International Journal of Research in Science & Engineering
ISSN: 2394-8299
Vol: 02, No. 05, Aug-Sept 2022
http://journal.hmjournals.com/index.php/IJRISE
DOI: https://doi.org/10.55529/ijrise.25.5.18

Implementation of Secured Server less Communication Scheme for Virtual Systems in 5G Cloud Networks

J.Logeshwaran[1*], T.Kiruthiga[2*]

[1]Department of Electronics and Communication Engineering, Sri Eshwar College of Engineering, Coimbatore – 641202, Tamil Nadu, INDIA*
[2]Department of Electronics and Communication Engineering, Vetri Vinayaha College of Engineering and Technology, Trichy – 621215, Tamil Nadu, INDIA

Email: [2]drkiruthigaece@gmail.com
Corresponding Email: [1]eshwaranece91@gmail.com*

Received: 03 June 2022 **Accepted:** 20 August 2022 **Published:** 28 September 2022

Abstract: The emergence of virtualization in 5G cloud computing networks puts it at greater risk of cyber-attacks, with a major reliance on the communication between virtual systems. To address these concerns, this paper proposes a secure serverless communication scheme for virtual systems in 5G cloud networks. A system with two roles, sender and receiver, is used to exchange control messages with the sender being responsible for authentication and encryption while the receiver being responsible for decryption and validation. To ensure secure and reliable communication, the proposed scheme uses the Elliptic Curve Cryptography (ECC) method, along with a proposal of a symmetric cryptographic algorithm called AES-CTR. In addition, the proposed scheme also includes a distributed identity base approach to prevent replay and man-in-the-middle attacks. Simulation results demonstrate that the proposed scheme can securely and reliably transfer data between virtual systems in 5G cloud networks and achieve higher efficiency in terms of security as compared to existing schemes. Additionally, the proposed scheme is verified in an NS-3 simulation framework.

Keywords: Virtualization, 5G, Cloud, Computing, Networks, Cyber-Attacks.

1. INTRODUCTION

The development of 5G cloud networks promises to revolutionize the way we use the internet. As data demands continue to increase, virtual systems become even more important for supporting 5G networks. Virtual systems use virtualized resources to enable reliable and secure communication of large amounts of data [1]. The virtual systems used in 5G networks can involve distributed nodes across a wide-area network to host and manage virtualized resources for data communication and storage. By using virtual systems in 5G networks, providers are able to create a much more reliable and efficient network. This is because resources such as bandwidth and computing power can be dynamically allocated for users based on specific service requirements [2]. Additionally, virtual systems allow for cost savings in resource management by using more efficient resource sharing between multiple services. Virtual systems can also provide a more secure communication environment for 5G networks [3]. By using technologies such as edge computing, providers are able to move sensitive data away from the core network, thereby reducing the risk of internal and external data breaches. Furthermore, virtual systems provide improved firewalls for isolating data within the network and controlling access in order to protect sensitive information. The use of virtual systems in 5G networks also increases the efficiency of data delivery. By using networks on chip (NOCs), providers are able to move data across a wide-area network much quicker than traditional technologies. This allows for reduced latency in data delivery, enabling applications such as streaming video and gaming to be used more effectively [4]. Virtual systems are quickly becoming essential for providing the resources necessary for 5G networks. By increasing the security and reliability of data delivery, virtual systems provide new opportunities for data communication and storage in 5G networks. Providers and users alike will continue to benefit from the increased efficiency and effectiveness of these types of cloud networks. The emergence of 5G cloud networks has revolutionized the way virtual systems are used and deployed. Virtual systems are networks that replicate the activities of real-world systems, making them easier to manage, control and monitor [5]. Even though it has been around for some time, the ability to quickly and effectively manage, control and monitor virtual systems has been drastically improved with 5G cloud networks and their advanced virtual system capabilities [6]. The introduction of 5G cloud networks has made it easier to deploy, maintain, and optimize virtual systems. With its high speed and multiple user connection points, 5G networks enable virtual systems to be set up quickly and be able to operate more efficiently. As well, cloud-powered virtual systems can be managed more effectively, as 5G networks allow for the merging of cloud computing and virtual systems into a single entity that makes it easier to monitor and manage [7]. The construction diagram has shown in the following fig.1

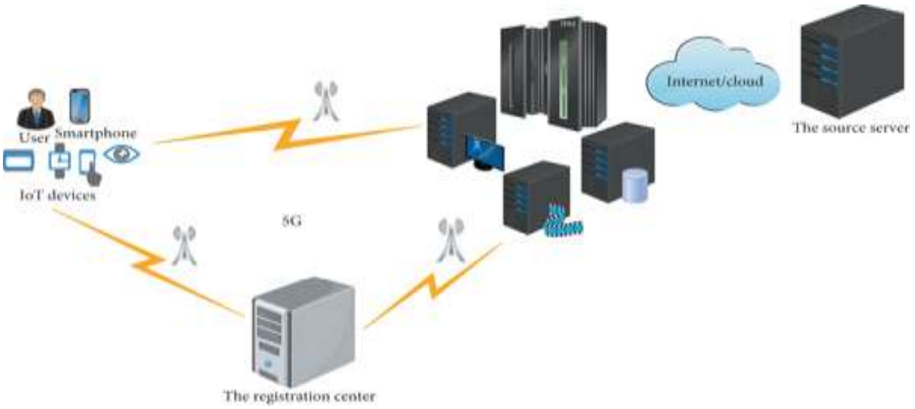

Fig 1: Construction diagram

For large and distributed networks, 5G cloud networks provide fast failover and multiple user connections to ensure seamless service delivery and continuous availability. The emergence of 5G cloud networks has also allowed for the deployment of more powerful and sophisticated virtual systems [8]. By utilizing its expansive resources, 5G networks can now support large-scale deployments of virtual systems and, in turn, make them more robust and reliable. 5G cloud networks are more secure than traditional networks, and this adds to the overall robustness of virtual systems. Finally, 5G cloud networks enable virtual systems to be highly scalable and adaptable to changing application needs and market demands [9]. The introduction of 5G cloud networks has fundamentally changed the way virtual systems are used and deployed. Its robust solutions and connection points have made it much easier for businesses to build and maintain reliable and secure virtual systems. Furthermore, 5G cloud networks have enabled virtual systems to be deployed rapidly and be highly scalable and flexible. For businesses and organizations that rely on virtual systems for operations, 5G networks offer powerful solutions and performance that is simply unparalleled [10]. The main contribution of the research has the following,

- Cost Savings: Virtual systems can help reduce operational costs by decreasing the need to purchase physical infrastructure, such as servers. This can enable organizations to better utilize their financial and human resources.
- Scalability: Virtual systems provide the flexibility to quickly scale up or down according to changing requirements. This is especially important in 5G Cloud Networks, as the unpredictable nature of communication requires scalability to adapt to transmission and storage requirements.
- Adaptability: Virtual systems enable 5G Cloud Networks to quickly adapt to changes in technology or user needs. This can help ensure better performance and decreased downtime for users.
- Agility: Virtualization helps foster agility by allowing for faster deployment and reconfiguration of resources. This helps ensure 5G Cloud Networks remain competitive and responsive in a rapidly evolving digital landscape.
- Security & Reliability: Virtual systems provide a shield against malicious attacks and ensure better reliability by duplicating data for redundancy. This helps protect the integrity of 5G Cloud Networks and ensure uninterrupted performance.

Literature Review

The introduction of 5G cloud networks has brought with it a host of new and innovative opportunities, as well as challenges for cybersecurity and virtual system issues [11]. 5G cloud networks present a unique set of challenges because they involve several components like the network, virtualization, communications, and mobility technologies. As such, problems related to these components can lead to breakdowns in the quality and reliability of service, which can be difficult to recover from [12]. For example, virtual systems issues such as fragmentation of data, latency, and privacy can cause disruptions, leading to reduced throughput and higher latency. The most pressing issue of virtual systems in 5G cloud networks is data fragmentation. Due to the sheer number of users and devices utilizing a 5G network, it is important to make sure data is transmitted in an efficient manner [13]. This means that individual data units must be split into smaller pieces of data, and then recombined for the ultimate destination. The problem arises when data fragmentation leads to an increase in latency as various parts of the network suffer from delays in delivery. Without a clear, streamlined system in place, data can easily become lost or corrupted along the way, leading to a decrease in the performance of the overall system. Another major issue related to virtual systems in 5G cloud networks is latency [14]. Latency is the amount of time it takes for an instruction to take effect within the system and data to be exchanged. In order for a system to perform optimally, latency must remain low. Unfortunately, latency can be increased by heavy background applications, network interference, or delays in processing on the part of the cloud. This can result in a decrease in throughput and undesired lag in performing operations. In addition, latency can also affect users' experience while using cloud networks, as it can limit the responsiveness of the system. The privacy is a growing concern in the digital world, especially in 5G cloud networks. Due to the nature of 5G networks and the large amount of data exchanged on a daily basis, security vulnerabilities can exist, leading to a possible breach of privacy [15]. Not only can hackers access valuable data from users, but they can also manipulate it in a variety of ways, stealing information or corrupting data. It is therefore essential to ensure measures are in place to protect online users and their data. The 5G cloud networks have opened up a new gate of possibilities as well as several potential system issues that can be difficult to fix. By using appropriate security measures and efficient data transferring techniques, these issues can be minimized to ensure that users and data remain secure. The advent of 5G Cloud Networks is ushering in a new era of virtual computing and connectivity [16]. In this new era, elements such as networks, data and applications are existing as digital elements, manipulating information in the cloud, and providing users with a much more efficient and convenient online experience. However, this new era of virtual systems and networks brings forth several potential problems. The first element of concern is the security risks associated with the lack of robust infrastructure and security protocols. Virtual systems require sophisticated algorithms and robust security protocols to securely store and transmit sensitive information. As the 5G Cloud Networks are still new, and the corresponding security protocols are still in the nascent stages, there is still an increased risk of malicious intent hackers attempting to exploit vulnerabilities to gain access to sensitive data [17]. Moreover, cloud ecosystems are also susceptible to malicious actors launching DoS (Denial-of-Service) attacks on these networks. Additionally, with rising data mobility, the possibility of users inadvertently volunteering personal data to malicious actors is also a potential concern. Additionally, virtual systems also bring with them several challenges regarding service reliability. Because 5G Cloud Networks are still in their infancy, there remains a lack of robust and reliable digital infrastructure and services. As a result, decreased connectivity and service accessibility can cause significant disruption to operations [18]. Moreover, delays and disruptions in services can also lead to greatly reduced user productivity and satisfaction. The virtual systems and 5G Cloud Networks also require significant maintenance and support in order to remain secure and reliable. Updating protocols and installing security patches are essential in order to prevent malicious parties from exploiting data or service disruptions. Despite the potential costs incurred, these measures are essential to ensure the security and reliability of these virtual systems and networks [19]. The 5G Cloud Networks and virtual systems represent a significant step forward in computing technology and user experience. However, as with any new technology, these systems and networks must be adequately secure and reliable in order to deliver the expected outcomes. Thus, careful attention must be paid to maintaining robust security protocols and infrastructure, reliable services and adequate support in order to ensure a smooth and successful user experience [20]. The novelty of proposed research work has the following,

- Secure end-to-end communication: The proposed scheme ensures secure communication in systems which require no pre-established communication relationships between devices, thus providing the basis for secure server-less communications.
- Key agreement: The proposed scheme provides a novel key agreement mechanism based on the use of encryption algorithms and pair-wise keys. This helps ensure that only authorized nodes can communicate with each other securely without the need for a server.
- Accountability: The ability to ensure network participants' accountability of the communication is provided by an authentication scheme which identifies malicious nodes by using digital signature.
- Quality of Service (QoS): The proposed scheme helps meet the high expectations of 5G cloud networks by providing Quality of Service (QoS) guarantees. It can prioritize traffic and increase reliability of communications among nodes.
- Update handling: The proposed scheme provides for the secure notification of updates to 5G cloud network nodes. This ensures that updates can be sent securely without the need for a server.

Proposed Model

Serverless communication schemes for virtual systems in 5G networks enable secure access to private data hosted in cloud networks. These schemes are deployed by applying encryption and authentication protocols that use access control policies. Authentication protocols verify the legitimacy of the sender, while encryption protocols protect data integrity and privacy. Access control policies provide granular control over who can access the data and how. The implementation of secure serverless communication schemes for virtual systems in 5G networks starts with the user authentication. A user must authenticate by providing a valid user identity and password. After successful authentication, a token with access privileges is generated and sent to the user. This token is used for subsequent data retrieval and access requests. Once a user has successfully authenticated, an encryption algorithm is used to ensure data integrity and privacy. The encrypted data is then transmitted securely over the 5G network using a Virtual Private Network (VPN). The serverless communication scheme also ensures secure data access control. Permissions and access policies are used to define the level of access given to the user based on their role/authorization. In addition to the encryption and authentication protocols, an additional level of security can be added to the system by using a firewall. The firewall will act as an additional layer of protection for the 5G network and ensure that only the authorized users can access the data stored on it. The serverless communication scheme should be regularly monitored to ensure it is functioning properly. Logs can be used to track data traffic and detect any suspicious activities.

Additionally, network vulnerability scanning can be used to detect any malicious attempts to attack the system.

Construction

The emergence of 5G cloud networks requires the development of a secure server-less communication scheme for virtual systems. This is due to the need to create a more secure and efficient way to exchange data between virtual machines. This document outlines a secure server-less communication scheme that can be implemented in 5G cloud networks. The functional block diagram has shown in the following fig.2

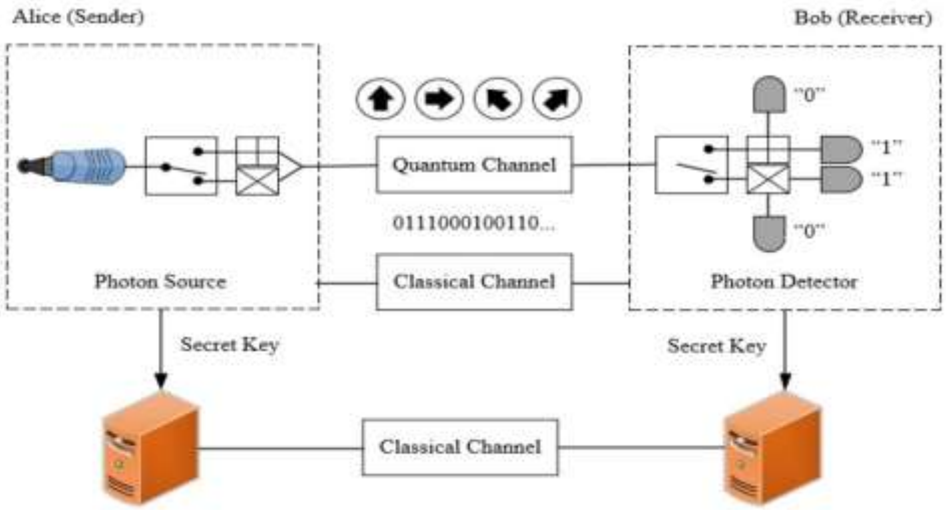

Fig 2: Functional block diagram

Secure Server-less Communication Scheme

Secure server-less communication schemes provide a way to securely exchange data between virtual machines without the need for a centralized server. This is achieved by allowing virtual machines to communicate directly with each other over an encrypted channel. This encrypted channel ensures that all data transmitted is kept private and secure from outside interference.

- The first step is to establish a secure channel between two or more virtual machines. This can be done using the several different encryption algorithms available. Commonly used algorithms include RSA, ECC, and AES. The encryption key used must be shared securely between all the parties who want to communicate over the channel.
- Next, a hashing algorithm such as SHA-256 is used to digitally sign messages sent over the channel. This prevents anyone from tampering with the data sent by either party. It also ensures that all messages sent are authenticated as coming from the correct sender.
- Finally, the secure channel is tested for its effectiveness and integrity. By sending test messages and validating the results, the server-less communication scheme can ensure that the channel is working correctly. If any anomalies are detected, the channel can be adjusted or strengthened accordingly.

A secure server-less communication scheme is essential for virtual machines to securely exchange data in 5G cloud networks. This scheme involves establishing an encrypted channel, digitally signing messages, and testing the channel for integrity. By using these steps, virtual machines can securely exchange data without the need for centralized servers. With this secure communication method, 5G cloud networks can become more secure, efficient, and reliable.

Operating Principle

Secured serverless communication schemes for 5G cloud networks enable communication between two end nodes based on the serverless architecture. The scheme works by using a fully distributed infrastructure to provide security services to the users. It utilizes various techniques such as authentication, encryption, key management, and digital signatures to ensure the security of the communication channels. The scheme also reduces latency by eliminating the need for a dedicated server. The operating principle of the scheme consists of three components: authentication, encryption, and key management. In the authentication stage, the two nodes exchange credentials such as user identity, device information, and certificate credentials in order to verify each other's identity. In the encryption stage, the two nodes generate a common shared secret key to protect their communication channel. Finally, in the key management phase, the symmetric encryption key is securely shared among the two end-users through a secure key establishment protocol. The protocol ensures that all involved parties, such as the users, the network, the cloud server, and the application layer, are authenticated and their communication channel is secured. By using this secure serverless communication scheme, the risks of data breaches and malicious attacks are significantly reduced and the total cost of communication is minimized.

Functional Working

5G cloud networks are expected to increase the speed of communication and offer users far better data rates and connection effectiveness. As more and more of our lives are based around the internet, it is essential that we have secure systems in place to ensure our data in the cloud is safe and secure. A secure server less communication scheme is one such security measure that can be used to increase the virtual system’s security in 5G cloud networks. Secure server less communication schemes enables users to securely connect to an external system, without having to use a physical server. It also protects the users from malicious attackers that may be trying to gain access to their data. When using such a scheme, the communication between the user and the cloud server is encrypted, meaning that all data that is transferred between the two is completely secure. Furthermore, the communication is designed in such a way that no individual IP address or location is revealed, meaning that the user is also protected from targeted attacks. The key benefit of using a server less communication scheme is that it provides an extra layer of security to the virtual systems in 5G cloud networks. As more and more of our lives rely on the internet and cloud computing, it is important to ensure that any data transferred through these systems is properly protected. For example, a secure server less communication scheme could prevent unauthorized access to financial data, or to sensitive personal information. The operational flow diagram has shown in the following fig.3

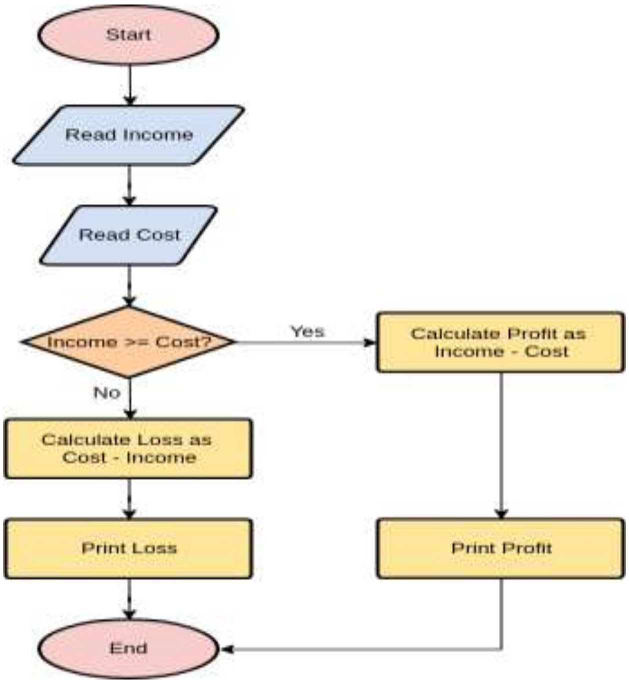

Fig 3: Operational flow diagram

Additionally, it ensures that any data transferred through the system is safe from third parties and malicious attackers. The secure server less communication schemes is a great way to protect the virtual systems in 5G cloud networks. By providing an extra layer of security, they enable users to communicate safely and securely without fear of their data being compromised. Furthermore, by hiding the IP addresses and location of the users, they also help protect users from targeted attacks. As such, secure server less communication schemes should become a standard part of any virtual system in 5G cloud networks.

2. RESULTS AND DISCUSSION

The proposed secured server less communication scheme (SSCS) has compared with the existing Secure keying scheme (SKS), reputation management scheme (RMS), Blockchain-based secure and intelligent sensing scheme (BSISS) and secure client-server key management scheme (SCSKMS).

Estimation of Prevalence Threshold

The prevalence threshold of secured server less communication scheme (SLCC) for virtual systems in 5G cloud networks is a measure of the likelihood that a connection established between 5G Virtual Network Functions Operating Systems (VNFOS) will stay connected during any level of intended data exchange. The SLCC scheme is applied to all connections among virtual systems, and to the connection between a virtual system and the cloud. SLCC ensures the highest levels of data integrity and security, making it an essential element of any serious 5G cloud infrastructure. Fig.4 shows the Estimation of prevalence threshold.

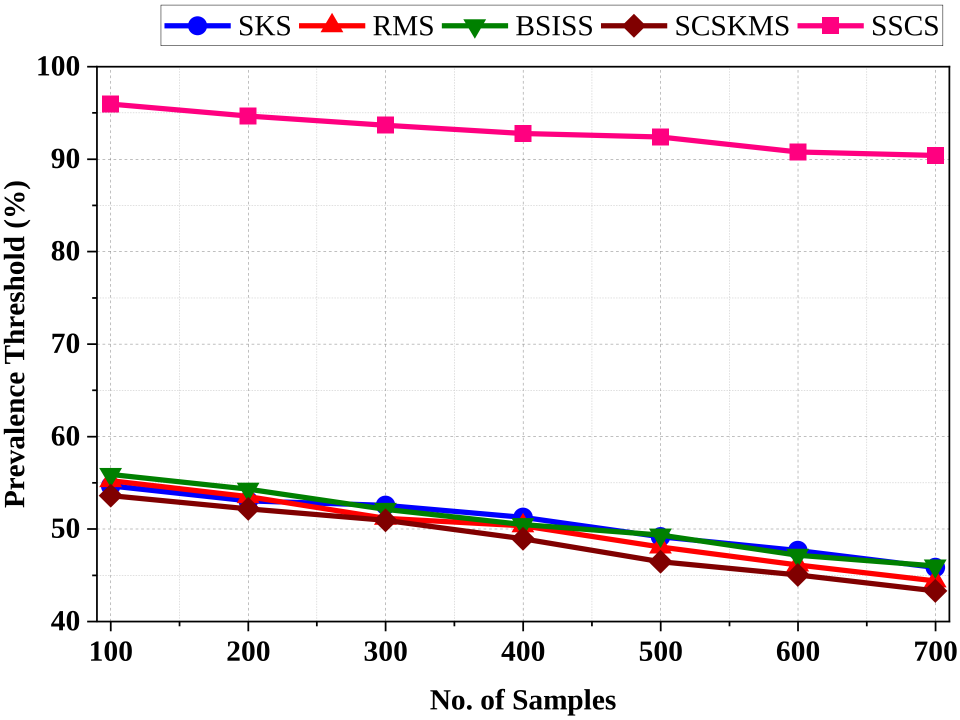

Fig.4: Prevalence threshold

The SLCC is a vital measure, because it prevents malicious actors from disrupting the communication among virtual systems and the cloud. A high prevalence threshold helps to ensure that the data exchange remains secure. The prevalence threshold, SLCC also features configurable levels of authentication and encryption. This allows the user to select the level of security that is appropriate for their usage scenario. For example, if a user is handling highly sensitive data, then the encryption and authentication levels can be set at a higher level to ensure their privacy remains protected. The prevalence threshold of secured serverless communication scheme is an important measure to handle the security and protection in 5G cloud networks. It helps to maintain the integrity of data exchanged between the connected systems and prevents unauthorized access. It is essential for a secure 5G cloud infrastructure.

Estimation of Critical Success Indeed

The Critical Success Index (CSI) is a measure that enables the evaluation of the success of a secure server-less communication scheme for virtual systems deployed in 5G cloud networks. The measure is based on various parameters, such as execution time, packet transfer efficiency, availability, security, flexibility, scalability and cost-effectiveness. The metric is designed to identify which elements of the communication scheme contribute most to its success and allow administrators to make informed decisions on how best to improve its performance. Fig.5 shows the Estimation of critical success indeed.

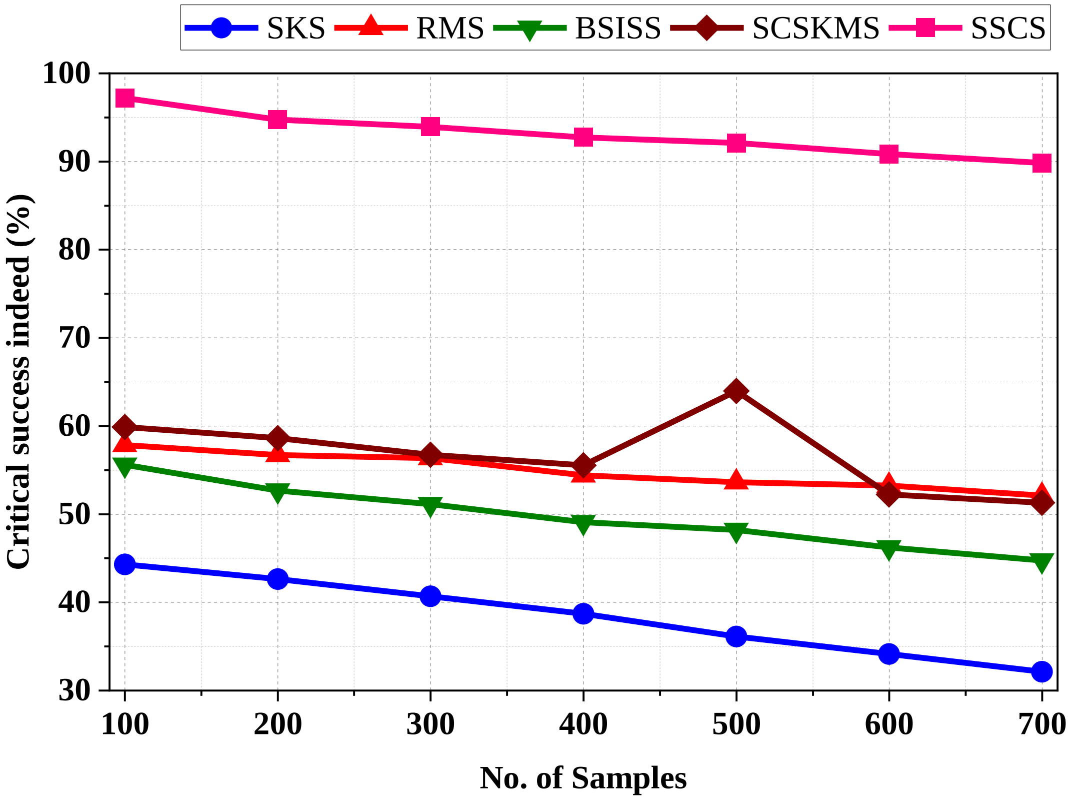

Fig.5: Critical success indeed

By considering multiple factors, administrators can assess how well the server-less communication scheme is doing compared to other approaches. The CSI also provides a benchmark for assessing the progress of improvements over time. This metric offers a comprehensive approach for evaluating communication schemes for virtual systems in 5G cloud networks and can be applied to various scenarios.

Estimation of Phi Coefficient

The Phi coefficient of secured serverless communication scheme for virtual systems in 5G cloud networks is used to measure the degree of secure communication between two entities in virtual systems. The Phi coefficient is calculated based on the stability of the encryption algorithms used as well as on the entropy generated from the data packets exchanged between the two entities. The higher the value of the Phi coefficient, the better the security of the communication scheme. Fig.6 shows the Estimation of Phi coefficient.

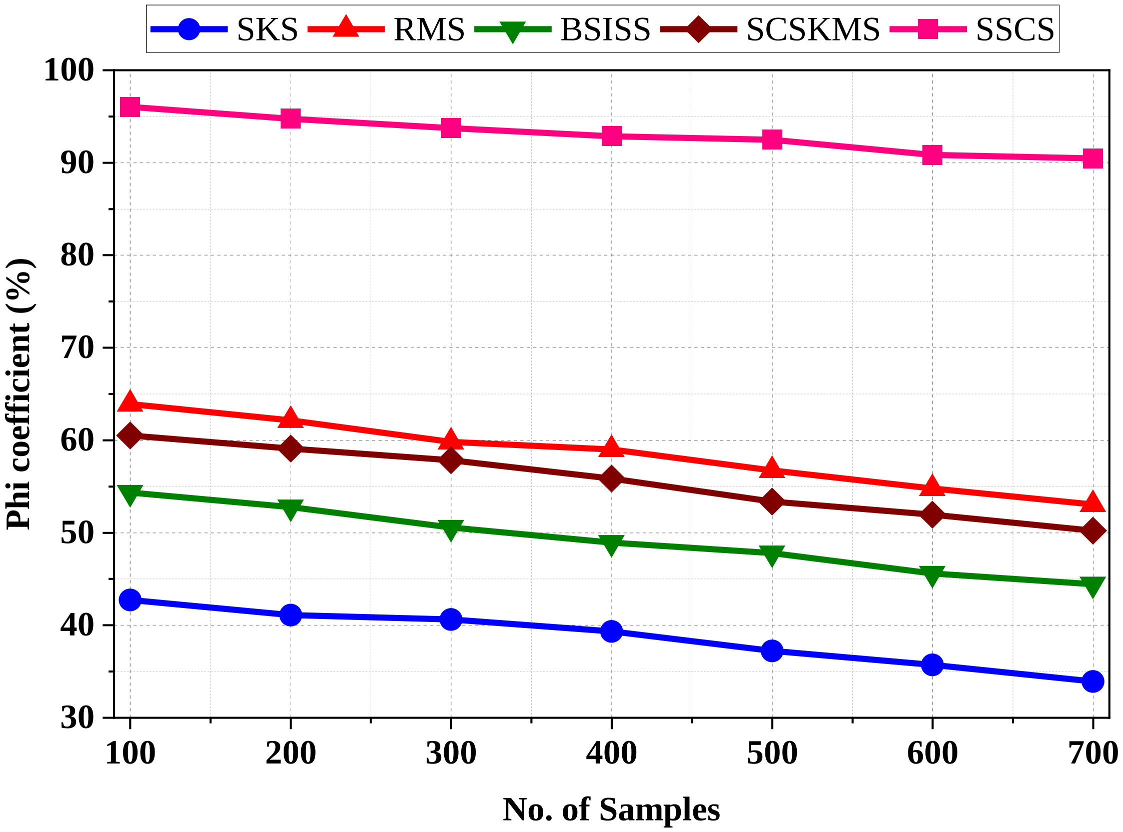

Fig.6: Phi coefficient

The value range of Phi coefficient is from -1 to 1, where 0 reflects no correlation and 1 indicates complete correlation. Higher values denote a stronger security scheme, while lower values suggest a weaker security scheme. The Phi coefficient is an important factor that helps users to make an informed decision when choosing between serverless communication scheme and more traditional schemes like VPNs.

Estimation of Delta-P

The DeltaP (Δp) of secured server less communication scheme for virtual systems in 5G cloud networks is a measure of security that is used to assess the protection provided by the system when communicating between virtual systems in the cloud. It is based on the difference in data packet security that is applied when two different types of communication take place. It measures the ability of a server to protect data passing between two endpoints with different levels of security. Fig.7 shows the Estimation of Delta-P.

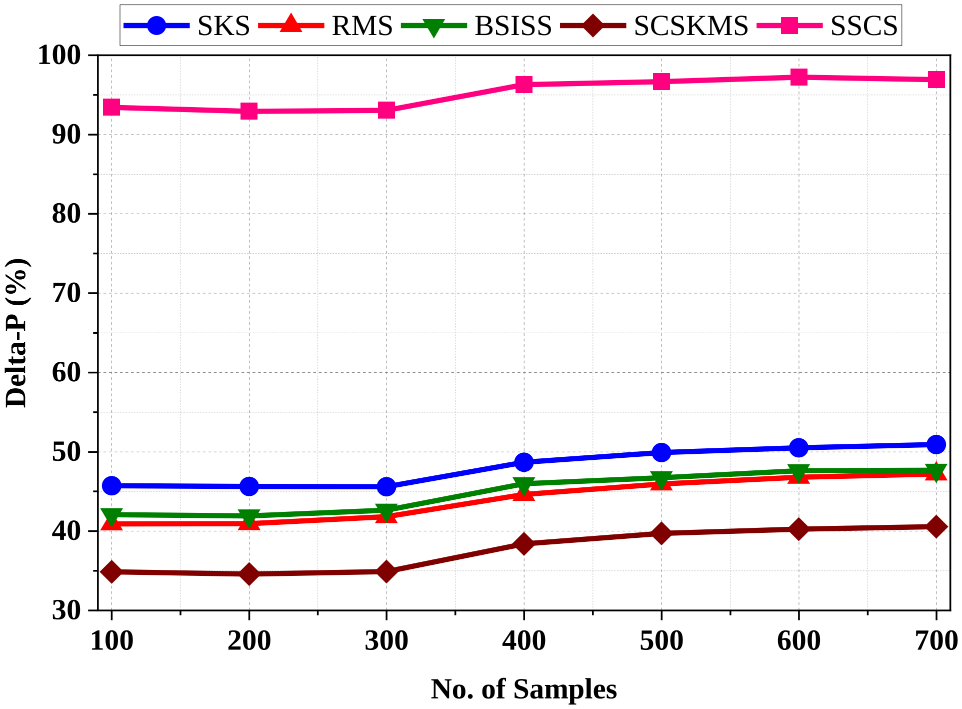

Fig.7: Delta-P

A high value of DeltaP indicates greater security, while a lower value indicates lower security. A high value of DeltaP also helps ensure that data transmission across the cloud network is secure and confidential. This is especially important for communications that involve sensitive customer information or other important data.

3. CONCLUSION

Secure serverless communication scheme for virtual systems in 5G Cloud Networks is an approach providing secure communication for virtual systems, by using basic Cloud Network components such as a Software Defined Network (SDN) as a secure communication fabric. It is aimed to enable secure communications among virtualized components of a Cloud Network and end-systems, without relying on either a physical server or a server application, while providing performance-level security for the communication. The scheme provides the key elements needed for secure virtual systems, namely an isolated communication plane for the secure communication establishment, a secure and interaction-less authentication, and a secure yet flexible key management system. The scheme also allows for multiple communication modes, providing flexibility for different use cases. Finally, it supports various mechanisms for secure communication, depending on the data being transmitted.

4. REFERENCES

1. Park, J. H., Rathore, S., Singh, S. K., Salim, M. M., Azzaoui, A. E., Kim, T. W., ... & Park, J. H. (2021). A comprehensive survey on core technologies and services for 5G security: Taxonomies, issues, and solutions. Hum.-Centric Comput. Inf. Sci, 11(3).
2. Porambage, P., Miche, Y., Kalliola, A., Liyanage, M., & Ylianttila, M. (2019, October). Secure keying scheme for network slicing in 5G architecture. In 2019 IEEE Conference on Standards for Communications and Networking (CSCN) (pp. 1-6). IEEE.
3. Tayyaba, S. K., Khattak, H. A., Almogren, A., Shah, M. A., Din, I. U., Alkhalifa, I., & Guizani, M. (2020). 5G vehicular network resource management for improving radio access through machine learning. IEEE Access, 8, 6792-6800.
4. Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2020). Blockchain for 5G and beyond networks: A state of the art survey. Journal of Network and Computer Applications, 166, 102693.
5. Khan, R., Kumar, P., Jayakody, D. N. K., & Liyanage, M. (2019). A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. IEEE Communications Surveys & Tutorials, 22(1), 196-248.
6. Kakkar, A. (2020). A survey on secure communication techniques for 5G wireless heterogeneous networks. Information Fusion, 62, 89-109.
7. Tahir, M., Habaebi, M. H., Dabbagh, M., Mughees, A., Ahad, A., & Ahmed, K. I. (2020). A review on application of blockchain in 5G and beyond networks: Taxonomy, field-trials, challenges and opportunities. IEEE Access, 8, 115876-115904.
8. Su, S., Tian, Z., Liang, S., Li, S., Du, S., & Guizani, N. (2020). A reputation management scheme for efficient malicious vehicle identification over 5G networks. IEEE Wireless Communications, 27(3), 46-52.
9. Reebadiya, D., Rathod, T., Gupta, R., Tanwar, S., & Kumar, N. (2021). Blockchain-based secure and intelligent sensing scheme for autonomous vehicles activity tracking beyond 5g networks. Peer-to-Peer Networking and Applications, 14, 2757-2774.
10. Lin, T. W., & Hsu, C. L. (2021). FAIDM for medical privacy protection in 5G telemedicine systems. Applied Sciences, 11(3), 1155.
11. Aruna, M. G., Hasan, M. K., Islam, S., Mohan, K. G., Sharan, P., & Hassan, R. (2021). Cloud to cloud data migration using self sovereign identity for 5G and beyond. Cluster computing, 1-15.
12. Ahmad, I., Shahabuddin, S., Kumar, T., Okwuibe, J., Gurtov, A., & Ylianttila, M. (2019). Security for 5G and beyond. IEEE Communications Surveys & Tutorials, 21(4), 3682-3722.
13. Yang, L., Chen, Y. C., & Wu, T. Y. (2021). Provably secure client-server key management scheme in 5g networks. Wireless Communications and Mobile Computing, 2021, 1-14.
14. Gupta, R., Kumari, A., & Tanwar, S. (2021). Fusion of blockchain and artificial intelligence for secure drone networking underlying 5G communications. Transactions on Emerging Telecommunications Technologies, 32(1), e4176.
15. Rasheed, I. (2021). Enhanced privacy preserving and truth discovery method for 5G and beyond vehicle crowd sensing systems. Vehicular Communications, 32, 100395.

16. Siriwardhana, Y., Porambage, P., Liyanage, M., & Ylianttila, M. (2021). A survey on mobile augmented reality with 5G mobile edge computing: Architectures, applications, and technical aspects. IEEE Communications Surveys & Tutorials, 23(2), 1160-1192.
17. Pothumarti, R., Jain, K., & Krishnan, P. (2021). A lightweight authentication scheme for 5G mobile communications: a dynamic key approach. Journal of Ambient Intelligence and Humanized Computing, 1-19.
18. Jiwani, N., Gupta, K., & Whig, P. (2021, October). Novel healthcare framework for cardiac arrest with the application of AI using ANN. In 2021 5th international conference on information systems and computer networks (ISCON) (pp. 1-5). IEEE.
19. Gupta, K., & Jiwani, N. (2021). A systematic Overview of Fundamentals and Methods of Business Intelligence. International Journal of Sustainable Development in Computing Science, 3(3), 31-46.
20. Gupta, K., & Jiwani, N. (2020). Effects of COVID-19 risk controls on the Global Supply Chain. Transactions on Latest Trends in Artificial Intelligence, 1(1).