Challenges and Solutions in Network Security for Serverless Computing

Sina Ahmadi

Challenges and Solutions in Network Security for Serverless Computing

Sina Ahmadi

Independent Researcher, United States

sina0@acm.org

ABSTRACT

This research study explores the challenges and solutions related to serverless computing so that the computer systems connected to the network can be protected. Serverless computing can be defined as a method of managing computer services without the need to have fixed servers. The qualitative research method is used by this research study, which does not include any numerical data and involves the examination of non-number data so that the network security challenges can be identified in detail. In the literature review, the past studies from 2019 to 2023 are reviewed to identify study gaps so that the foundation for investigating serverless network security. The literature review is based on thematic analysis, so all the data can be organized into meaningful themes. The findings of this research study include the solutions to the challenges like data privacy, insecure dependencies and limited control. The strategies to overcome these challenges include encryption, strong monitoring and other relevant strategies. This research study also suggests the use of blockchain technology and Artificial Intelligence. In short, this research study provides insights to improve serverless computing security and also guides future researchers to innovate creative solutions for developing security challenges.

KEYWORDS: Serverless Computing, Network Security, Cloud Security, Data Privacy Issues, Insecure Dependencies

I. INTRODUCTION

Serverless computing can be defined as the approach to providing backend services on an as-used basis. Serverless does not mean servers are not used; they are used, but the organizations getting serverless computing services are charged based on the services they use [1]. This means the amount or the number of servers still needs to be fixed. Serverless computing comes with several benefits and differs from traditional cloud computing. For instance, it offers great scalability, enhanced processing time, more flexibility, reduced cost and quicker time to release. It is important to consider that server computing not only comes with benefits but also significant challenges that need to be overcome by organizations to enjoy its advantages. The major challenges are related to the network's security, which includes the security of the connected devices and users and the data getting transferred from one device to another. This research study aims to explain the challenges related to network security for serverless computing along with their solutions. The best way to overcome such challenges is to limit access to the network to protect it from unauthorized access. Moreover, security systems must be implemented, such as a two-factor authentication method, so that no unauthorized person or device could harm a specific network's personal and sensitive information.

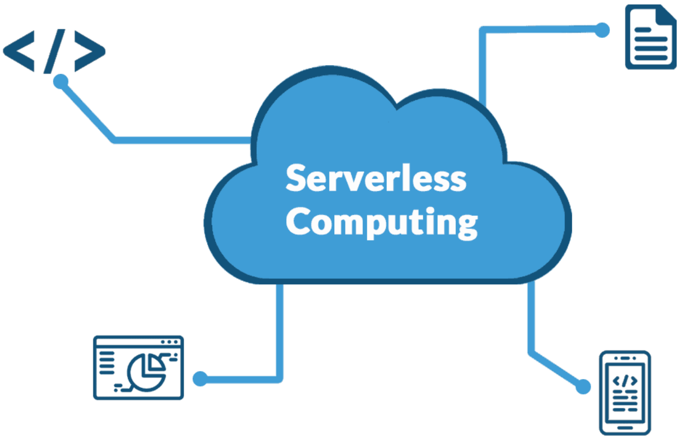


Figure 1: Serverless Computing [2]

II. PROBLEM DEFINITION

Serverless computing is the main part of the cloud server. Its reliability and lower cost make it suitable and useful for large projects. However, they have to face many challenges, especially regarding network security [3]. They can solve this problem to reduce their challenges.

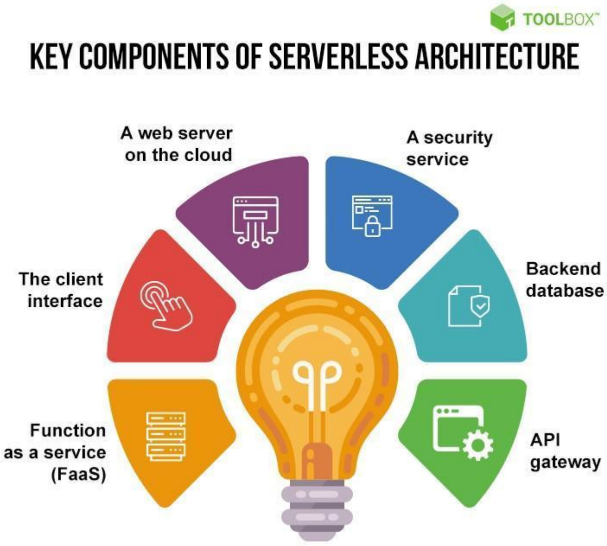

TOOLBOX
KEY COMPONENTS OF SERVERLESS ARCHITECTURE
A web server on the cloud
A security service
The client interface
Backend database
Function as a service (FaaS)
API gateway

Figure 2: Serverless computing architecture in cloud network [4]

A. Limited Visibility and Control

In serverless computing, there is always a challenge which they have to face. The challenge is the loss of control and limited visibility [5]. In traditional security approaches, the administrators have direct access to the system, but this needs to be updated in serverless computing. The lack of insight into these areas and the absence of traditional networking controls give the unauthorized user a chance to get access to the system or data. These challenges can be solved by monitoring the system and increasing its security. Without strong visibility over the network, an organization can face a lot of challenges in detecting and responding to security incidents.

B. Insecure Dependencies

Serverless applications depend on third-party libraries like APIs, leading them to face different security threats [6]. This dependency creates a path for hackers or other unauthorized users to access the network or data. Organizations should understand how to control this to secure the network and data. Effective measures should be created to monitor and update the third-party libraries. When the organization starts to reduce these challenges, it can help the system remain protected from external illegal access.

C. Cold Start Attacks

There is another challenge for serverless computing named "cold start", characterized by early functions that have not been executed recently [7]. This temporary delay creates a window for the attackers to gain access to data, which raises security concerns. Currently, traditional security measures cannot be proven effective, highlighting the importance of new solutions. To reduce the effect of this challenge, they need to create new strategies to reduce the cold start time without compromising security. These risks can be reduced by implementing security measures on serverless applications. As the organization overcomes these challenges, the solutions to reduce the external access during the cold start phase ensure the increase of reliability of the serverless computing system.

D. Data Privacy and Resilience

Adding data processing in serverless computing increases the chances of damaging the data privacy and reliability of the system [8]. Organizations may hesitate to share sensitive data due to these data privacy issues in serverless systems. The danger of data loss or corruption comes as a challenge to the reliance on the serverless system. To solve this issue, they require a nuanced approach to data management, strong encryption, security measures and effective backup strategies. Ensuring a good balance between data privacy and the advantages of serverless computing becomes important for the organization.

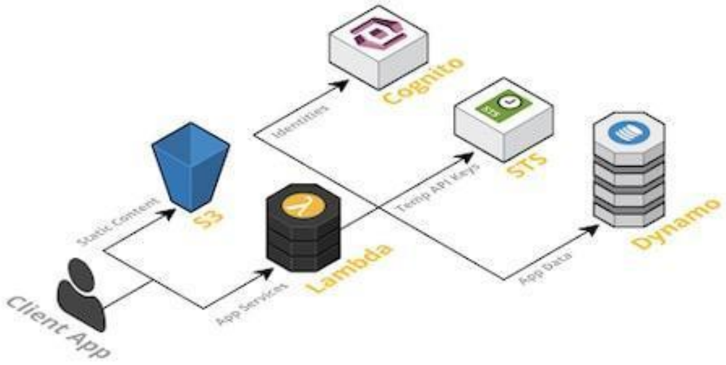


Figure 3: Serverless Security in Cloud Network [9]

E. Injection Attacks and Isolation

Serverless functions sharing a limited run time system cause isolation challenges like injection attacks [10]. These challenges can cause an attacker to gain a golden chance to have unauthorized access. This highlights that the organisation must apply a strong run time protection mechanism and good isolation strategy. The main difficulty comes in making the system strong from different attacks while maintaining efficiency in a serverless structure. The organization must apply strong security measures to detect attackers early, ensuring the system's integrity during the shared run time environment. As the system progresses, solving these challenges to create a safe and reliable system becomes important.

F. Resource Exhaustion and Denial-of-Service (DoS)

The scaling of resources in serverless computing environments leads to increased challenges related to resource exhaustion and the threat of denial-of-service attacks [11]. The harmful hacker may try to overpower or control the serverless system, which causes bad performance or unavailability of services. They must apply proactive measures to solve these challenges, including effective rate limiting and planned utilization of auto-scaling features. By improving how resources are assigned and increasing responsiveness, an organization can save their serverless system against unauthorized access, ensuring strong performance even when there are malicious attempts by attackers to take advantage of this dynamic scaling serverless computing model.

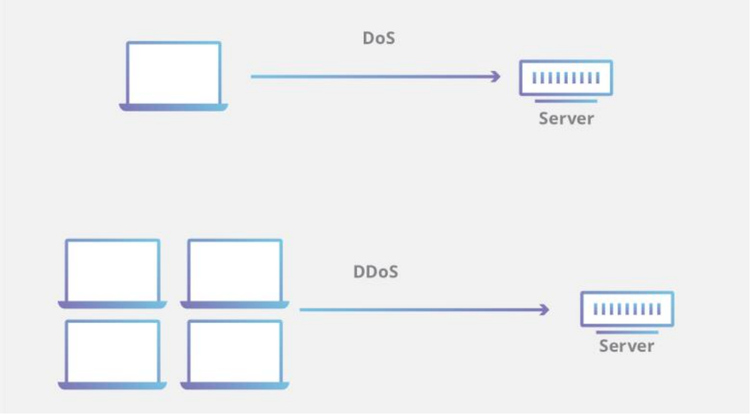


Figure 4: Denial-of-service (DoS) attack [12]

III. LITERATURE REVIEW

A. Introduction to Serverless Computing

Serverless computing mainly relates to providing backend services based on 'as-used.' This means the servers are still used, but a firm that avails backend services from a serverless provider is charged based on usage instead of a specific number of servers or bandwidth. [13] researched serverless computing in the case of the Internet of Things. The research showed that with the help of serverless computing, solutions can operate in an integrated manner on cloud, fog, and edge layers. Besides, many critical functions can be performed on fog and edge to gain benefits from low-latency responses. On the other hand, heavy functions can be performed on the cloud to process large amounts of data created by IoT sensors.

[14] also focused on serverless computing and its adoption. The researchers stated that serverless computing is becoming famous because of its management simplicity and lightweight-ness. It attains these merits by lessening the granularity of the computing unit. Particularly, serverless computing enables users to emphasize the function instead of other scheduling or management problems faced by the platform provider. The researchers mainly conducted a detailed survey on serverless computing, focusing on its infrastructure features. It was also seen that serverless computing is expected to dominate future cloud platforms.

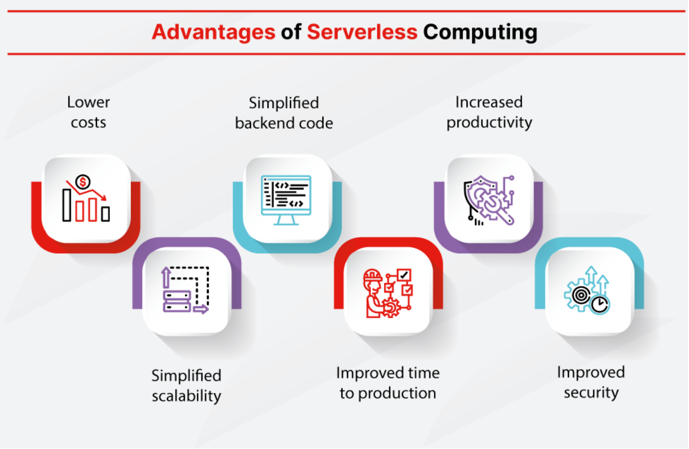


Figure 5: Introduction to Serverless Computing [15]

B. Security Challenges in Serverless Computing

Serverless computing encounters many security issues and challenges. One major issue is the occurrence of cold-start attacks. In serverless computing, idle resources are usually released in case of favourable pricing policy and energy efficiency. This procedure is called scaling to zero. When the resources are scaled to zero, it takes some time to be processed further for usage when a new function comes. This latency is thus known as a cold start. [16] focused on this issue and conducted research to mitigate it. The researchers stated that the cold start relates to the time delay between attaining a lambda request in the application and the initiation of executing code for it. AWS is one of the famous serverless service providers and has developed Snap Start to resolve the issue of cold start attacks.

Another area for improvement with serverless computing is inadequate authorization and authentication. In this case, the user does not have direct control over their visibility over the infrastructure and servers and has to depend on the cloud provider to protect and secure the code and data. [17] also researched this issue and stated that serverless computing features, like fragmented application boundaries, have led to security issues. Different serverless platforms also adopt different security measures to improve the serverless environment. Thus, the researchers analyzed the literature in detail and conducted a gap analysis based on industrial solutions regarding serverless computing.

A major issue with serverless computing is data at rest and transit. Data at rest relates to when data is stored in one place instead of moved to another place (in transit) or loaded into memory to be utilized by a software program. This feature of serverless computing faces many issues. [18] also focused on such issues with data at rest. It can encounter the issue of ransomware, a kind of malware that encrypts the data at rest. This makes the data unusable by anyone. Besides, it is also susceptible to data breaches by malicious attackers who can access and leak the data. Another issue is linked to excessive or unauthorized access to data at rest. All these issues enhance the security threats to serverless computing.

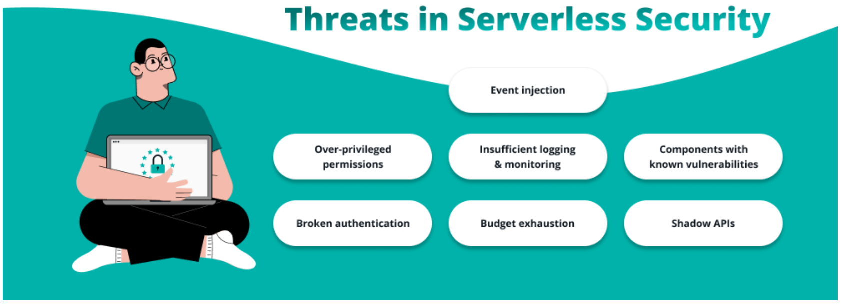
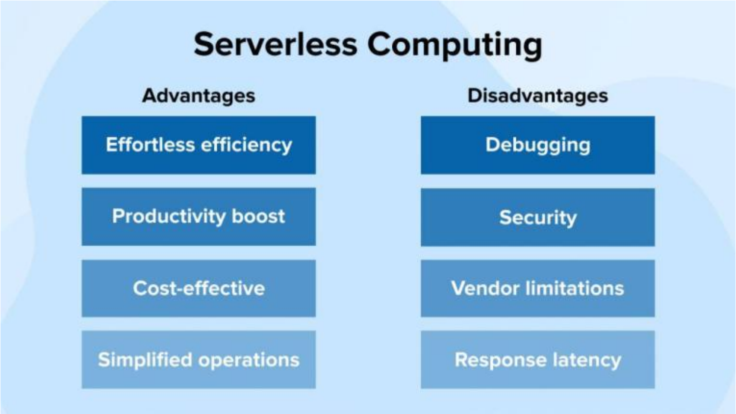

Threats in Serverless Security
Event injection
Over-privileged permissions
Insufficient logging & monitoring
Components with known vulnerabilities
Broken authentication
Budget exhaustion
Shadow APIs

Figure 6: Threats in Serverless Computing [19]

Shared resources and multi-tenancy also lead to security issues in serverless computing. A multi-tenant serverless platform mainly allows various tenants or users to utilize the same resources. Each user has access to their resources without interfering with others. [20] also focused on the aspect of resource sharing in serverless computing. Multitenancy is a major threat of hacking. No matter how safe or secure an encryption is, it can be hacked with the right information. Thus, The researchers proposed a new serverless computing platform, MXFaaS, which is secure and has improved efficiency levels.

Another major issue with serverless computing is dependency security. The aspect of third-party dependencies in serverless computing raises security concerns. [21] conducted research on this security problem. The researchers stated that the issue of third-party dependency is increased in serverless platforms because of the complexity that occurs in deploying cloud services based on users' demands. Serverless computing demands a dynamic allocation of different computer resources. The researchers stated that there are many shortcomings of serverless platforms, and there is a need for proper security solutions to such issues.

C. Solutions to Security Challenges



Serverless Computing

Advantages	Disadvantages
Effortless efficiency	Debugging
Productivity boost	Security
Cost-effective	Vendor limitations
Simplified operations	Response latency

Figure 7: Solutions to Security Challenges in Serverless Computing [22]

To overcome the security issues that occur in serverless computing, there is a need to implement proper mitigation measures. The issue of cold-start attacks can be mitigated with the help of full memory encryption and disabling sleep capabilities. [23] also focused on mitigating this issue. Encrypting RAM helps reduce the possibility of an intruder being able to attain the encryption keys or any other data from the memory through a cold boot attack. This technique mainly requires hardware, applications, or operating system changes. Besides, the computer system will never go into sleep mode if one turns off sleep capabilities. This will help prevent cold boot attacks.

The issue of authorization and authentication in serverless computing can be resolved by implementing IAM (Identity and Access Management) and Least Privilege Principle. [24] also conducted research in this regard. According to the researchers, this principle mainly allows users to execute or read only the necessary resources and files. In this case, time-limited privileges can also be implemented to ensure that users can access sensitive information only for a limited time. The overall benefit is that serverless computing easily mitigates and prevents security issues.

Data security issues in serverless computing can also be mitigated by implementing encryption practices. [25] researched improving encryption in data security in serverless computing. The researchers found that serverless computing is becoming common because of its rapid adoption by tenants and cloud providers due to its flexibility, elasticity, and scalability. However, it encounters security issues and needs proper encryption measures. The researchers developed an efficient and secure access control system for serverless security computing for resource and knowledge sharing with the help of attribute-based encryption. The security analysis revealed that the method proposed by the researchers successfully improved data security in serverless computing.

Implementing proper multi tenancy security measures like resource allocation and segregation strategies is also important. The multi-tenant security model is very crucial in this regard. [26] conducted research on this concept. This model helps firms in protecting their cloud architecture. Properly maintaining and optimising this model is very important; otherwise, it can lead to potential security risks. Multi-tenancy can be of different degrees, such as high, middle, and low. It can provide many benefits to the users, such as effective resource usage, easier deployment and optimized bills.

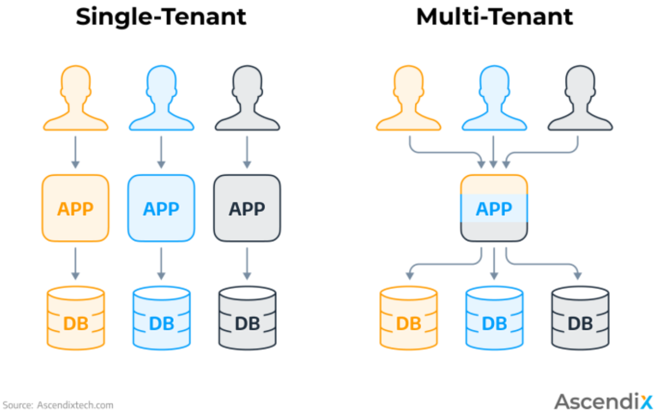


Figure 8: Single-Tenant vs Multi-Tenant [27]

Using real-time monitoring tools and anomaly detection can also help improve monitoring solutions. CSPM (Cloud Security Posture Management) plays a very important role in improving the security of serverless platforms. It mainly relates to a set of practices, technologies, and tools developed to enhance, manage, and assess the security posture of cloud platforms. According to [28], CSPM helps companies address and identify security problems, vulnerabilities, and misconfigurations that can expose their technological infrastructure to probable threats. CSPM also offers consistent automated remediation and monitoring to manage a strong security stance in cloud environments. Moreover, it also helps firms in governance and compliance, risk assessment and identification, real-time monitoring, cost optimization, and automated remediation.

D. Serverless Security Tools and Technologies

Serverless security demands a shift in how companies focus on application security. Rather than developing security around the application, companies should additionally develop security around different functions within the application, which third-party providers provide. According to [29], this extra layer of security helps ensure the least privileged access control and proper application hardening so that every single function does exactly what it is supposed to do. This helps companies maintain compliance and improve their security posture. The researchers stated that Amazon was the first to develop a serverless platform named Lambda in 2014. Today, many other firms offer much more secure serverless computing services.

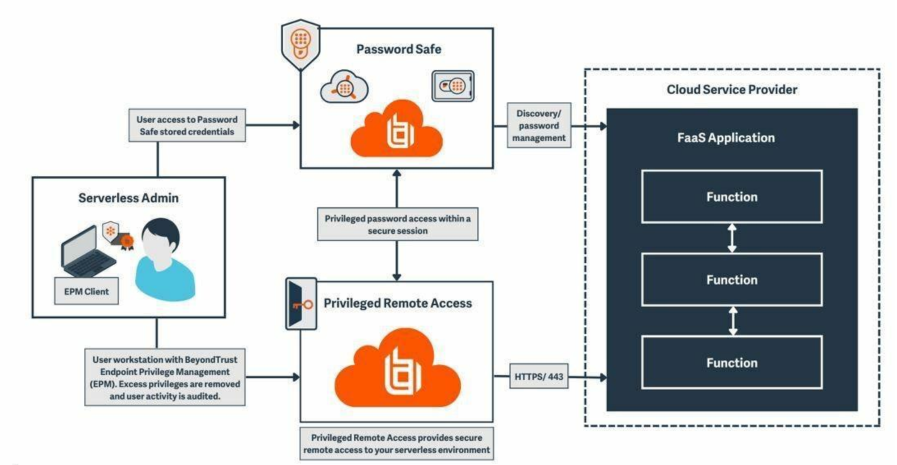

Password Safe
User access to Password Safe stored credentials
Discovery/ password management
Cloud Service Provider
FaaS Application
Function
Function
Function
Serverless Admin
EPM Client
Privileged password access within a secure session
Privileged Remote Access
User workstation with BeyondTrust Endpoint Privilege Management (EPM). Excess privileges are removed and user activity is audited.
HTTPS/ 443
Privileged Remote Access provides secure remote access to your serverless environment

Figure 9: Serverless Security Practices [30]

[31] also conducted research in this regard. They found that the serverless platforms can be a circumscriptive topic, but it is a complex and vast subject. The research focused on different security aspects within the cloud, mobile, and its applications. Serverless computing has improved security measures since it is stateless and ephemeral. Different serverless functions, such as AWS Lambda, operate for a short time and then die. Since they have no memory, long-term security attacks are not risky. Therefore, the overall security of such systems can be improved easily.

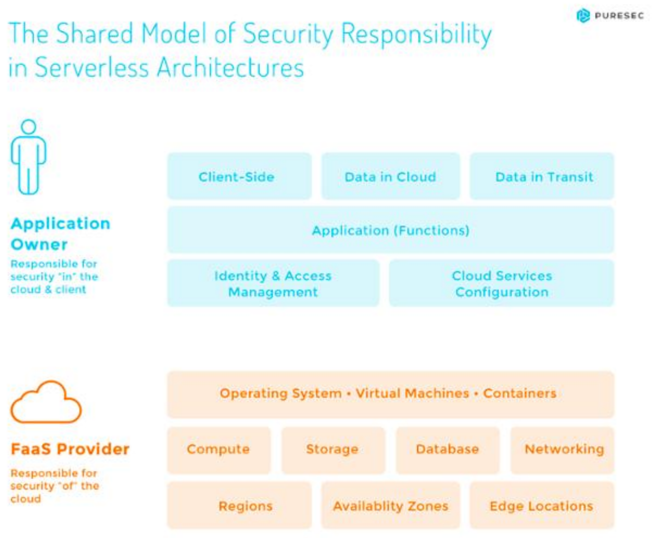

The Shared Model of Security Responsibility in Serverless Architectures
PURESEC
Application Owner
Responsible for security "in" the cloud & client
Client-Side
Data in Cloud
Data in Transit
Application (Functions)
Identity & Access Management
Cloud Services Configuration
FaaS Provider
Responsible for security "of" the cloud
Operating System • Virtual Machines • Containers
Compute
Storage
Database
Networking
Regions
Availablity Zones
Edge Locations

Figure 10: Serverless Security Using the Shared Model [32]

IV. METHODOLOGY/APPROACH

A. *Research Design*

- **Qualitative Approach**

A qualitative research method has been chosen to conduct this research study. It can be defined as a method that includes collecting and analysing non-numerical data to extract important and accurate information. This methodology is chosen to explore the network security challenges within serverless computing environments in detail. With the help of this methodology, this research study can explore the depth of contextual information, which provides a holistic understanding of multiple issues related to serverless network security.

- **Literature Review as Foundation**

Literature review plays a significant role in this research study, which explains the role of different past studies from 2019 to 2023. For this purpose, several scholarly articles and publications have been explored based on themes, and the thematic analysis method was used to conduct the literature review. The purpose of conducting a literature review is to identify the gaps in the research that are helpful for future research studies. Moreover, this process also helps the research design to gain a strong footing, which ensures a thorough and well-informed investigation into the challenges and solutions in network security for serverless computing.

B. *Data Collection Methods*

- **Comprehensive Literature Review**

The comprehensive literature review plays a significant role in collecting data for this research study, including the exhaustive and systematic search for relevant scholarly publications and articles. It also involves the analysis of databases like ScienceDirect, ACM Digital Library, and IEEE Xplore; all of these are up-to-date and high-quality sources to get accurate information. The criteria to find the data are relevance to network security challenges in serverless computing, the credibility of the source, and recent publication dates. Moreover, keywords like solutions, challenges, network security, serverless computing, etc., are used to ensure thorough and targeted exploration of the existing knowledge.

C. *Data Analysis Technique*

- **Thematic Analysis**

A literature review based on thematic analysis has been conducted to collect data for this research study's authentication. It is considered one of the most significant data analysis techniques, which provides an insightful and structured approach for uncovering patterns within the collected data. It can be stated that thematic analysis is the best for identifying, analysing and reporting important themes relevant to network security challenges and solutions in serverless computing. The data is organized in meaningful themes so that the complex issues can be addressed effectively. This approach goes far beyond data summarization because it provides deep insights into the research questions by highlighting important patterns and relationships.

- **Theme Identification Process**

Identifying themes in the literature review is also an important step to be considered, as it involves organising the collected data into meaningful and appropriate themes. For this purpose, the research objectives are considered, and the themes are created based on these objectives related to network security challenges in serverless computing. Accuracy has been ensured by organizing all the gathered data under these significant themes and documenting all the details and findings of each research study to maintain transparency.

- **Results and Discussion**

Studying how to keep serverless computing secure and safe in cloud servers has expressed a lot about the difficulties and its solutions in network marketing. The security challenges recognized include limited visibility, insecure dependencies, cold start attacks, data privacy issues and resource exhaustion. These challenges have encouraged the employment of targeted solutions.

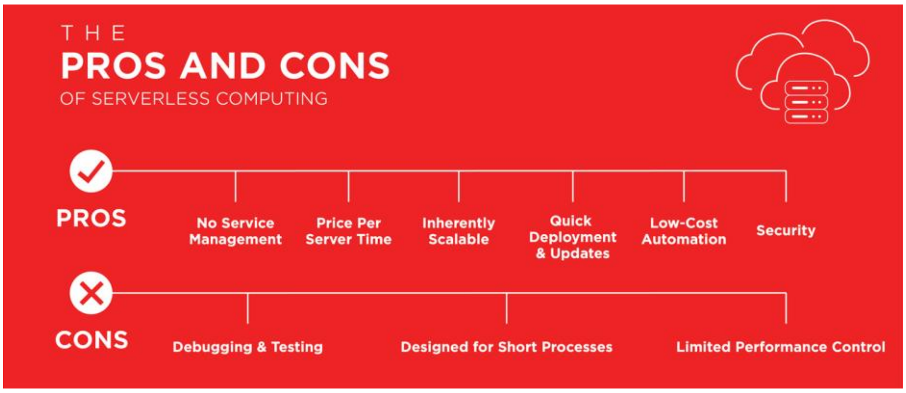


Figure 11: Pros and Cons of Serverless Computing [33]

- **Limited Visibility and Control**

The logging mechanism and strict monitoring have proven effective in response to the limited visibility and control. Implementing cloud-native monitoring tools during the implementation phase has improved the ability to observe serverless computing behaviour [34]. In addition, adding real-time data on the execution of the functions, network interaction and resource usage helps to solve the challenge of limited control. This type of outcome gives power to the organization to properly detect and respond to security incidents and ensures a high level of awareness in the serverless system. Moreover, a successful approach strengthens the security protocols and generates a strong foundation for more informed and effective management of serverless computing systems. It also highlights this cloud-based system's crucial need for visibility and control.

- **Insecure Dependencies**

To solve the challenges of insecure dependencies, the strategy includes regular audits, static code analysis for third-party libraries and updates. Proactive approaches have been proven to reduce weaknesses and secure serverless systems effectively. By carefully monitoring and updating the dependencies from time to time, the organization reduces the number of points where attackers can attack and gain access to sensitive data. This results in more serverless components, reducing the risks of unauthorized access and data loss. This implementation success highlights the importance of a proactive approach and the need for continuous monitoring and management from any external dependencies to secure serverless computing from other harmful access or attackers.

- **Cold Start Attacks**

Continuously facing weaknesses are caused by cold start attackers in the serverless system. It can be stopped by making a serverless system more efficient. Adopting strategies like function warm-up mechanisms and strategic placement has proven very successful [35]. Organizations have minimized the vulnerability during the initial phase, directly enhancing the serverless computing system's security and overall performance. Function warm-up mechanisms include periodically activating the function, ensuring that they are in the warm-up phase and they are ready for rapid execution, which reduces the delays during a cold start. In strategic placement, functions should be distributed in serverless architecture, while factors like anticipated demand and resource allocation should be considered. If these techniques are successful, they will not only increase the security of the system from attackers but also make the most efficient and responsive serverless computing system.

- **Data Privacy and Resilience**

Encryption measures have always proven to be effective when applied to data. Encryption plays an important role in securing data integrity [36]. It makes it unreadable by unauthorized users and secure during transmission. This not only helps in compliance requirements but also injects confidence in the organization and the user about the security of their sensitive information. These successful encryption measures create a reliable defence, adjusting the serverless computing system in the best practice of data security and increasing the overall trust in data security in serverless computing systems.

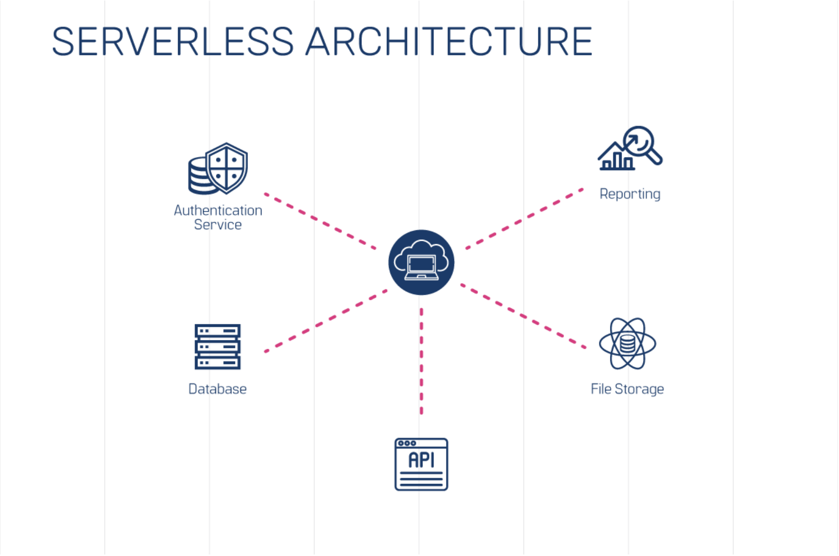


Figure 12: Data Privacy in Serverless Architecture [37]

- **Injection Vulnerabilities**

The successful injecting vulnerabilities include a proactive run time mechanism, especially Web Application Firewalls (WAFs). This strategy has proven highly effective in reducing the risks of injection attacks [38]. The WAFs operate by detecting and blocking the injection attacks; therefore, the security of the serverless environment remains balanced. This step results as an important defence against unauthorized access and data unreliability, which could result from malicious injection attempts. By adding WAFs to the serverless system, the organization increases its overall security, ensuring the reliability and integrity of data.

- **Resource Exhaustion and Denial-of-Service (DoS)**

The charging of serverless systems based on the number of resources being consumed results in facing the challenge of resource exhaustion attacks. The attackers may try to overpower the system by triggering many functions like this, which results in Denial of service and rising costs. The strategic solution is to implement such measures to stop the threats. Applying rate-limiting mechanisms helps in controlling the frequency of function; on the other hand, continuous monitoring shows unusual spikes in the system activity. Implementing billing alerts results in an early warning to the system, which enables a rapid response to potential attacks on the system. In addition, by applying automated scaling policies, it adjusts the resources according to their demand, enhancing the system's overall reliability against resource exhaustion attacks by the attackers. By implementing these steps, the organization can strengthen its serverless system, ensuring efficient resource consumption, effective cost control, and protection against dangerous attempts to take advantage of the platform.

- **Vendor Lock-in Risks**

Using serverless computing generally ties an organization to the specific cloud service providers, which raises concerns about vendor lock-in [40]. The complications of sharing serverless applications between different providers result in the creation of challenges, including the maintenance of consistent security protocols across the cloud system. To solve these challenges, the organization must adopt a multi-cloud strategy where feasible to reduce the risks related to vendor lock-in. This allows the organization to vary its cloud service providers, decreasing dependency on a single vendor and providing flexibility in managing resources. In addition, adopting open standards and confirming the portability of serverless applications can result in a smoother transition between cloud providers. By adopting a multi-cloud approach and prioritizing interoperability, the organizations not only enhance their monitoring flexibility but also decrease their potential challenges and the risks which are related to being bound with only a single cloud service provider in the evolving system of the serverless environment.

V. CONCLUSION

To conclude, this research study has highlighted the methods and strategies used to make computer systems safer, especially when connected to a serverless computing network. It explored the challenges and innovative solutions by focusing on the studies conducted by past researchers related to serverless network security. According to this research study, encryption and strong monitoring are important to overcome such challenges as insecure dependencies and limited control over data and devices connected with the network. Moreover, it highlighted the importance of advanced technologies like AI and blockchain technology so that emerging challenges could be overcome with smart and advanced technologies. All these technologies are helpful in staying alert of upcoming threats in real time. The findings of this research study provide a basis for future researchers to focus on developing innovative strategies so that serverless computing systems can be kept secure and protected.

VI. FUTURE SCOPE

This study provides scope for future researchers to focus on significant factors that could enhance their study regarding challenges and solutions in network security for serverless computing. For instance, they can focus on integrating advanced technologies such as blockchain technology and Artificial Intelligence to explain the security of serverless computing. Future researchers can explore how these emerging technologies can complement existing security measures so that innovative solutions can be developed for the purpose of addressing emerging threats and enhancing serverless systems as a whole.

As modern organizations are moving towards using multi-cloud strategies, it is important to explore security considerations across different cloud providers. This research study enables future researchers to focus on developing advanced mitigating security approaches so that such challenges can be resolved within diverse cloud environments. This will lead to protecting data as well as the applications within the network.

Future studies need to focus on the identification of advanced threats related to security in serverless computing. They must explore new attack vectors and innovative applications that can be used for data breaching and data theft. Moreover, they must also focus on real-time threat intelligence and adaptive security measures that play an important role in helping organizations overcome potential risks in the world of ever-evolving cybersecurity.

REFERENCES

[1] H. Javed, A. N. Toosi and M. S. Aslanpour, "Serverless platforms on edge: a performance analysis," New Frontiers in Cloud Computing and Internet of Things, pp. 165-184, 2022.

[2] M. Mahajan, "Azure Serverless Computing: Architecture, Advantages, Azure Function," 27 September 2023. [Online]. Available: https://k21academy.com/microsoft-azure/az-303/azure-serverless-computing-architecture-advantages-azure-function/.

[3] P. K. Gadepalli, G. Peach, L. Cherkasova, R. Aitken and G. Parmer, "Challenges and opportunities for efficient serverless computing at the edge," 2019 38th Symposium on Reliable Distributed Systems (SRDS), pp. 261-2615, 2019.

[4] C. BasuMallick, "What Is Serverless? Definition, Architecture, Examples, and Applications," 24 March 2022. [Online]. Available: https://www.spiceworks.com/tech/devops/articles/what-is-serverless/.

[5] M. Kumar, "Serverless architectures review, future trend and the solutions to open problems," American Journal of Software Engineering, pp. 1-10, 2019.

[6] V. Yussupov, U. Breitenbücher, F. Leymann and C. Müller, "Facing the unplanned migration of serverless applications: A study on portability problems, solutions, and dead ends," Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing, pp. 273-283, 2019.

[7] M. Golec, G. K. Walia, M. Kumar, F. Cuadrado, S. S. Gill and S. Uhlig, "Cold start latency in serverless computing: A systematic review, taxonomy, and future directions," arXiv preprint arXiv:2310.08437, 2023.

[8] P. Singh, M. Masud, M. S. Hossain, A. Kaur, G. Muhammad and A. Ghoneim, "Privacy-preserving serverless computing using federated learning for smart grids," IEEE Transactions on Industrial Informatics, pp. 7843-7852, 2021.

[9] Paloaltonetworks, "What Is Serverless Security?" 2020. [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-serverless-security.

[10] J. Xiong, M. Wei, Z. Lu and Y. Liu, "Warmonger: inflicting denial-of-service via serverless functions in the cloud," Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, pp. 955-969, 2021.

[11] D. Kelly, F. G. Glavin and E. Barrett, "Denial of wallet—defining a looming threat to serverless computing," Journal of Information Security and Applications, p. 102843, 2021.

[12] Cloudflare, "What is a denial-of-service (DoS) attack?" 2020. [Online]. Available: https://www.cloudflare.com/en-gb/learning/ddos/glossary/denial-of-service/.

[13] G. A. S. Cassel, V. F. Rodrigues, R. da Rosa Righi, M. R. Bez, A. C. Nepomuceno and C. A. da Costa, "Serverless computing for Internet of Things: A systematic literature review," Future Generation Computer Systems, pp. 299-316, 2022.

[14] Y. Li, Y. Lin, Y. Wang, K. Ye and C. Xu, "Serverless computing: state-of-the-art, challenges and opportunities," IEEE Transactions on Services Computing, pp. 1522-1539, 2022.

[15] Fortinet, "What Is Serverless Computing?," 2020. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/serverless-computing.

[16] K. Solaiman, "Novel architecture for mitigating cold start problem in serverless computing," 2023.

[17] X. Li, X. Leng and Y. Chen, "Securing Serverless Computing: Challenges, Solutions, and Opportunities," IEEE Network, 2022.

[18] A. Kumari, M. K. Patra and B. Sahoo, "Data Controlling and Security Issues in Cloud: A Step Towards Serverless," Perspectives on Social Welfare Applications' Optimization and Enhanced Computer Applications, pp. 105-124, 2023.

[19] R. Kolodiy, "Importance of Security in Serverless Technologies," 31 March 2022. [Online]. Available: https://www.techmagic.co/blog/serverless-security-main-threats-and-how-to-overcome-them/.

[20] J. Stojkovic, T. Xu, H. Franke and J. Torrellas, "MXFaaS: Resource Sharing in Serverless Environments for Parallelism and Efficiency," Proceedings of the 50th Annual International Symposium on Computer Architecture, pp. 1-15, 2023.

[21] E. Marin, D. Perino and R. Di Pietro, "Serverless computing: a security perspective," Journal of Cloud Computing, pp. 1-12, 2022.

[22] I. Sharma, "Serverless Computing: Advantages and Disadvantages," 2020. [Online]. Available: https://www.tatvasoft.com/outsourcing/2022/11/benefits-of-serverless.html.

[23] A. Kumari and B. Sahoo, "ACPM: adaptive container provisioning model to mitigate serverless cold-start," Cluster Computing, pp. 1-28, 2023.

[24] W. Wu and W. C. Feng, "Game to dethrone: The least privilege CTF," IEEE 6th International Conference on Smart Cloud (SmartCloud), pp. 132-137, 2021.

[25] A. Arulprakash and K. Sampath Kumar, "Improved Encryption Towards Data Security in Serverless Computing," Journal of Computational and Theoretical Nanoscience, pp. 5256-5260, 2020.

[26] A. A. Prakash and K. S. Kumar, "Cloud serverless security and services: a survey," Applications of Computational Methods in Manufacturing and Product Design: Select Proceedings of IPDIMS, pp. 453-462, 2022.

[27] D. Torkut, "How to Mitigate Risks Of Your Multi-Tenant Security Model," 17 May 2023. [Online]. Available: https://ascendixtech.com/multi-tenant-security-model/.

[28] R. Loaiza Enriquez, "Cloud Security Posture Management/CSPM) in Azure," 2021.

[29] W. O'Meara and R. G. Lennon, "Serverless computing security: Protecting application logic," 31st Irish Signals and Systems Conference (ISSC), pp. 1-5, 2020.

[30] B. Casey, "Serverless Security Best Practices," 12 April 2023. [Online]. Available: https://www.beyondtrust.com/blog/entry/serverless-security-best-practices.

[31] N. Mateus-Coelho and M. Cruz-Cunha, "Serverless Service Architectures and Security Minimals," 10th International Symposium on Digital Forensics and Security (ISDFS), pp. 1-6, 2022.

[32] P. a. P. T. Center, "Serverless Security: Everything You Need to Know About It," 11 July 2019. [Online]. Available: https://www.plugandplaytechcenter.com/resources/serverless-security-everything-you-need-know-about-it/.

[33] Adastracorp, "The Pros and Cons of Serverless Computing," 12 JULY 2020. [Online]. Available: https://adastracorp.com/insights/the-pros-and-cons-of-serverless-computing/.

[34] M. V. L. N. Venugopal and C. R. K. Reddy, "Serverless through cloud-native architecture," Int. J. Eng. Res. Technol, pp. 484-496, 2021.

[35] Z. Li, L. Guo, J. Cheng, Q. Chen, B. He and M. Guo, "The serverless computing survey: A technical primer for design architecture," ACM Computing Surveys (CSUR), pp. 1-34, 2022.

[36] B. Seth, S. Dalal, V. Jaglan, D. N. Le, S. Mohan and G. Srivastava, "Integrating encryption techniques for secure data storage in the cloud," Transactions on Emerging Telecommunications Technologies, p. 4108, 2022.

[37] S. Addeppally, "Serverless Architecture – The What, When and Why," 2020. [Online]. Available: https://www.cloudnowtech.com/blog/serverless-architecture-the-what-when-and-why/.

[38] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," Electronics, p. 1333, 2023.

[39] C. Ngo, P. Wang, T. Tran and S. Chung, "Serverless Computing Architecture Security and Quality Analysis for Backend Development," Journal of The Colloquium for Information Systems Security Education, pp. 8-8, 2020.

[40] D. Harauzek, "Cloud Computing: Challenges of cloud computing from business users perspective-vendor lock-in," 2022.

[41] Y. Papazov, G. Sharkov, G. Koykov and C. Todorova, "Managing Cyber-Education Environments with Serverless Computing," Digital Transformation, Cyber Security and Resilience of Modern Societies, pp. 49-60, 2021.