It deals only with unauthorized hosts and does not allow permitting connections.*

**10) DNS Security**

*A DNS security attack is also called a cache poisoning attack. This type of attack can be attempted by hackers sending requests to spiteful websites. The attacker is successful in injecting spiteful DNS data into recursive DNS servers, which can be operating many ISPs. It is closest to the network users and damages the localization of the users which is connected to those servers. It can also happen when hackers take over one or more reliable DNS server domains. They also attempt when hackers register for the domain itself, and the network user can access the altered DNS servers which are assigned to the user.*

**• Solution for Security Attack**

*Use a private and protected resolver, which is restricted to the users on your network, and help find the cache poisoning attack outside of an organization. Measurement Factory's online tool is*

*used as a DNS solver. Another Approach is adding variables for outgoing requests, which can be harder for hackers. If we follow the steps for security attacks:*

***i)*** *We use a random port instead of a UDP port for communication*

***ii)*** *Used different types of query ID Another Approach is used intrusion prevention system (IPS) and intrusion detection and prevention systems (IDPS) monitoring the networks and protecting unreliable activities. IPS also take place in the action of alarms and dropping packets as well as restarting the connection and blocking outside traffic.*

## 4. Attack Associated with the PaaS Model

*In the PaaS model, one can develop, manage and execute requests offered under the IaaS model, it is complex due to the lack of tools that enable the creation of applications. The common attacks associated with the PaaS model in public cloud infrastructure are divided into the following five groups.*

*1) Denial of Service Attack*

*2) Cloud Malware Injection Attack*

*3) Side Channel Attack*

*4) Authentication Attack*

*5) Man in the Middle Attack*

### 1) Denial of Service Attack

*A denial of service attack can be attempted when the attacker wants the machine and resources of the network to be unavailable to the users and disconnect the connection of the users from the servers. This type of attack can be attempted on target websites, and high-load servers like bank transactions, ATM transactions, etc, are used by criminals to attempt this type of attack.*

### • Solution for Denial of Service Attack

***i)****Dos attack can be detected by using traffic block tools in which they respond that can easily detect unauthorized and authorized users.*

***ii)*** *Firewalls are used to detect to allow or deny the traffic to accessing IP and port number. If an unauthorized IP address comes, they drop all unauthorized traffic coming from hackers.*

***iii)*** *Automatic filtering mechanism detects IP filtering and WAN failure over and balancing mechanism.*

*To avoid this type of attack, we introduce the File Allocation system FAT, which is a straightforward technique which supports all operating systems. The FAT table can fetch all customers in the cloud who are using cloud services and also check old requests which are already executed. For this purpose, a hypervisor is installed at the provider's end. It must secure communication and check all integrity from the FAT table to the user's Virtual Machine. The hypervisor machine works line host machine and monitors all the clients of the cloud.*

### 3) Side Channel Attack

*This type of attack is mostly in the PaaS cloud, which targets the server machine. It is the most effective thread of security that designs cryptographic algorithms. It can watch and monitor the CPU and memory, how to take executed, and try to find out some secret key. Side Channel Attack can be done if the cloud users utilise spiteful activity from Virtual machine requests.*

### • Solution for Side-Channel Attack

*There are different methods by which side-channel attacks can be secure by using Virtual Firewall and random encryption and decryption techniques.*

***i) Virtual Firewall***

*In a virtual firewall, it works like when any request can be from a user or attacker it identifies first by using authentication techniques and places a request Virtual Machine to target machine which can stop sharing confidential information. The side channel attack can be prevented inside a firewall.*

***ii) Random Encryption Decryption Techniques***

*Nowadays cloud computing is involved in all business applications, office organizations, medical stores and banks, but they need secure information security. It encrypts the plain text to cipher text by using different keys and making it as complex as possible, which is harder to detect.*

*By random encryption and decryption documents and important secret files can been crypted by encryption algorithms like Data Encryption Standard (DES), 3 DES and Advance Encryption Standard are used for converting the information to more complex. It takes user data converting every time and it is complicated for the attacker and harder to find out information.*

**4) Authentication Attack**

*This type of attack can happen. They target to exploit the authentication process a website uses to verify the identity of the client's Service and Running applications. The authentication process is mostly secure in the IaaS cloud but mostly in secure in PaaS and SaaS. If the transmitted data is highly confidential, then the IaaS security mechanism is best for secure communication.*

*The attempt several types of attacks can be attempted based on authentication attacks:*

*i) Brute force Attack*

*ii) Insufficient Authentication*

*iii) Weak Password*

*A brute force attack can be an attempt that allows the hacker to guess the user name, password and credit card numbers and allow some transactions. Insufficient Authentication can be an attempt to access the websites and find sensitive information from the websites. Hackers can attempt Weak Passwords, and they can change, alter and use password recovery mechanisms from websites.*

**• Solution for the Authentication Attack**

*Authentication Attacks can be prevented by using knowledge-based authentication by using site keys, keyboards and sharing secret questions, making it too difficult to attempt this type of attack. By adding random content on the page for all clients who can access the websites. This mechanism is impossible to succeed for hackers.*

**5) Man in the Middle Attack**

*This type of attack can be attempting an attacker place himself in between two parties. The attacker can easily alter and modify the combination. This attack can happen when two parties are communicating and the attacker comes in when the 1st party share the key with the 2nd party the hacker can replace the 1st party key with his own key and send it back to the1st party and the first party think it is a 2nd party key, then it synchronization with it, and secret information will be spread out.*

**• Solution for Man in the Middle Attack**

*The solution for this attack is using the Cryptographic tool Hash functions. It is stronger for public and private keyen cryption, and security sent data from one party to another. The secret sharing keys between two parties can reduce this type of attack. Using an authentication process to check valid users of the cloud is a very effective process. By using a random encryption mechanism when sending data over the network.*

**5. Attack associated with SaaS Model**

*In the SaaS model, maintaining security is the responsibility of the service and cloud provider. The*

*common attacks associated with the SaaS model in public cloud infrastructure are divided into the following six groups.*

*1) Denial of Service Attack*

*2) Account Lockout*

*3) Access Control Weakness*

*4) Session Hijacking*

*5) Authentication weakness*

### 1) Denial of Service Attack

*A denial of service attack can be attempted when the attacker wants the machine and resources of the network to be unavailable to the users and disconnect the connection of the users from the servers. This type of attack can be attempted on target websites, and high-load servers like bank transactions, ATM transactions, etc, are used by criminals to attempt this type of attack.*

#### • Solution for Denial of Service Attack

*i) Dos attack can be detected by using traffic block tools in which they respond that can easily detect unauthorized and authorized users.*

*ii) Firewalls are used to detect to allow or deny the traffic to accessing IP and port number. If an unauthorized IP address comes, they drop all unauthorized traffic coming from hackers.*

*iii) An automatic filtering mechanism is used to detect IP filtering and also detect WAN failure over and balancing mechanism.*

### 2) Account Lockout

*This type of attack can be attempted by using an authentication process that fails many times and triggers. It can be used for valid clients and access the account information. If a hacker attempts three times login, it can lock out a user's account and launch a denial of service on many client accounts.*

*If we implement an account lockout policy, there is a risk of mistake locking authorized user accounts. This attack can mostly happen when authorized users can mistype and enter the wrong password. The computer wants to authorize it with an incorrect password and tries to authenticate it, but the user account will be locked after too many tries.*

#### • Solution for Account Lockout

*By using an account security mechanism Microsoft company introduced different types of securities like Low security, Medium security and High security.*

*The use of low security in account lockout duration cannot be defined, and resetting the account lock out counter after is also not defined. By using a medium security mechanism in which the account lockout duration is 30 minutes and reset account counter after=30 minute*

*Similarly, by the use of a high-security mechanism in which the lockout duration is zero and reset account lockout counter=30 minutes, The possible defence against this attack is a loose account policy and using strong passwords, including upper case characters. Numbers and special characters.*

### 3) Access Control Weakness

*Access control weakness is the weak point in SaaS, which is responsible for making decisions and allows permitting the request of the user. If any unauthorized user can access it, then it creates a problem for the cloud as well as data may be infected. These types of attacks basically attempt on web services. The attack is network intrusion and infected data and applications, too. This attack can also be attempted when unauthorized code can be running.*

**• Solution for the Access Control Weakness**

*Access control can be prevented by Microsoft companies. Microsoft allows customer to all to access the data from multiple organizations within a cloud. The ABAC service is used for access control, which can manage the network, and is specially designed for cloud environment communication. The third party are designed for access control for specific services only but is not deployed for all applications for SaaS, PaaS and IaaS because of certain weak points. Ping Identity access control solution is used for the access control mechanism.*

**4) Session Hijacking Attack:**

*Session attacks can be attempted on the web session control mechanism, which is managing tokens. The session tokens can be composed of a string of variables and used indifferent ways. Session hijacking is an attempt to steal valid session tokens to access unauthorized access to the server cloud. In this type of session, tokens could be attempted in different ways. For example, a man-in-middle attack session sniffing, client-side attacks, a man-in-the-middle attack, a man-in-the-browser attack, and cross-site attacks may be included in the session Hijacking attack.*

**• Solution for Session Hijacking Attack:**

*The best solution for a session hijacking attack is to Trace the session in which they identify the sequence number of packets in it. When any illegal activity happens, it desynchronizes the connection. TCP can reset it and finish the packet and its session. There are three methods for session Hijacking attacks:*

*1)Session calculation*

*2) Session Capture*

*3) Session Fixation*

*In session calculation random number of string are used and reduce the risk of attacks In session capture, data can be transmitted between two parties by a particular session key, and sniffing attacks can be prevented. The Session Fixation is used to identify every session, and the process is called session identifier, accept form URLs and tells the session information.*

**5) Authentication weakness**

*It is a weak point, and hackers mostly target this attack. If we talk about SaaS, PaaS and IaaS architecture models, only IaaS provides this protection and data encryption method. Weak passwords are significant authentication, and if possible, password rules are used for every system on the network and Borden on the network. A weak password can be easily guessed.*

**• Solution for Authentication weakness**

*Password and authentication processes cannot protect your data, but the use of access requests either accept or deny. Authentication bypass attacks, but almost all are avoided in this cloud.*

## 6. Conclusion

In this paper, we identify the attacks of cloud computing services, i.e. IaaS, PaaS and SaaS models and show that security testing can be challenges are met.

They show several security issues and how specific processes can solve them. Security is related to protecting our information and must have issues of availability. SaaS and PaaS services are not secure, but IaaS provides the best infrastructure for cloud data.

## References

[1] Josyula, V., Orr, M., Page, G. (2011). Cloud Computing: Automating the Virtualized Data Center. *Cisco Systems, Inc., Indianapolis*, USA.

[2] Liu, F., et al. (2011). NIST Cloud Computing Reference Architecture. *National Institute of*

*Standards and Technology, U.S Department of Commerce*, Special Publication 500-292.

[3] CCRA Team., Buzetti, M. (2011). Cloud Computing Reference Architecture 2.0: Overview. *IBM Corporation.*

[4] Hanna, A., Rance, S. (2011). *ITIL® - ITIL Glossaries*. Retrieved from itil-officialsite.com

[5] Oxford Consulting. (2012, December). *The Importance of IT Service Management*. Retrieved from http://info.oxfordconsulting.com/blog/bid/138721/The-importance-of-IT-service-management

[6] Orea, J., et al. (2011). Quick guide to the reference architecture: Trusted Cloud Initiative. *Cloud Security Alliance.*

[7] Takabi, H., Joshi, J. *Security and Privacy Challenges in Cloud Computing Environments*. Retrieved from http://www.sis.pitt.edu/~jjoshi/courses/IS2620/Spring13/S&P.pdf

[8] Hurwitz, J., et al. *Understanding IT Governance in Cloud Computing*. Retrieved from http://www.dummies.com/howto/content/understanding-it-governance-in-cloud-computing

[9] DeCarlo, A. L. *Cloud Service Management and Cloud Monitoring for providers: A primer*. Retrieved from http://searchcloudprovider.techtarget.com/feature/Cloud-service-management-and-cloud-monitoring-for-providers-

[10] Oracle. (2012, November). *Cloud Reference Architecture*. Retrieved from http://www.oracle.com/technetwork/topics/entarch/oracle-wp-cloud-ref-arch-1883533.pdf

[11] Lindquist, D., et al. (2007). IBM Service Management architecture. *IBM Systems Journal*, 46(3).

[12] Plummer, D. C., Kennedy, L. F. (2009, November). Three types of cloud brokerages will enhance cloud service. *Gartner Special Report on Cloud Computing*.

[13] Cloud Security Alliance. (2012). *TCI Reference Architecture Model*. Retrieved from https://cloudsecurityalliance.org/download/tci-reference-architecture-v2-

DLINE JOURNALS

Journal of Information Security Research

Print ISSN: 0976-4143
Online ISSN: 0976-4151

JISR 2024; 15 (1)
https://doi.org/10.6025/jisr/2024/15/1/11-22

# Enterprise Risk Assessment of Agricultural Supply Chain Based on CRITIC- Entropy Weight -VIKOR Model

Xiaodong Lou
College of Digital Commerce
Zhejiang Business Technology Institute
315012, Ningbo Zhejiang, P. R. China
{10820015@zbti.edu.cn}

**ABSTRACT**

*Agriculture is the primary industry which plays a foundational role in our national economy. It is the most essential material production department. Agricultural supply chain management can ensure the safety of food production, protect the rights and interests of consumers, improve the operational efficiency of the agricultural supply chain, and increase the income of agricultural enterprises and farmers. Therefore, the key link of agricultural supply chain risk management is identifying and evaluating the risk. To improve the scientific merit and accuracy of enterprise risk assessment in the agricultural supply chain, this study constructed a risk assessment model integrating CRITIC, entropy weight and VIKOR method. It proposed five first-level indexes, including policy environment risk, market environment risk, policy adjustment risk, consumer demand change risk and natural change risk. Based on the index system, composed of 17 secondary indexes, the risk index weights of agricultural supply chain enterprises were determined jointly by the CRITIC and entropy weight methods. VIKOR method was used to carry out a risk assessment on 15 agricultural supply chain enterprises in an agricultural economic development zone. The results show that the evaluation index system of enterprise risk of agricultural supply chain proposed in this study is more scientific and reasonable. The CRITIC indicators of X-1-1, X-5-1, and X-5-2 have the largest weight. The entropy weight of X-5-1, X-5-2 and X-1-2 is the largest. The critical-entropy weight-VIKOR model can effectively distinguish the risk degree of different agricultural supply chain enterprises and provide decision support for enterprises to formulate targeted risk management countermeasures. The research results of this study are of great value for the scientific and accurate risk assessment of enterprises in the high agricultural supply chain, improving the effectiveness of risk management, enriching the methods and tools of risk assessment research in the agricultural supply chain, and realizing the safe and stable operation of the agricultural supply chain.*

**Received: 4 September 2023**
**Revised: 4 December 2023**
**Accepted: 22 December 2023**


**Keywords:** CRITIC, Entropy Weight, VIKOR, Agricultural Supply Chain, Enterprise Risk, Risk Assessment

## 1. Introduction

*With the development of the social economy, people's demand and quality requirements for agricultural products continue to increase. However, due to the cyclical, regional and natural constraints of agricultural production, the supply of agricultural products will often fluctuate. A complete supply chain of agricultural products must be established to meet the market demand. The supply chain of agricultural products covers the production, acquisition, processing, storage, transportation and sales of agricultural products. Compared with the supply chain of industrial products, the supply chain of agricultural products is more affected by external factors such as the natural environment, policies, regulations and social environment, and there are many uncertainties and high risks. Identifying and controlling various risk factors in the supply chain of agricultural products is very important to ensure the safe and efficient operation of agricultural products. The agricultural supply chain refers to the whole process from agricultural production, agricultural product processing, storage and transportation, sales and after-sales service. In this process, various risk factors are involved, such as natural risk, market risk, policy risk, technical risk and so on. These risk factors affect different links in the agricultural supply chain, making problems in the operation process easy. For example, in agricultural production, natural disasters, climate change and other factors may lead to crop failure, thus affecting the stable operation of the agricultural supply chain. In the processing, storage and transportation of agricultural products, technical equipment failure, loss during transportation, etc., may lead to the decline of agricultural product quality, affecting the quality and efficiency of the agricultural supply chain. In the marketing link, market fluctuations, policy changes and other factors may make the price of agricultural products fluctuate, affecting the efficiency of the agricultural supply chain.*

*The agricultural supply chain is one of the foundations of agricultural industrialization and modernization, so improving the overall agricultural supply chain can lay the foundation for agricultural and rural economic development and even rural revitalization. However, there is more serious information asymmetry and interest disharmony among the participants of the agricultural supply chain under the market behaviour. From the external environment, problems such as imperfect credit systems and unbalanced strength of participants in the agricultural economy will further aggravate this information asymmetry and uncoordinated interests. The study of agricultural supply chain risk factors is of great significance for improving the overall competitiveness of the agricultural industry, ensuring national food security and safeguarding the interests of consumers. An in-depth study of agricultural supply chain risk assessment can help related enterprises and decision-making departments identify risks in advance and take effective measures to prevent and control them. This can reduce the supply chain's impact in natural disasters, market changes, etc., to ensure a stable supply of agricultural products. The scientific identification of agricultural supply chain risk factors can provide a basis for agricultural capital subsidies, industrial support, and fiscal and tax policies and help formulate feasible policies and measures to promote agriculture's sustainable and healthy development. It also helps agricultural enterprises to identify risk factors in their operations according to the research results, formulate practical and effective coping strategies, and improve their anti-risk ability.*

## 2. Literature Review

*Due to the agricultural supply chain's complexity and uncertainty, enterprises face various risks, such as market risk, credit risk, logistics risk, quality risk and so on. Therefore, it is very necessary to evaluate the risk of agricultural supply chain enterprises. The research on enterprise risk assessment of agricultural supply chains has been widely concerned worldwide. Agricultural supply chain enterprise risk assessment is a complex process requiring various factors and evaluation methods. In terms of supply chain risk assessment, Tran et al. (2018) made a comprehensive analysis of all aspects of supply chain risk assessment in the literature, including the definition of heterogeneity, focus, procedures, methods and indexes of supply chain risk assessment mentioned in previous studies, and prospected future studies. Aqlan & Lam (2015) proposed a comprehensive framework for supply chain risk assessment, consisting of three main components: investigation, bow analysis, and fuzzy reasoning system. The results showed that such an analytical framework could be used to evaluate supply chain risk effectively.*

*According to Jaffee et al. (2010), the main influencing factors of agricultural supply chain risk included unpredictable weather, unpredictability of biological processes, obvious seasonality of production and market cycle, uncertain political economy, etc. They provided a conceptual framework*

*for system-wide assessment and a set of detailed guidelines for agricultural internal risk, risk management and vulnerability assessment supply chains. Bloemh of et al. (2015) proposed a quantitative risk assessment method, which integrated three steps of risk identification, estimation and evaluation. The method was applied to the meat supply chain, taking into account risks in terms of animal welfare and food safety. The research showed that quantitative models could effectively assess the risks of complex agricultural supply chains. Leat & Revoredo Giha (2013) constructed a dynamic stochastic general equilibrium model to simulate the risks and uncertainties agricultural supply chains face. The model considered random factors such as productivity, demand and price fluctuations. The results showed that different types of agricultural enterprises had different risk tolerance. Banterle & Stranieri (2008) used the editable analytic hierarchy process (AHP) to assess the risks of the Italian agricultural supply chain, including production, storage, processing and distribution links. Policy and market factors were the main risk factors in this supply chain, and this approach supported the development of risk management strategies. Dong& Stranieri (2016) developed an ex-ante supply chain risk assessment model based on order of magnitude AHP (OM-AHP) to compare tangible and intangible factors affecting supply chain risk and provided an example to prove the effectiveness of the proposed risk assessment framework. Ganguly & Kumar (2019) provided a method based on a fuzzy analytic hierarchy process (FuzzyAHP) to assess supply chain risks, identifying 16 risk factors. The results showed that this method can effectively identify supply chain risks. Nakandala et al. (2017) proposed a hybrid model that includes fuzzy logic (FL) and hierarchical holographic modelling (HHM) techniques, and a case study of a fresh food supply chain company showed that this novel approach took advantage of the advantages of both techniques. Jiang et al. (2018) showed that port service process risk, operation risk, port relationship process risk and external environment-related risk were too high in the supply chain. Ghadge et al. (2017) used data triangulation to collect and analyze data through interviews, questionnaires, expert opinions, and quantitative modelling, and the findings suggested that managers should conduct robust risk assessments at the design stage to avoid product safety and security risks. Jaberidoost et al. (2015) used AHP and rating scales to conduct questionnaire surveys and expert consultations for risk analysis and used simple additive weighting methods for risk assessment to identify 86 major risks in the drug supply chain, which were divided into 11 categories. Liu et al. (2022) identified risk factors in intelligent supply chain, adopted hierarchical cluster analysis, and proposed an improved risk assessment model containing 22 risk factors. Chaudhuri et al. (2013) proposed a step-by-step approach to supply chain risk assessment in the new product development process, including group decision-making. The results showed that by using this approach, organizations could develop control plans to mitigate vendor-related risks during new product development. Vishwakarma et al. (2016) proposed a multi-criteria decision-making method based on fuzzy analytic Hierarchy Process (AHP). They identified 24 kinds of risks under five risk measures in the Indian drug supply chain. The result analysis showed that supply and supplier risk were the most important risks in the Indian drug supply chain.*

*Junaid et al. (2019) proposed a comprehensive supply chain risk management method, which combined the analytic hierarchy process (AHP) and ideal solution similarity ranking technology. The research showed supply chain elasticity is the most important standard for managing supply chain risk. Tummala & Schoenherr(2011) showed that applying the supply chain risk management process (SCRMP) can effectively manage supply chain risk. Diaz-Curbelo et al. (2020) found that integrated and destructive analytical methods with multi-criteria decision-making were the most common type and tended towards Petri nets and multi-criteria decision-making methods. Supply risk was the most studied type in supply chain risk management, and identification and evaluation are the most developed processes. Sreedharan et al. (2019) found that supplier, production, demand, infrastructure, and macro risks were the sources of supply chain risk in the pharmaceutical industry. Tuncel & Alpan's (2010) findings indicate that system performance can be enhanced through risk management measures, and overall system costs can be reduced through mitigation measures. Ritchie et al. (2008) believed risk structure should be included in measuring organizational performance. Radivojevic & Gajoviæ (2014) described the main features of the supply chain and established a risk assessment model based on AHP and fuzzy AHP. The results showed that AHP and FAHP could be used to rank supply chain risk categories, determine their share in the total risk, and as a supply chain risk assessment method. It can be seen from the existing research literature that the research of supply chain risk evaluation arose in the 1990s, and the research of supply chain risk evaluation mainly focuses on three aspects: risk identification, risk assessment method and risk control strategy.*

*The study determined the supply chain risk dimensions and specific risk factors in the risk identification. In terms of evaluation methods, both qualitative and quantitative evaluation methods are paid equal attention, and simulation evaluation based on system dynamics appears. In terms of risk control strategy, strengthening supply chain cooperation, improving supply chain transparency and using information technology are effective countermeasures. Overall, the supply chain risk assessment research framework has initially taken shape, but the model-building and management countermeasures still need further exploration. Future research can be expanded in case verification and risk control optimization. Therefore, the critical-entropy weight-VIKOR model is proposed in this study, aiming to further optimize the index weight of agricultural supply chain risk and carry out a more scientific and objective evaluation of agricultural supply chain enterprises. The traditional subjective weighting method has the randomness of determining weights, but the entropy weighting method is too absolute and does not consider the correlation between indexes. Therefore, the critical-entropy weigh-VIKOR model is proposed in this study, aiming at further optimizing the determination of index weight of agricultural supply chain risk and carrying out a more scientific and objective evaluation for agricultural supply chain enterprises, which can effectively distinguish the risk degree of agricultural supply chain enterprises and provide decision support for agricultural supply chain enterprises to formulate differentiated risk management strategies.*

## 3. Methodology

### 3.1. Model Introduction

#### (1) Combination Weight Determination

*Firstly, it calculates weight using the CRITIC (Criteria Importance through Intercriteria Correlation) empowerment method. CRITIC method is an indicator weight determination method based on indicator correlation and is an objective weighting method proposed by Diakoulaki et al. (1995). In the comprehensive analysis of multi-index evaluation objects, this method takes into the consideration of conflict between each evaluation index and the change of index weight caused by the change of measured value. With* $n$ *evaluation indexes and* $m$ *and measured data, matrix* $A = [a_{ij}]_{mxn}$ *is established, where* $a_{ij}$ *represents the value of the* $j^{th}$ *index of the ITH scheme. In Toiminate the difference between different indexes, the benefit indexes are treated positively. The cost index is reverse-processed. The normalized matrix* $B = [b_{ij}]_{mxn}$ *is obtained. The correlation coefficient matrix* $R = [r_{ij}]_{mxn}$ *is calculated, where* $r_{ij}$ *is the Pearson correlation coefficient between the* $i^{th}$ *index and the* $j^{th}$ *index, and its calculation formula is shown in Eq. (1).*

$$r_{ij} = \frac{\sum_{k=1}^{n} (b_{ik} - \bar{b}_i)(b_{jk} - \bar{b}_j)}{\sqrt{\sum_{k=1}^{n} (b_{ik} - \bar{b}_i)^2} \times \sqrt{\sum_{k=1}^{n} (b_{ik} - \bar{b}_i)^2}} \quad (1)$$

*In formula (1),* $\bar{b}_i$ *and* $\bar{b}_j$ *represent the mean of index i and index j in matrix B, respectively. Then, the Gini coefficient is calculated by Eq. (2).*

$$\gamma_j = \frac{\sum_{i=1}^{m} \sum_{k=1}^{m} |b_{ij} - b_{kj}|}{2m \sum_{i=1}^{m} b_{ij}} \quad (2)$$

*In formula (2),* $\gamma_j \in [0,1]$ *and j are closer to 1, indicating that the information distribution of indicator j is more unbalanced, the greater the amount of information. The closer to 0 is, the more balanced the information distribution of index j and the smaller the amount of information. Then, the information coefficient* $g_j$ *is calculated. To ensure the correctness of the final result, the absolute value of the Pearson correlation coefficient was used to calculate the information coefficient. The calculation is shown in Eq. (3).*

$$g_j = \sum_{j=1}^{n} (1-|r_{ij}|) \tag{3}$$

*The comprehensive information amount $G_j$ of indexes is calculated, and the weight $\omega_j$ is determined. The greater the $G_j$, the greater the amount of information in the j index, and the greater the corresponding weight. The calculation is shown in Eq. (4).*

$$g_j = \gamma_j \cdot g_j,\ \omega_j = \frac{G_j}{\sum_{i=1}^{n} G_j} \tag{4}$$

*Then, the entropy weight model is used to further calculate the weight. Zeleny (1998) systematically proposed the concept of entropy weight method for the first time and gave a specific calculation method. He uses the concept of information entropy to determine the weight of each evaluation index according to its universality and recognition. In the entropy weight model, the information entropy $E_j$ of the horizontal $j^{th}$ index.*

$$E_j = -K \sum_{j=1}^{n} P_{ij}\, ln\,(P_{ij}) \tag{5}$$

*Among them, $K = \frac{1}{\ln n}$, $0 \le E_j \le 1$. Then, continue to calculate the difference coefficient $d_j$, as shown in Eq. (6).*

$$d_j = 1 - E_j \tag{6}$$

*Then, the weights of each measurement index are determined, as shown in Eq. (7).*

$$W_j = \frac{d_j}{\sum_{j=1}^{m} d_j} \tag{7}$$

*According to Eqs. (4) and (7), the weights calculated by CRITIC method and entropy weight method are combined and weighted, as shown in Eq. (8).*

$$Y_j = (G_j + W_j) / 2 \tag{8}$$

**(2) Risk Assessment**

*The VIKOR method was proposed by Opricovic & Tzeng (2004). VIKOR method is a multi-criteria decision analysis method. The multi-attribute decision scheme is sorted and selected by calculating group utility, individual regret, and compromise values the basic idea is that the optimal solution and the worst solution are determined in the set of all feasible solutions. Then, a comprehensive evaluation is carried out according to the degree of proximity between each solution and the optimal solution and the degree of distance between the worst solution; that is, the closer the optimal solution is and the more distant the worst solution is. In this process, it is often necessary to make compromises among decision attributes to obtain a feasible solution that considers maximizing group utility and minimizing individual loss. The specific steps are as follows: the matrix $A = [a_{ij}]_{mxn}$*

$$X = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{bmatrix} \tag{9}$$

*is weighted. The combined weight $Y_j$ is obtained using the formula (8).The weighted matrix X is obtained as shown in Eq. (9).*

*Then, positive ideal solutions $x^+_j$ and negative ideal solutions $x^-_j$ for each index are determined, as shown in Eq. (10).*

$$x^+_j = \{max\, x_{1j}, max\, x_{2j}, ..., max\, x_{nj}\}\ (j = 1, 2, ..., m)$$
$$x^+_j = \{min\, x_{1j}, min\, x_{2j}, ..., min\, x_{nj}\}\ (j = 1, 2, ..., n) \quad (10)$$

*When the positive ideal solution is taken as a reference, the group utility value and individual regret value of each scheme are shown in Eq. (11).*

$$S^+_j = \sum_{i=1}^{m} w_i (x^+_t - x_{ij}) / (x^+_t - x^-_t)$$
$$R^+_j = max\, [w_i (x_{ij} - x^-_t) / (x^+_t - x^-_t)] \quad (11)$$

*When the negative ideal solution is taken as a reference, the group utility value and individual regret value of each scheme are shown in Eq. (12).*

$$S^-_j = \sum_{i=1}^{m} w_i (x_{ij} - x^-_i) / (x^+_t - x^-_i)$$
$$R+_j = max\, (w_i (x_{ij} - x^-_i) / (x^+_i - x^-_i)) \quad (12)$$

*Finally, the compromise value $Q_i$ of each scheme is calculated, as shown in Eq. (13).*

$$S^+ = min_i \{S_i\},\quad S^- = max_i \{S_i\}$$
$$R^+ = min_i \{R_i\},\quad R^- = max_i \{R_i\} \quad (13)$$
$$Q_i = \mu \frac{S_i - S^-}{S^+ - S^-} + (1-\mu) \frac{R_i - R^-}{R^+ - R^-}$$

*In Eq. (13), $\mu$ represents the compromise coefficient, also known as decision mechanism coefficient, and represents the proportion of group utility. Its general value is 0.5, which is also adopted in this study.*

### 3.2. Data Source

*By expanding the reading of relevant literature on enterprise risk of agricultural supply chain, this study sorted out and understood the current research status and main influencing factors of enterprise risk of agricultural supply chain, and preliminarily determined the risk assessment framework. Then, 8 experts in enterprise risk assessment of agricultural supply chain were consulted, and the indexes of influencing factors were collected through interviews and questionnaires. Then, according to the data and suggestions provided by 8 experts, combined with the results of literature research, the index system was optimized and integrated by brainstorming method. Finally, experts were invited again to comment on the optimized index system, and finally, a consensus was formed. This study finally put forward a two-level, multi-classification index system of agricultural supply chain enterprise risk, which consists of five indexes: policy environment risk, market environment risk, policy adjustment risk, consumer demand change risk and natural change risk, and 17 secondary indexes. The specific index system of enterprise risk influencing factors of the agricultural supply chain is shown as follows(Table 1).*

| Primary index | Secondary index | Index number |
|---|---|---|
| Policy environment risk | Policy adjustment risk | X-1-1 |
| | Risk of changes in government subsidies | X-1-2 |
| | Trade barrier risk | X-1-3 |
| Market environment risk | Market supply and demand changes risk | X-2-1 |
| | Price fluctuation risk | X-2-2 |
| | Risk of changes in consumer demand | X-2-3 |
| | Import policy change | X-3-1 |
| Policy adjustment risk | Export policy adjustment | X-3-2 |
| | Industrial policy | X-3-3 |
| | Change of consumption concept | X-4-1 |
| Risk of changes in consumer demand | Improvement of consumption level | X-4-2 |
| | Change in consumption preference | X-4-3 |
| | Increase in extreme weather | X-5-1 |
| | Agricultural season getting longer | X-5-2 |
| Natural variation risk | Resource supply risk | X-5-3 |
| | Climate change risk | X-5-4 |
| | Disaster risk | X-5-5 |

**Table 1. Index system of enterprise risk influencing factors in agricultural supply chain**

*After establishing the enterprise risk factor index system of agricultural supply chain, we invited 8 experts in the field of agricultural supply chain enterprise risk assessment to conduct risk assessment on 15 representative agricultural supply chain enterprises in the agricultural economic development zone of a city in Shandong Province. According to the constructed index system, each expert needs to consider the effect of various influencing factors on the risk of enterprises and use the scoring method of 1-10 points to score 15 enterprises. To make the scoring results more fair and representative, each expert must fully understand the indicator system and scoring criteria before scoring and evaluate and score according to the operation and management data provided by the enterprise. After the score, the study collects the score table submitted by the experts. Firstly, it removes one of the highest and one of the lowest scores, calculates the average score of 15 companies, and finally gets the original data set.*

## 4. Results

### 4.1. CRITIC Weight

*Index weights of X-1-1, X-5-1 and X-5-2 are the largest, which are 6.76%, 6.75% and 6.57% respectively (Table 2). First of all, it is mainly because there are certain policy controls in the production and circulation of agricultural products, such as the regulation of the proportion of planting area and the price guidance of the sales link. These policies will have a significant impact on the structure of agricultural production and the functioning of supply chains. When the policy is greatly adjusted, policy changes will lead to greater risks in the supply chain. It's because agricultural production and supply chain operation are cyclical and cannot immediately adapt to the new policy requirements. Secondly, the increase in extreme weather affects primary agricultural production more directly. Storms, floods, fog, drought and other extreme weather will seriously hinder the normal growth of crops, resulting in a significant reduction in production. This will not only affect farmers' planting income but also cause the processing and sales enterprises in the entire supply*

| Index number | Index variability | Index conflict | Amount of information | Amount of information |
|---|---|---|---|---|
| X-1-1 | 2.149 | 15.413 | 33.123 | 6.76% |
| X-1-2 | 1.956 | 15.124 | 29.586 | 6.04% |
| X-1-3 | 1.847 | 17.018 | 31.429 | 6.42% |
| X-2-1 | 1.562 | 14.261 | 22.278 | 4.55% |
| X-2-2 | 1.730 | 16.186 | 28.007 | 5.72% |
| X-2-3 | 1.864 | 16.290 | 30.362 | 6.20% |
| X-3-1 | 1.737 | 15.562 | 27.030 | 5.52% |
| X-3-2 | 1.740 | 17.132 | 29.817 | 6.09% |
| X-3-3 | 1.733 | 14.633 | 25.359 | 5.18% |
| X-4-1 | 1.769 | 14.390 | 25.458 | 5.20% |
| X-4-2 | 1.836 | 17.482 | 32.100 | 6.56% |
| X-4-3 | 1.936 | 15.736 | 30.459 | 6.22% |
| X-5-1 | 2.139 | 15.459 | 33.072 | 6.75% |
| X-5-2 | 2.060 | 15.619 | 32.179 | 6.57% |
| X-5-3 | 1.618 | 15.594 | 25.231 | 5.15% |
| X-5-4 | 1.846 | 15.572 | 28.743 | 5.87% |
| X-5-5 | 1.554 | 16.347 | 25.410 | 5.19% |

**Table 2. CRITIC weight results**

*chain to face a shortage of raw materials. Extreme weather can also disrupt certain infrastructure and logistics transport conditions, such as typhoons that cause road disruptions, further impeding the flow of products through the supply chain. These consequences will seriously disrupt the regular operation of the supply chain so that enterprises cannot carry out production and sales according to the scheduled plan. Finally, the longer agricultural season is related to climate change, which has already affected the planting season of traditional agriculture. The uncertain change in the timing of the bearing season also makes it difficult for supply chain enterprises to estimate the quantity of raw material purchased accurately. In general, the longer agricultural season has increased the difficulty of supply chain coordination, and it is impossible to effectively adjust the production and marketing relationship according to the traditional model.*

### 4.2. Entropy Weight

*Entropy weight of X-5-1, X-5-2 and X-1-2 is the largest, which are 8.91%, 8.08% and 7.79% respectively (Table 3). Two of the top three index weights obtained by the entropy weight method (i.e. X-5-1, X-5-2) are consistent with the CRITIC weight method. The X-1-2 weight obtained by entropy weight method ranks third, mainly because, from the perspective of supply chain management theory, changes in government subsidies will have a significant impact on the dynamic balance of agricultural supply chain. Agricultural production is highly dependent on government subsidies, which will not only affect the planting structure and output, but also produce a signal guiding effect on farmers' planting expectations, thus affecting the supply of agricultural products.*

*At the same time, the processing and circulation links will also adjust their procurement scale, capacity layout and production and marketing strategies according to the government's support for agricultural products. It can be said that changes in government subsidies will lead to changes in the cost-benefit structure of the upstream and downstream of the supply chain, impacting the original equilibrium state of the supply chain. This impact stems from the interaction between two major forces, policies and the market, and is amplified through the traction between various links in the supply chain. As a result, the risks associated with changes in government subsidies can be more systemic than other common risks.*

| Item | Information entropy value e | Information utility value d | Weight coefficient *w* |
|---|---|---|---|
| X-1-1 | 0.9729 | 0.0271 | 6.86% |
| X-1-2 | 0.9692 | 0.0308 | 7.79% |
| X-1-3 | 0.9783 | 0.0217 | 5.50% |
| X-2-1 | 0.9851 | 0.0149 | 3.78% |
| X-2-2 | 0.9776 | 0.0224 | 5.68% |
| X-2-3 | 0.9759 | 0.0241 | 6.10% |
| X-3-1 | 0.9817 | 0.0183 | 4.63% |
| X-3-2 | 0.9789 | 0.0211 | 5.34% |
| X-3-3 | 0.9844 | 0.0156 | 3.94% |
| X-4-1 | 0.9796 | 0.0204 | 5.16% |
| X-4-2 | 0.9754 | 0.0246 | 6.22% |
| X-4-3 | 0.9744 | 0.0256 | 6.48% |
| X-5-1 | 0.9648 | 0.0352 | 8.91% |
| X-5-2 | 0.9681 | 0.0319 | 8.08% |
| X-5-3 | 0.9789 | 0.0211 | 5.34% |
| X-5-4 | 0.9746 | 0.0254 | 6.43% |
| X-5-5 | 0.9851 | 0.0149 | 3.77% |

**Table 3. Entropy weight results**

### 4.3. VIKOR Sort

*According to the ranking results of Q value (Table 4), enterprise 14 is the best overall performer, and its S value of 0.2899 and R-value of 0.0539 are the smallest. This shows that Enterprise 14 is close to the optimal level in combating policy environment risk, market environment risk, policy adjustment risk, consumer demand change risk, natural change risk and so on, and can be used as a model enterprise. The main reason may be that Enterprise 14 has established a sound risk identification mechanism and can find various risk points in the supply chain promptly. An organizational structure matching supply chain risk management and control has been established to ensure that risk decisions and measures are effectively implemented. At the same time, it has many supply chain risk management talents, adopts information technology to improve the*

*transparency and response speed of the supply chain and attaches importance to strategic cooperation with supply chain partners. Thus, this reduces the risk of cooperation and gives it the supply chain's industry-leading overall control and coordination ability. In particular, the R-value of enterprise 8 is second only to that of enterprise 14, which shows that its strong agricultural supply chain management ability is very strong, and these two enterprises also have strong overall supply chain coordination ability. Enterprise 13, enterprise 7 and enterprise 15 are rated as the top three, and their S-value and R-value are large, especially the S-value of enterprise 7 reaches the highest 1, indicating that there is still a large gap between its supply chain management index and the optimal level. Based on the critical-entropy weight-VIKOR model, this study evaluates different agricultural supply chain enterprises in the face of agricultural supply chain risks and can more accurately identify benchmarking enterprises with outstanding supply chain management ability in the sample enterprises and inefficient enterprises with shortcomings that need to be focused on improving. This study objectively divides the levels of supply chain management between enterprises through quantitative data and provides a reference for the future development path of agricultural supply chain enterprises.*

| Agricultural supply chain enterprise number | The sum of distance ratio S of the optimal scheme | The maximum value of the optimal scheme distance ratio R | Profit ratio Q value | Scheme (Q value) ranking |
|---|---|---|---|---|
| 1 | 0.5567 | 0.0584 | 0.9065 | 11 |
| 2 | 0.3869 | 0.0562 | 0.4492 | 3 |
| 3 | 0.4803 | 0.0588 | 0.8149 | 9 |
| 4 | 0.4236 | 0.0588 | 0.7211 | 7 |
| 5 | 0.3888 | 0.0588 | 0.6635 | 6 |
| 6 | 0.4739 | 0.0556 | 0.5465 | 4 |
| 7 | 0.5922 | 0.0588 | 1.0000 | 15 |
| 8 | 0.3933 | 0.0526 | 0.1710 | 2 |
| 9 | 0.4703 | 0.0587 | 0.7873 | 8 |
| 10 | 0.5804 | 0.0588 | 0.9805 | 13 |
| 11 | 0.5323 | 0.0588 | 0.9010 | 10 |
| 12 | 0.4143 | 0.0577 | 0.6148 | 5 |
| 13 | 0.5912 | 0.0588 | 0.9984 | 14 |
| 14 | 0.2899 | 0.0539 | 0.1070 | 1 |
| 15 | 0.5416 | 0.0588 | 0.9163 | 12 |

**Table 4. VIKOR analysis results**

## 5. Conclusions

*China is in a critical period of agricultural supply-side structural reform. Optimizing the agricultural supply chain, constructing a systematic agricultural supply chain risk assessment framework and model, and implementing quantitative risk monitoring have become the inevitable needs of current research. This study proposes an enterprise risk evaluation index system for the agricultural supply*

*chain, consisting of five primary and 17 secondary indexes. The CRITIC and entropy weight methods are adopted to determine the enterprise risk index weight of the agricultural supply chain. The VIKOR method evaluates risk on 15 agricultural supply chain enterprises in an agricultural economic development zone. This study draws three conclusions. (1) Based on the existing literature, the enterprise risk evaluation index system of the agricultural supply chain constructed in this study is relatively scientific and reasonable. (2) The CRITIC weights of X-1-1, X-5-1, and X-5-2 are the highest. The entropy weight of X-5-1, X-5-2 and X-1-2 is the largest. (3) The critical-entropy weight-VIKOR model can effectively distinguish the degree of risk of different agricultural supply chain enterprises. It is suggested that further research should be carried out on the construction of dynamic risk assessment models, real-time monitoring of agricultural supply chain risk, integration of multi-source heterogeneous data to improve model prediction, and development of risk management systems to support decision-making.*

## Declarations of Interest

*None*

## Acknowledgements

*This work has been supported by the Science and Technology Commissioner Project for Rural Revitalization in Ningbo in 2022 (No. 2022S232).*

## References

[1] Tran, T. H., Dobrovnik, M., Kummer, S. (2018). Supply chain risk assessment: a content analysis-based literature review.International Journal of Logistics Systems and Management, 31(4), 562-591.

[2] Aqlan, F., Lam, S. S. (2015). A fuzzy-based integrated framework for supply chain risk assessment. *Internnaional Journal of Production Economics*, 161, 54-63.

[3] Jaffee, S., Siegel, P., Andrews, C. (2010). Rapid agricultural supply chain risk assessment: A conceptual framework. *Agriculture and Rural Development Discussion Study*, 47(1), 1-64.

[4] Bloemhof, J. M., van der Vorst, J. G., Bastl, M., Allaoui, H. (2015). Sustainability assessment of food chain logistics. *International Journal of Logistics Research and Applications*, 18(2), 101-117.

[5] Leat, P., Revoredo Giha, C. (2013). Risk and resilience in agri food supply chains: The case of the ASDA PorkLink supply chain in Scotland. *Supply Chain Management: An International Journal*, 18(2), 219-231.

[6] Banterle, A., Stranieri, S. (2008). The consequences of voluntary traceability system for supply chain relationships. *An application of transaction cost economics*. Food Policy, 33(6), 560-569.

[7] Dong, Q., Cooper, O. (2016). An orders-of-magnitude AHP supply chain risk assessment framework. *International Journal of Production Economics*, 182, 144-156.

[8] Ganguly, K., Kumar, G. (2019). Supply chain risk assessment: a fuzzy AHP approach. *Operations and Supply Chain Management: An International Journal*, 12(1), 1-13.

[9] Nakandala, D., Lau, H., Zhao, L. (2017). Development of a hybrid fresh food supply chain risk assessment model. *International Journal of Production Research*, 55(14), 4180-4195.

[10] Jiang, B., Li, J., Shen, S. (2018). Supply chain risk assessment and control of port enterprises: Qingdao port as case study. *The Asian Journal of Shipping and Logistics*, 34(3), 198-208.

[11] Ghadge, A., Fang, X., Dani, S., Antony, J. (2017). Supply chain risk assessment approach for process quality risks. *International Journal of Quality & Reliability Management*, 34(7), 940-954.

[12] Jaberidoost, M., Olfat, L., Hosseini, A., Kebriaeezadeh, A., Abdollahi, M., Alaeddini, M.,

Dinarvand, R. (2015). Pharmaceutical supply chain risk assessment in Iran using analytic hierarchy process (AHP) and simple additive weighting (SAW) methods. *Journal of Pharmaceutical Policy and Practice*, 8, 9.

[13] Liu, C., Ji, H., Wei, J. (2022). Smart supply chain risk assessment in intelligent manufacturing. *Journal of Computer Information Systems*, 62(3), 609-621.

[14] Chaudhuri, A., Mohanty, B. K., Singh, K. N. (2013). Supply chain risk assessment during new product development: a group decision making approach using numeric and linguistic data. *International Journal of Production Research*, 51(10), 2790-2804.

[15] Vishwakarma, V., Prakash, C., Barua, M. K. (2016). A fuzzy-based multi criteria decision making approach for supply chain risk assessment in Indian pharmaceutical industry. *International Journal of Logistics Systems and Management*, 25(2), 245-265.

[16] Junaid, M., Xue, Y., Syed, M. W., Li, J. Z., Ziaullah, M. (2019). A neutrosophic AHP and TOPSIS framework for supply chain risk assessment in automotive industry of Pakistan. *Sustainability*, 12(1), 154.

[17] Tummala, R., Schoenherr, T. (2011). Assessing and managing risks using the supply chain risk management process (SCRMP). *Supply Chain Management: An International Journal*, 16(6), 474-483.

[18] Díaz-Curbelo, A., Espin Andrade, R. A., Gento Municio, Á. M. (2020). The role of fuzzy logic to dealing with epistemic uncertainty in supply chain risk assessment: Review standpoints. *International Journal of Fuzzy Systems*, 22(8), 2769-2791.

[19] Sreedharan, V. R., Kamala, V., Arunprasad, P. (2019). Supply chain risk assessment in pharmaceutical industries: an empirical approach. *International Journal of Business Innovation and Research*, 18(4), 541-571.

[20] Tuncel, G., Alpan, G. (2010). Risk assessment and management for supply chain networks: A case study. *Computers in Industry*, 61(3), 250-259.

[21] Ritchie, B., Brindley, C. S., Armstrong, N. (2008). Risk assessment and relationship management: practical approach to supply chain risk management. *International Journal of Agile Systems and Management*, 3(3-4), 228-247.

[22] Radivojevic, G., Gajovic, V. (2014). Supply chain risk modeling by AHP and Fuzzy AHP methods. *Journal of Risk Research*, 17(3), 337-352.

[23] Diakoulaki, D., Mavrotas, G., Papayannakis, L. (1995). Determining objective weights in multiple criteria problems: The critic method. *Computers & Operations Research*, 22(7), 763-770.

[24] Zeleny, M. (1998). Multiple criteria decision making: Eight concepts of optimality. *Human Systems Management*, 17(2), 97-107.

[25] Opricovic, S., Tzeng, G.H. (2004). Compromise solution by MCDM methods: A comparative analysis of VIKOR and TOPSIS. *European Journal of Operational Research*, 156(2), 445-455).

DLINE JOURNALS

Journal of Information Security Research

Print ISSN: 0976-4143
Online ISSN: 0976-4151

JISR 2024; 15 (1)
https://doi.org/10.6025/jisr/2024/15/1/23-29

# An Efficient Security Framework for Cloud Computing

Farhan Nisar[1] Samad Baseer[2] Arshad khan[3]
[1,3]Department of Computer Science and Information Technology
Qurtaba University

[2]Department of Engineering & Technology
University of Engineering & Technology, Peshawar
Pakistan

{farhansnisar@yahoo.com}
{Drsamadbaseer@uetpeshawar.edu.pk}
{Arshidkhan1991@gmail.com}

**ABSTRACT**

*Many organisations have been established due to the rapid development of cloud in business environments. Today, our scenario related to cloud attacks on computer networks has increased because of security vernal ability and breaches in establishments. Many attack spenetrate our edge network device; some of the most prone attacks are ICMP attacks, CDP attacks and port security attacks, leading to a denial of service. In this paper, we analyze different mechanisms to provide network security by using different policies and rules on edge network devices to protect the network devices. We can be tested in Lab in Lab by using the GNS3 simulator. We are implementing these mechanisms to protect internal and external networks from attacks like ICMP, CDP, and Port Security.*

**Received: 27 August 2023**
**Revised: 20 November 2023**
**Accepted: 30 November 2023**


**Keywords:** Attacks, Security, Network, DoS, ICMP, CDP, Port Security

## 1. Introduction

*With the rapid increase in the use of networks for storing and sharing data, security attacks on computer networks have also increased [1] at an alarming rate. Even inside attacks have increased in the past few years. In an annual survey on cyber security, not only large organizations but also small organization businesses have been targeted by 63%. [2][3]. DOS Attack is an attack where the attacker shows him an authorized user and wants to access the service. The DOS attack may be attempted on a single machine but may be carried out by different computer attacks and Distributed Denial of service attacks. CDP attacks will control the network device, and local events can be impacted and lead to network instability, resulting in a loss of connection and data. Security will be solved by encryption and decryption of data and policies that enforce the data. Resources will be allocated to memory and the secure algorithm for security [4].*

*Finally, they can find data mining techniques for security, but they cannot be solved. In clouds many types of attacks can happen on cloud data centres, like random, strong and weak attacks. (i.e. criminal or terrorism). The cloud service is on web pages, and most data is on it, and hackers can target Amazon and Microsoft. It also explains the security and cybercrimes. If exceeded, the data store limit will cause such types of attacks. Cloud applications are concerned with data, and data must be reliable, and most threads are based on network layer distributed attacks. Denial of service attacks are related to network flooding of packets and hardware failure in the clouds.*

## 2. Types of Different Attacks

*There are many types of DOS attacks. Some major attacks can be classified as follows:*

• ***Distributed Attacks:*** *They can be attempted by online applications like trades, banking, and e-commerce. A specific host can target a particular application or be a small or large network with many hosts.*

• ***Insider Attacks:*** *A trusted person inside the organization does the attacks. These types of attacks are difficult to detect because the attacker knows the policies and rules of the network organisation, and the attacker can misuse information.*

• ***Active Attacks:*** *These can be initiated from a single PC and compromise many PCs around the globe connected to the internet with a low level of Security.*

• ***Close-in-Attacks:*** *Attackers analyzed traffic using Homeport to initiate the attack and tried to exploit them by sending emails and obtaining confidential information about the account, etc.*

• ***DOS Attacks:*** *DoS attack from a single source and compromised source with spoofed IP. Those attacks are huge in volume and paralyzed the network. The attacker tries to find out the vulnerability of the network and target to some specific service and consist of many hosts of small/extensive networks.*

## 3. Types of Dos Attacks

*The first attack was attempted on 2 November 1988[6]. This attack was self-propagating and stopped 15% of the system of the network, which was infected. There are several attacks of DoS, the popular as follows:*

- *Port Security Attacks*
- *ICMP Attacks*
- *CDP Attacks*
- *DHCP Attacks*

• ***Port Security Attacks:*** *A Port security attack is one of the most important attacks. Confidential information will be lost and damaged when any intruder inside an organization has easy access to the server.[5] If the port is shut down, it will not be implemented easily. It can simulate in Gns3 how to prevent port security attacks. We can see in this diagram that two users are connected to the network, and the remaining ports are empty. Then, a port security attack should be implemented.*

• ***ICMP Attacks:*** *Ping causes the remote system to hang, reboot or crash. The attacker will exploit the internet control message protocol, which enables the user to send an echo message to check whether it is alive. During a Dos attack, many ICMP_ECHO_Reply packets use ping messages [6]. These packets request and reply from unauthorized users and are the result of the bandwidth of the victim network connection. The attacker mostly sends ping commands to the router and checks whether the router gives any response or not.*

• ***CDP Attacks:*** *Before launching the Cisco Discovery Protocol flooding attack, it shows how it*

*affects our topology. The CPU utilization of the switch before the attack is 5%. The steps in OS that should be performed during the Cisco Discovery Packet attack are the following:*

*Go to Launch attack → Cisco Discovery Packet → Flooding CDP Table → OK.*

*After launching the attack and running for a few minutes, the CPU utilization of the switch is increased to 59%. If the attack runs a bit longer, the switch will drop packets because it will become too busy.*

• ***DHCP Attacks:*** *Before launching an attack, the following steps allow the practical execution of a DHCP attack using GNS3.*

*Create a network sub-interface on the machine as the default gateway to route our rogue DHCP client. Set an IP on the new Ethernet 0/1 interface to another unused IP address. Allow IP forwarding on your machine. Set the default gateway and default route on the Ethernet interface 0/1 sub-interface. Show the route table. Launch the DHCP module and show the optional and required options that have to be set to run a rogue DHCP server. In another terminal window, launch the DHCP attack. Start the Rogue DHCP server from the console. When a new user connects to the network and IP address, he gets assigned from the DHCP server; now, the default gateway is actually the IP address of the running machine. The attacker is now in the middle of the communication between the DHCP server and the User.*

## 4. Control Mechanism

*Many mechanisms are available for network security, and a few will be discussed briefly.*

• ***Firewall:*** *The firewall is a type of security that will control intrusion and monitor the incoming and outgoing traffic of the network in cloud Computing.*

• ***IDS System:*** *IDS stand for intrusion detection system, and it will protect the network from application-level attacks. It will identify the attempts, alert the system to maintain each user's log, and block and stop it.*

• ***ISP edge Router:*** *The edge device will accept traffic only from the source and monitor traffic between the sender and receiver on both sides.*

• ***Reactive Mechanism:*** *The mechanism will reduce attack and is also called an early working system, which responds to an attack immediately.*

*In this paper, we apply some mechanisms on edge networks and test these policies by simulating them in a GNS3 network simulator.*

## 5. Main Contribution of Our Work

*Analyze the different types of security as*

• *Studying different types of DoS attacks.*

• *Enhance different types of security mechanisms on edge network router*

• *GNS3 network to protect our network, like*

• *CDP, DHCP, ICMP and Port Security Attacks*

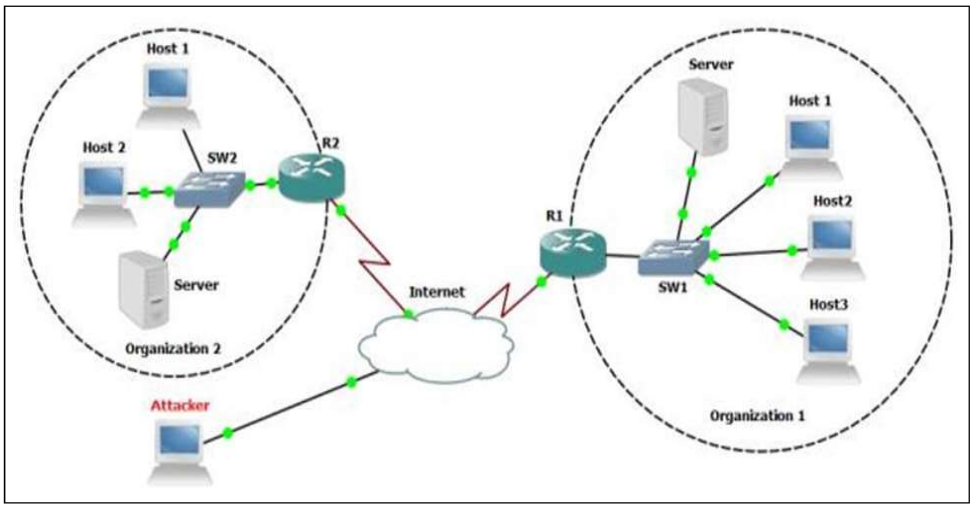
## 6. Simulation and Experimentation

***1.*** *For the Port, from the network, Port security is used for inside organization security because the attack ratio will be random and communication from source to destination will be random. When any attacker or intruder connects the port, it is necessary to disconnect the interface automatically*

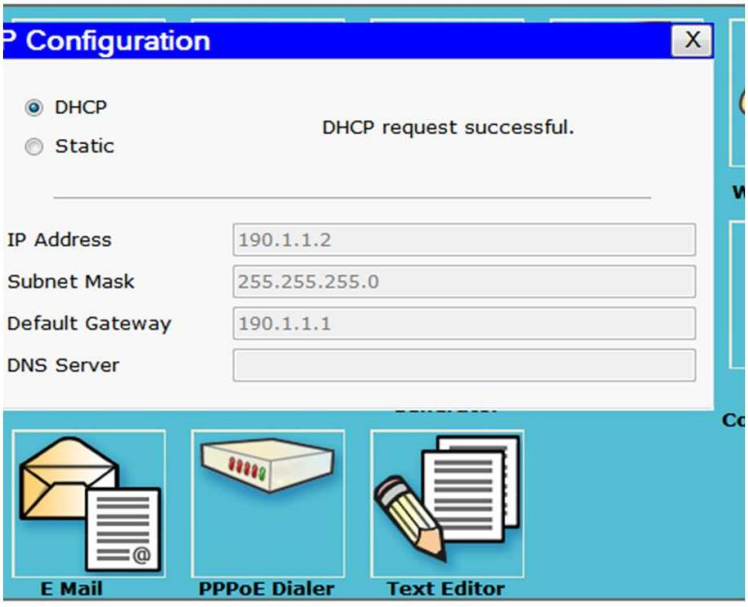
*by using this command.*

*The above result shows the result more clearly about the status of the packets dropped. When the packet increases, drops of packets will increase, and the attack must decrease at an optimal level.[7]*

*We apply policies on all router edges, switch off all interfaces when unused, and disable the ping command.*




***2.*** *There are several ways of preventing a DHCP attack with a rogue server for the DHCP attack. DHCP snooping is also used for these attacks. It provides network security by filtering un-trusted DHCP messages and maintains DHCP snooping in the table. Ports must be trusted and un-trusted. Un-trusted ports can be source requests only, and trusted ports contain all DHCP messages. After enabling DHCP spoofing using the command IP DHCP snooping, IP DHCP snooping vlan1 Attacker cannot be performed successfully. The command can be implemented in routers.*




***3.*** *For the CDP Attack, the only easy step to prevent a CDP flooding attack in GNS3 is to command disable CDP features on all the ports, and it will never share neighbour information and the attack*

*of DOS is prevented.*

*Before disabling the CDP, it will show the neighbour information, as shown in the figure.*

```
Office-R1#
Office-R1#
Office-R1#sh cdp nei
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID       Local Intrfce Holdtme Capability Platform Port ID
```

*The figure shows that the router and switch are connected to the internet with an interface connected to the network.*
*The command is run in the GNS3 simulator, as shown. When simulating in Gns3, it will never share information with any other router, and many organizations have disabled CDP.*

***4.*** *We apply policies called ICMP protocol, which will work in parameters like access group, bandwidth burst size, etc.*

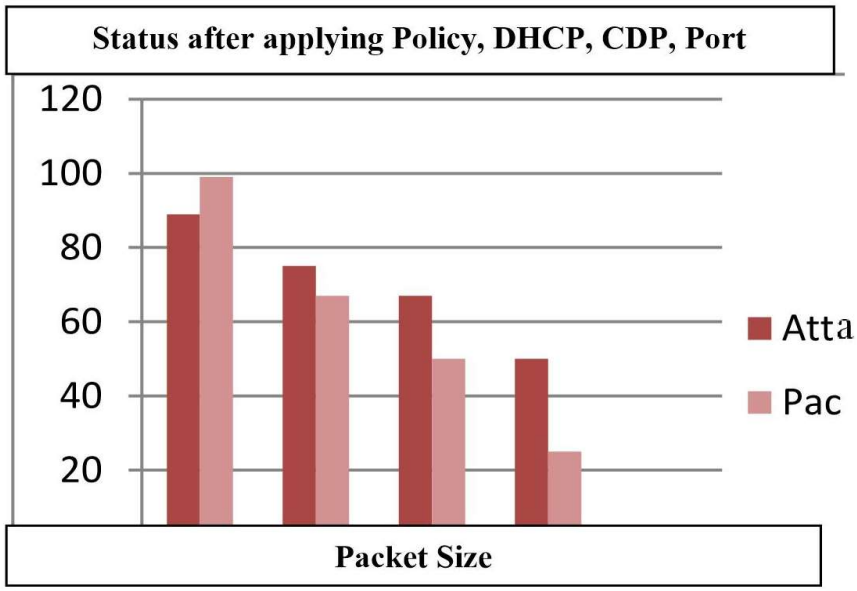
*Before we apply the policy, the success rate is high, and in time intervals, the attack is generated successfully up to 100%. We also sent different sizes of packets sent and reached up to the host network. It indicates a successful percentage of up to 99%.*

*Before we apply any policy in the GNS3 lab, we must check the success rate of attacks of different sizes of packets with different time intervals. The attack is generated and successful up to 100%. The outside attacker should ping the server user within the organization, and there is another problem inside the organization. If an authorized person becomes unfaithful, then he tries to destroy the network or give confidential information to another one, then it will be very unfaithful. So, we implement security for this type of attack. The diagram shows that the server will respond to the attack and then implement such a security mechanism for the attackers.*

*The table shows the result obtained after applying policies on edge and considering different parameters like packet size and repetition, and different values will be obtained. We see a gradual decrease in packets from 99% to 89% and reaching 0% status. The mechanism must be implemented in the organization, and the third party will also trust that your security will be secure and the success rate of attack is dropped concerning more packet size and taking readings at different time intervals.[8] If we apply the proper countermeasures mechanism, large and small organizations can be protected by applying policies like routers, web servers, firewalls, etc., and protect them to the maximum level. We implement such types of attacks with higher success rates and efficiency.*

| ICMP, DHCP, Port Security Attack with Policy Mechanism | | | |
|---|---|---|---|
| **ICMP echo** | **Packet Size** | **Attack success** | **Packet drops** |
| 100 | 250 | 98% | 2 |
| 100 | 500 | 91% | 9 |
| 100 | 750 | 70% | 30 |
| 100 | 1000 | 67% | 33 |
| 100 | 1500 | 0% | 100 |

*The graph will show the existing work with the new work after applying such types of security for it. They will show the new techniques are reliable for cloud users.*




*The Graph shows the above result more clearly and checks the packet's status dropped. The size of the packet increases, then more impact on attack success, and the drop rate of the packet increases. The attack must be decreased optimally by applying such a policy for internal and external edges on the network. It is more successful as packet size increases and packet dropped rate increases, and even reaches the maximum level.*

## 7. Reltad Work

*Many researchers have done lots of work on security and establishing the network; a few papers related to our work are:*

*In 2012 [4], Bellovin implemented a mechanism on the routers and provided a pushback mechanism for the flooding attacks, but he discussed only countermeasures.*

*Rao Kompella, in 2007 [5], proposed a novel data structure called a partial completion filter that can detect claim and hold attacks in the network. Still, he demonstrated the low false positive and false negative probability of the network.*

*Katerina and David in 2009 [6] presented Active Internet Traffic filtering based on internet Bandwidth flooding Attacks but provided scalable deployment solutions for the bandwidth flooding attack.*

*Xin Liu in 2010 [7] presents a novel mechanism to enable robust congestion policing feedback inside the network. It can used to unsecure traffic. They are using ns2 simulation and theoretical analysis for the DoS solution. Mitko and Risteski, in 2011 [8],sent bogus packets to the router and disrupted and intercepted communication from the wireless access point. They approach the ICMP Ping flood attack and provide different types of countermeasures. Simulation results affect the link failure recovery mechanism against this type of attack.[10]*

## 8. Comparative Analysis

*In Katrina's 2009 paper, they present Active internet Traffic filtering for flooding attacks. They have shown that:*

***1.** It allows the receiver to preserve, on average, 80%, and its tail circuit of Syn-flooding attack has ten times the rate of its capacity.*

***2.*** *Each participating ISP need thousands of filters and a few megabytes of Dynamic RAM per client; the per-client cost is not expected to increase unless bot net size outpaces Moore's law.*

*These two active internet traffic filters enable networks to maintain their communication during the flooding attack, and the path between them cannot be compromised.*

*Mitko and Risteski 2011 discussed the behaviour of wireless networks under different numbers of attackers and ping packet sizes; they found QoS parameters can be reduced under these types of flooding attacks. During their work, they simulated the same scenarios when a firewall and fast recovery of filtering of ICMP ECHO massage is used. In all these situation results, they intend to continue exploring the possibility of setting an optimal threshold for successor and recovery mechanism if an active large number of packets or greater size ICMP packet was received.*

*Our approach in this paper has the following aspects.*

***1)*** *Our approach is straightforward to implement.*

***2)*** *The result clearly shows the packet size increased and decreased, reaching up to 99%.*

***3)*** *There is no effect related to time. These policy, CDP, and DHCP mechanisms will be successful for the Local area networks. Still, there are many areas of effective inputs that could be referred from the work by earlier research.*

## 9. Conclusion and Future Work

*This research identifies the attack attempts and shows that security testing can be challenged and met. They show several security issues and how specific processes can solve them. Security is related to protecting our information, and we must have issues of availability and how to prevent DoS attacks in cloud computing. It is vital to protect our office network from newly evolved attacks. Recently, a survey has revealed that attacks on smaller organizations are to a great extent. Our simulation results show that policy, DHCP, CDP and Port Security mechanism success rate becomes high and packet drops rate and reach to maximum level. Furthermore, investigating a high level of monitoring is necessary to know attacks and their signature, which an edge router can implement to counter the maximum types of attacks with a higher success rate and efficiency.*

## References

[1] Harshita. (2013). A survey of different types of security threats and its countermeasures.

[2] Computerweekly.com.

[3] Ponemon Institute/Symantic.com.

[4] Ionanidis, J., Bellovin, S. (2012). Implementing PushBack: Router-based Defense Against DDoS Attacks.

[5] Rao, R. (2007). On Scalable Attack Detection in the Network.

[6] Karerna., David. (2009). Scalable Network-Layer Defense Mechanism against Internet Bandwidth Flooding Attack.

[7] Lui, X. (2010). Preventing Internet Denial of Service from Inside Out.

[8] Bogdanoshi, M. (2011). Wireless Network Behavior under ICMP Flood DoS Attack and Mitigation Techniques.

[9] TELELINK. (2013). Corporate WAN Threats, IT Threats – Control Plane Attack.

[10] CSA, Security Guidance. (2014). Construction of digital campus security based cloud computing.

# NOTIFICATION

---

## AI Workshop

Instats is pleased to present three exclusive livestreaming seminars on integrating AI into your research, demystifying the fundamentals of AI and large language models with a deep dive into the theory and practice of their use in various research fields. They offer a cutting-edge exploration of how AI in general and generative AI specifically can revolutionize your research, empowering you with the knowledge and tools you need to advance your research agenda in the ever-evolving landscape of AI technology.

**A Gentle Introduction to Artificial Intelligence** by computer science professor Ricardo Vilalta, running Jan 25 - 26, offers a comprehensive overview of AI with hands-on applications and an overview of AI's relevance in academic research - including discussions of ethical considerations and future trends in AI.

**Using Generative AI for Qualitative Research** by Professor Christina Silver, running Feb 1 - 2, is a comprehensive workshop that will equip researchers with the skills to utilize AI appropriately in qualitative analyses, covering a range of topics from understanding AI software tools to ethical considerations as well as troubleshooting typical roadblocks to integrating AI into your research.

**Large Language Models: AI Foundations and Applications in Python** by former CERN physicist and senior data scientist Dr. Jayanti Prasad, running Feb 5 - 9, provides a comprehensive understanding of large language models, their AI foundations, and applications in Python including hands-on coding sessions, case studies, and discussions on the future of large language models in academic research.

We also have a few places left for the upcoming workshops on Using ChatGPT for Advanced Data Analysis 2.0, offered Jan 18 - 19 for the Americas/Australasian time zones as well as Feb 21 - 23 for European time zones. With the tools these workshops are offering you'll be able to incorporate AI into your research seamlessly. Please tell your friends and colleagues, and we hope to see you there!
**instats.org**

**********

## Monitor levels of interdisciplinary research

### *Report*

As part of a broader initiative to measure and understand the University of Manchester's interdisciplinary research activities, we have been exploring the potential of bibliometric indicators to monitor levels of interdisciplinary research over time. In news which we are sure will not surprise us, this is proving to be a very difficult task! Over the past year, various approaches have been experimented with and assessed, each offering distinct perspectives and encountering specific limitations.

**1. Citation based**: Using a set of publications from one of our Research Institutes, we focused on the diversity of subject categories cited within these articles as a proxy for interdisciplinarity. This employed three specific bibliometric indicators (Variety: Count of different subject categories cited / Balance: Evenness in the distribution of cited categories, quantified using an adjusted Gini coefficient / Disparity: Cognitive distance between cited subject categories, determined by their relative positions on a cognitive map of academic disciplines).

**2. Analysis based on organisational affiliations:** This approach assessed the interdisciplinary nature of research outputs by counting the distinct organisational units in the author lists of papers from the past year. The number of different units was used as a potential proxy for interdisciplinary activity.

**3. Distinct Subject Area Count and Expert Review Comparison:** The Library analyzed papers associated with research publications from 2018 to 2023 for two of our Research Institutes. The process involved systematically collecting publication data, mapping each paper's All Science Journal Classification (ASJC) codes to broader subject areas, thus calculating a distinct subject area count per paper. Domain experts then reviewed and scored these same papers based on their perceived interdisciplinarity. The final stage involved a comparative analysis of the distinct subject areas count and expert scores to evaluate the method's effectiveness in accurately identifying interdisciplinary research.

**All of the approaches above encountered significant limitations:**

1. Despite the robust analysis, no clear correlation was found consistently linking high scores on these indicators with interdisciplinary research. The complex methodology also created challenges regarding the scalability of this approach.

2. The working group found that the diversity of organisational affiliations did not reliably indicate interdisciplinary research. It was noted that disciplinary research is often conducted across various units, not confined to a single department or school. As a result, collaboration between authors from different units did not necessarily equate to interdisciplinary research, making this proxy too simplistic and unreliable for accurately identifying interdisciplinary work.

3. Expert reviews did not support The assumption that a higher Distinct Subject Areas Count correlates with increased interdisciplinarity, indicating variability in how interdisciplinarity is perceived and assessed. Moreover, the use of broad subject areas for categorisation may not capture the nuanced, specific intersections in interdisciplinary work, potentially leading to over- or underestimation.

As a result of the above, we are very interested in the development work currently undertaken by THE / Schmidt relating to the ISF.

While we have noted some of the concerns around the methodologies employed, we are very interested in understanding more about how the bibliometric indicators (based on Open Alex data) were generated for these rankings. Not least, how papers were identified as interdisciplinary in the first place!

Does anybody have any insight at all on the methodology that has been used by THE/ Schmidt in their development work, which they would be willing to share? We are hoping it might provide us with some more avenues for experimentation. Failing that, if anybody has any success stories to share - related to mapping interdisciplinary research across their own institution.

John Hynes - Research Services Co-ordinator:
The University of Manchester Library

**********

## Open Data Report

### The State of Open Data 2023: A more analytical approach provides unparalleled insights Laura Day

Figshare, Part of Digital Science.

Digital Science, Figshare and Springer Nature are proud to publish The State of Open Data 2023. Now in its eighth year, the survey is the longest-running longitudinal study into researchers' attitudes towards open data and data sharing.

The 2023 survey saw over 6,000 responses and the report that has now been published takes an in-depth look at the responses and purposefully takes a much more analytical approach than has been seen in previous years, unveiling unprecedented insights.

### 1. Five key takeaways from the State of Open Data 2023

**1. Support is not making its way to those who need it :** Over three-quarters of respondents had never received any support with making their data openly available.

**2. One size does not fit all :** Variations in responses from different subject expertise and geographies highlight a need for a more nuanced approach to research data management support globally.

**3. Challenging stereotypes :** Are later career academics really opposed to progress?

The results of the 2023 survey indicate that career stage is not a significant factor in open data awareness or support levels.

**4. Credit is an ongoing issue :** For eight years running, our survey has revealed a recurring concern among researchers: the perception that they don't receive sufficient recognition for openly sharing their data.

**5. AI awareness hasn't translated to action :** For the first time, this year we asked survey respondents to indicate if they were using ChatGPT or similar AI tools for data collection, processing and metadata creation.

### 2. Diving deeper into the data than ever before

This year, we dive deeper into the data than ever before and look at the differing opinions of our respondents when we compare their regions, career stages, job titles and subject areas of expertise.

Figshare founder and CEO Mark Hahnel said of this approach, *"It feels like the right time to do this. Whilst a global funder push towards FAIR data has researchers globally*

*moving in the same direction, it is important to recognize the subtleties in researchers' behaviors based on variables in who they are and where they are."*

This year features extensive analysis of the survey results data and provides an in-depth and unique view of attitudes towards open data.

This analysis provided some key insights; notably that researchers at all stages of their careers share similar enthusiasm for open data, are motivated by shared incentives and struggle to overcome the same obstacles.

These results are encouraging and challenge the stereotype that more experienced academics are opposed to progress in the space and that those driving progress are primarily early career researchers.

We were also able to look into the nuanced differences in responses from different regions and subject areas of expertise, illuminating areas for targeted outreach and support. These demographic variations also led us to issue a recommendation to the academic research community to look to understand the 'state of open data' in their specific setting.

### 3. Benchmarking attitudes towards the application of AI

In light of the intense focus on artificial intelligence (AI) and its application this year, for the first time, we decided to ask our survey respondents if they were using any AI tools for data collection, processing or metadata collection.

The most common answer to all three questions was,*"I'm aware of these tools but haven't considered it."*

Although the results don't yet tell a story, we've taken an important step in benchmarking how researchers are currently using AI in the data-sharing process. Within our report, we hear from *Niki Scaplehorn* and *Henning Schoenenberger* from Springer Nature in their piece 'AI and open science: the start of a beautiful relationship?' as they share some thoughts on what the future could hold for research data and open science more generally in the age of AI.

We are looking forward to evaluating the longitudinal response trends for this survey question in years to come as the fast-moving space of AI and its applications to various aspects of the research lifecycle accelerate farther ahead.

### 4. Recommendations for the road ahead

In our report, we have shared some recommendations that take the findings of our more analytical investigation and use them to inform action points for various

stakeholders in the community. This is an exciting step for The State of Open Data, as we more explicitly encourage real-world action from the academic community when it comes to data-sharing and open data.

**Understanding the state of open data in our specific settings:** Owing to the variations in responses from different geographies and areas of expertise, we're encouraging the academic community to investigate the 'state of open data' in their specific research setting, to inform tailored and targeted support.

**Credit where credit's due:** For eight years running, our respondents have repeatedly reported that they don't feel researchers get sufficient credit for sharing their data. Our recommendation asks stakeholders to consider innovative approaches that encourage data re-use and ultimately greater recognition.

**Help and guidance for the greater good:** The same technical challenges and concerns that pose a barrier to data sharing transcend different software and disciplines. Our recommendation suggests that support should move beyond specific platform help and instead tackle the bigger questions of open data and open science practices.

**Making outreach inclusive:** Through our investigation of the 2023 survey results, we saw that the stage of an academic's career was not a significant factor in determining attitudes towards open data and we saw consensus between early career researchers and more established academics. Those looking to engage research communities should be inclusive and deliberate with their outreach, engaging those who have not yet published their first paper as well as those who first published over 30 years ago.

## 5. What's next for the State of Open Data?

The State of Open Data 2023 report is a deliberate change from our usual format; usually, our report has contributed pieces authored by open data stakeholders around the globe. This year, we've changed our approach and we are beginning with the publication of this first report, which looks at the survey data through a closer lens than before. We've compared different subsets of the data in a way we haven't before, in an effort to provide more insights and actionable data for the community.

In early 2024, we'll be releasing a follow-up report, with a selection of contributed pieces from global stakeholders, reflecting on the survey results in their context. Using the results showcased in this first report as a basis, it's our hope that this follow-up report will apply different contexts to these initial findings and bring new insights and ideas.

In the meantime, we're hosting two webinars to celebrate the launch of our first report and share the key takeaways. In our first session, The State of Open Data 2023: The Headlines, we'll be sharing a TL;DR summary of the full report; our second session, The State of Open Data 2023: In Conversation, will convene a panel of global experts to discuss the survey results.

**CALL FOR PAPERS**

**Fourth International Conference on Digital Data Processing (DDP 2024)**
**Yeshiva University, New York, US**
**September 25-27, 2024**
**IEEE Xplore**
(www.socio.org.uk/ddp)

Data grows voluminously and exponentially with heterogeneity and complexity. A single organization or industry processes over a few million transactions hourly and stores several petabytes of data. We live in a world of tremendous pressure to analyze and process data more efficiently where theData analytics can reflect hidden patterns, incomprehensible relationships, intrinsic information relations, and segmentation. The data applications have introduced cutting-edge possibilities in every activity in our lives. Thus, studying data and its underlying structure, dynamics of data relations, and newer data technologies is a never-ending process. The literature and research on data management are enormous; they do not sufficiently solve the data processing requirements.

Currently, the use of technology and interrelations among information pieces generate enormous amounts of data. Many studies tend to develop models and systems to analyze voluminous datasets. Analyzing the impact of data leads to application domains on decisions that have a systematic influence. Knowledge generated from the data analysis can enable the production of critical information for several domains.

Hence, this conference reviews and discusses the recent trends, opportunities, and pitfalls of data management and how it has impacted organizations to create successful business and technology strategies and remain updated in data technology. This conference also highlights the current open research directions of data analytics that require further consideration.

The proposed conference will discuss topics not limited to

- Data applications in various domains and activities
- Data in cloud
- Real-world data processing
- Data inaccuracy and reliability issues
- Data Ecosystem
- Business Analytics
- New data analytics techniques
- Physical and management challenges

• Privacy and Security

• Crowdsourcing and Sensing

• Data modelling

• Deep learning techniques

• Data fusion

• Descriptive analytics, Diagnostic analytics, Predictive Analytics, and Prescriptive analytics

• Machine learning

• Network optimization

• Data in Biomedical Engineering

• Data in Materials science and mechanics

• Data handling and applications in domains

• Wireless Networking Data Management

• Data of Electronic & Embedded Systems

• Multi-media Systems Data

• Artificial intelligence Models and Systems Data

• E-Computing Data

• Renewable Energies Data

**Publications**

Besides, modified versions of the papers will appear in the following journals.

1. Journal on Data Semantics
2. Technologies
3. Data Technologies and Applications
4. Webology
5. Journal of Digital Information Management
6. International Journal of Computational Linguistics
7. Journal of Optimization
8. International Journal of Distributed Systems and Technologies1

## Important Dates

| | |
|---|---|
| Submission of Workshop Proposals: | March 31, 2024 |
| Submission of Papers: | June 15, 2024 |
| Notification of Acceptance/Rejection: | July 20, 2024 |
| Camera-ready: | September 01, 2024 |
| Registration: | September 01, 2024 |
| Conference Dates: | September 25-27, 2024 |

## Paper Submission:

**Contact:** stm@socio.org.uk

# CALL FOR PAPERS

5th workshop on DATA FOR THE WELLBEING OF MOST VULNERABLE
https://sites.google.com/view/dataforvulnerable24
June 3, 2024
Buffalo, NY, USA

* Submissions due: March 24, 2024 *

At the International AAAI Conference on Web and Social Media (ICWSM)
https://www.icwsm.org/2024

The scale, reach, and real-time nature of the Internet is opening new frontiers for understanding the vulnerabilities in our societies, including inequalities and fragility in the face of a changing world. From tracking seasonal illnesses like the flu across countries and populations, to understanding the context of mental conditions such as anorexia and bulimia, web data has the potential to capture the struggles and wellbeing of diverse groups of people. Vulnerable populations including children, elderly, racial or ethnic minorities, socioeconomically disadvantaged, underinsured or those with certain medical conditions, are often absent in commonly used data sources. Further, data and algorithmic biases, especially in the light of the recent generative AI models, spotlight the awareness needed to build inclusive and fair systems when dealing with crisis management.

Thus, the aim of this workshop is to encourage the community to use new sources of data as well as methodologies to study the wellbeing of vulnerable populations. The selection of appropriate data sources, identification of vulnerable groups, and ethical considerations in the subsequent analysis are of great importance in the extension of the benefits of big data revolution to these populations. As such, the topic is highly multidisciplinary, bringing together researchers and practitioners in computer science & AI, epidemiology, demography, linguistics, and many others.

• Relevant topics include, but are not limited to:

• Establishing cohorts, data de-biasing

• Validation via individual-level or aggregate-level data

• Linking data to disease and other well-being

• Population data sources for validation

• Correlation analysis and other statistical methods

• Longitudinal analysis on social media

• Spatial, linguistic, and temporal analyses

• Privacy, ethics, and informed consent

• Biases and quality concerns around vulnerable groups in LLMs

• Data quality issues

The workshop will be held on June 3, 2024 in a hybrid format (both in person in Buffalo, NY, and online). The accepted papers will be presented in person at the workshop and published in the workshop proceedings of the conference.

**Important Dates**
Papers Submissions: March 24, 2024

Paper Acceptance Notification: April 14, 2024

Final Camera-Ready Paper Due: May 5, 2024

ICWSM-2024 Workshops Day: June 3, 2024

**Submission Instructions**

We welcome both 2-page abstracts, as well as Long (8 pages) and Short (4 pages) papers - excluding references (11 pages max with references). The Long and Short papers will be published in ICWSM Workshop proceedings (http://workshop-proceedings.icwsm.org/).

The papers have to follow the AAAI format, as outlined here: https://www.overleaf.com/latex/templates/aaai-2023-author-kit/wxnmhzcrjbpc

Submit here: https://easychair.org/conferences/?conf=dwmv24

**Contact**

Feel free to contact organizers with any questions:

Yelena Mejova
https://yelenamejova.com

Kyriaki Kalimeri
https://www.linkedin.com/in/kalimeri/

Daniela Paolotti
https://www.isi.it/en/people/daniela-paolotti

# The International School on Foundations of Security Analysis and Design (FOSAD)

## FOSAD series

### 2024: 26-30 August

Cybersecurity emerged as one of the most challenging research areas in computer science and engineering. The International School on Foundations of Security Analysis and Design (FOSAD) has been one of the foremost events established with the goal of disseminating knowledge in this critical area. The aim of the FOSAD school is to offer a good spectrum of current research in foundations of cybersecurity - ranging from programming languages to cryptographic protocols verification, from data protection to software systems security - that can be of help for graduate students and young researchers from academia or industry who intend to approach the field.

Since the first event in 2000 and until its 22nd edition in 2023, FOSAD attracted about 1020 participants and 180 lecturers from all over the world. The school programme alternates monographic courses given by well-known experts. Moreover, FOSAD encourages presentations given by those participants who intend to take advantage of the audience for discussing their current research in the area. Many of the young speakers of the FOSAD open session are now appreciated researchers and professors.
Location

The FOSAD school is held annually at the University Residential Center of Bertinoro, in the fascinating scenario of a former convent and episcopal fortress that has been transformed into a modern conference facility with computing services and Internet access.
Contact

To receive the latest updates on the school, the satellite events, and further security related events, subscribe to:

security@fosad.org

A mailing list for the scientific community interested in computer security.