SMART ENTERPRISES NETWORK USING CLOUD COMPUTING

Sudha M [1], Kesavan M [2], Muthu Kumara Vel U [3], Madhavan P.S [4]

Student [2,3,4] ,Dept. of Electronics communication Engineering, Paavai Engineering college, Namakkal, Tamil Nadu,India.

Professor [1] ,Dept. of Electronics communication Engineering, Paavai Engineering college , Namakkal,Tamil Nadu, India.

ABSTRACT

The Enterprise network effectively comprises the infrastructure, hardware and software systems, and the communication protocols used to deliver end-to-end services. The network may be architected, designed, deployed, optimized, and configured to perform a unique set of business and technical objectives. In this project we can create multiple
connections to a single sever and upload all the data with the help of cloud computing by this we can able to achieve the high data transfer in low cost as we going to pay for what we use and with this we save lots of physical space, reduce the power consumption with high security.

Today manufacturing enterprises must organize themselves into effective system architectures to match fast changing market demands. These architectures can be realized only by using computer networks to co-ordinate the production of the distributed units forming different types of networked enterprises (NE). Cloud Computing (CC) is an important up to date computing technology for Networked Enterprises, as it offers significant financial and technical advantages beside high level collaboration possibilities. The paper introduces the
main characteristics of future internet-based enterprises and the different CC models. Additionally, the advantages and disadvantages of cloud computing have been summarized giving special focus on interoperability challenges.

I. INTRODUCTION

An enterprise network helps employees and machines communicate, share files, access systems, and analyses the performance of an IT environment that drives business operations. Enterprise networks are configured to connect a limited number of authorized systems, apps, and individuals. Enable a secure and efficient communication channel to perform specific business operations. Based on the results of the information and communications technologies (ICTs), a new "digital" economy is arising. This new economy needs a new set of rules and values, which determine the behaviour of its actors. Participants in the digital market realize that traditional attitudes and perspectives in doing business need to be redefined. In this dynamic and turbulent environment that requires flexible and fast responses to changing business needs organizations have to respond by adopting decentralized, team-based, and distributed structures variously described in the literature as e.g., virtual, networked, cluster and resilient virtual organizations /enterprises.

Cloud Computing has become one of the most talked about technologies in recent times and has got lots of attention from media as well as analysts because of the opportunities it is offering. The market research and analysis firm IDC suggests that the market for Cloud Computing services was $16 billion in 2008 and will rise to $42billion/year by 2012. It has been estimated that the cost advantages of Cloud Computing to be three to five times for business applications.

Enterprises have been striving to reduce computing costs and for that reason most of them start consolidating their IT operations and later using virtualization technologies. In the enterprise, the "adoption of Cloud Computing is as much dependent on the Technology. Many companies have invested in Cloud Computing technology by building their public clouds, which include Amazon, Google and Microsoft These companies are often releasing. new features and updates of their services. For instance, Amazon Web Services (AWS) released a Security and Economics centre on their website to have academic and community advice regarding these issues. This shows that there are still lots of doubts about the costs and security for enterprises to adopt Cloud Computing. Hence, the issues of economics and security in Cloud Computing for enterprises must be researched.

Cloud Computing is a term used to describe both a platform and type of application. As a platform it supplies, configures, and reconfigures servers, while the servers can be physical machines or virtual machines. On the other hand, As large organizations are inherently complex hence, it is very important for Cloud Computing to deliver the real value rather than just be a platform for simple tasks such as application testing or running product demos. For this reason, issues around migrating application systems to the cloud and satisfying the needs of key stakeholders should be explored the stakeholders include technical, project, operations, and financial managers.

Cloud computing has revolutionized the way enterprises operate, allowing them to scale their IT infrastructure and resources without the need for significant capital investment. However, as cloud environments become more complex and dynamic, enterprises are faced with new challenges in terms of network management, security, and performance. In particular, the rapid growth of cloud-based applications and services has led to a need for smarter and more efficient network architectures that can support real-time data access and processing, while also ensuring optimal performance, security, and reliability.

To address these challenges, we propose a smart enterprises network for cloud computing that leverages advanced networking technologies such as Software-Defined Networking (SDN) and Network Function Virtualization (NFV). The proposed network architecture is designed to enable enterprises to deploy and manage their cloud resources in a more efficient and automated manner, while also reducing operational costs.

II. PROBLEM STATEMENT

Enterprises today are increasingly adopting cloud computing for its numerous advantages such as scalability, flexibility, and cost-efficiency. However, managing a cloud-based infrastructure can be complex and challenging, especially when dealing with large-scale deployments. Smart enterprises require a robust network infrastructure that can provide reliable connectivity, security, and high-performance for their cloud applications and services.

As enterprises increasingly move their business operations to the cloud, they face challenges in managing and securing their networks. With the growing use of cloud computing, there is a need for smart enterprises networks that can provide secure and reliable connectivity between different cloud services and the users.

One of the major challenges faced by enterprises is the complexity of managing multiple cloud services. Different cloud providers have different requirements and managing them separately can lead to inefficiencies and security risks. Moreover, as the amount of data being generated and transmitted increases, enterprises need to ensure that their networks are scalable and can handle large amounts of traffic without compromising performance.

Another challenge faced by enterprises is the security of their data and network. With the growing threat of cyber-attacks and data breaches, enterprises need to ensure that their networks are secure and protected from unauthorized access. This requires implementing strong security measures, such as encryption and access controls, and regularly monitoring and updating these measures to stay ahead of potential threats.

To address these challenges, enterprises need a smart network solution that can provide seamless connectivity between different cloud services while ensuring the security and reliability of the network. Such a solution should be easy to manage, scalable, and able to provide real-time monitoring and analysis of network performance and security.

III. EXISTING SYSTEM

The existing system for smart enterprises network for cloud computing typically consists of a combination of network hardware and software, cloud services, and security solutions. Network hardware includes routers, switches, and other networking devices that enable communication between different cloud services and the enterprise's on-premises systems. These devices are typically configured and managed using network management software. Cloud services are hosted by third-party providers and can include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) offerings. Enterprises typically use multiple cloud services from different providers to meet their business needs.

To manage and secure their network and cloud services, enterprises use a range of security solutions, including firewalls, intrusion detection and prevention systems, virtual private networks (VPNs), and identity and access management (IAM) solutions. These solutions help to protect against unauthorized access, data breaches, and other

security threats. The existing system can be complex to manage, as each cloud service and security solution typically has its own management interface and configuration requirements. This can lead to inefficiencies, inconsistencies, and potential security risks if not managed properly. Furthermore, the existing system may not be scalable enough to handle large amounts of traffic or adapt to changing business needs. This can lead to performance issues and potential downtime, which can impact business operations and revenue.

The existing system for smart enterprise network for cloud computing consists of various components and technologies that are used by enterprises to manage and secure their cloud-based networks.

1. Virtual Private Network (VPN): Enterprises use VPNs to create a secure and encrypted connection between their on-premises network and their cloud-based resources. This allows them to securely access their cloud resources from anywhere, without compromising security.
2. Software-Defined Networking (SDN): SDN is a network architecture that allows enterprises to manage their network infrastructure using software instead of hardware. This makes it easier to manage and scale their network and enables them to quickly adapt to changing business needs.
3. Cloud Access Security Broker (CASB): CASB is a security tool that helps enterprises monitor and secure their cloud applications and data. It provides visibility into user activity, data access, and application usage, and can enforce security policies to prevent data breaches and other security threats.
4. Multi-Cloud Management: As enterprises increasingly use multiple cloud providers, multi-cloud management tools have become essential. These tools help enterprises manage their cloud resources across different providers, and provide visibility into costs, usage, and performance.
5. Network Function Virtualization (NFV): NFV is a technology that allows enterprises to virtualize network functions, such as firewalls and routers, and run them on commodity hardware. This reduces the cost and complexity of network infrastructure and allows enterprises to quickly deploy and scale network functions as needed.

Overall, the existing system for smart enterprise network for cloud computing is a combination of different technologies and tools that work together to provide secure and reliable connectivity between different cloud services and users. However, there are still challenges in managing and securing cloud-based networks, and enterprises need to continually adapt and update their network infrastructure to stay ahead of potential threats.

IV. SMART ENTERPRISES NETWORK FOR CLOUD COMPUTING

The proposed smart enterprises network for cloud computing is based on the principles of SDN and NFV, which enable the network to be more agile, programmable, and efficient. SDN separates the control plane from the data plane, allowing for centralized network management and control, while NFV enables network functions to be virtualized and run on commodity hardware, reducing the need for expensive and proprietary networking equipment.

The proposed network architecture consists of three layers: the infrastructure layer, the control layer, and the application layer. The infrastructure layer comprises physical networking devices such as switches, routers, and servers, while the control layer includes the SDN controller and NFV orchestrator. The application layer consists of cloud-based applications and services that run on top of the network infrastructure.

The SDN controller and NFV orchestrator work together to enable network automation and orchestration. The SDN controller provides centralized network management and control, allowing administrators to configure and manage the network from a single location. The NFV orchestrator enables the deployment and management of virtual network functions, such as firewalls, load balancers, and intrusion detection systems, on commodity hardware.

The proposed network architecture also includes several key features to improve network performance, security, and reliability. These features include:

1. Dynamic network provisioning: The network can be automatically provisioned based on application demands, enabling enterprises to scale their cloud resources in real-time.
2. Service chaining: Network functions can be dynamically chained together to create customized network services, allowing enterprises to optimize network performance and security.

3. Multi-tenancy: The network can be partitioned into multiple virtual networks, enabling enterprises to isolate and secure their cloud resources.
4. Quality of Service (QoS): The network can be configured to prioritize traffic based on application requirements, ensuring optimal network performance.

V. PROPOSED SYSTEM

Consider the case of the software-based virtual switch. The virtual switch inside the same physical server can be used to switch the traffic between the virtual machines (VMs) and aggregate the traffic for connection to the external physical switch. The virtual switch is often implemented as a plug-in to the hypervisor. The VMs have virtual Ethernet adapters that connect to the virtual switch, which in turn connects to the physical Ethernet adapter on the server and to the external Ethernet switch. Unlike physical switches, the virtual switch does not necessarily have to run network protocols for its operation; nor does it need to treat all its ports the same because it knows that some of them are connected to virtual Ethernet ports. It can function through appropriate configuration from an external management entity.

Network architecture is one of the key building blocks of cloud computing. A cloud user connects to the network to access the cloud resources. The cloud is accessible through a public network (the Internet) or through a private network infrastructure (e.g., multiprotocol label switching, MPLS, or dedicated links). The most significant effect of cloud computing on a network is in the data center. The data center consists mainly of servers in the racks interconnected through a top-of-rack (TOR) Ethernet switch, which in turn connects to an aggregation switch, also known as an end-of-rack (EOR) switch. The aggregation switch connects to other aggregation switches and through these switches to other servers in the data center. A core switch connects to the various aggregation switches and provides connectivity to the outside world, typically through layer 3 (IP). Since most intra-datacenter traffic traverses only the TOR and the aggregation switches, a fat-tree.

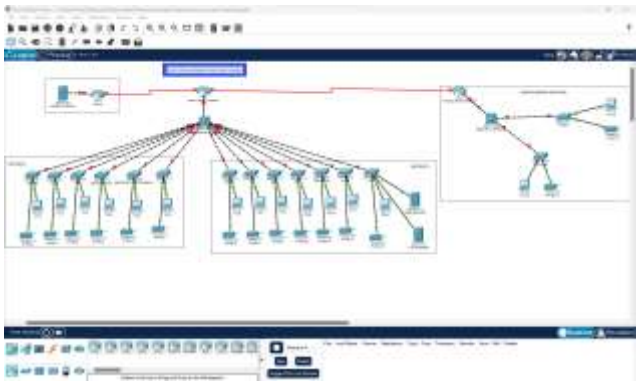
Although cloud computing does not necessarily depend on virtualization, several cloud infrastructures are built with virtualized servers. Within a virtualized environment, some of the networking functionalities (e.g., switching, firewall, application delivery controllers, and load balancers) can reside inside a physical server.

Consider the case of the software-based virtual switch. The virtual switch inside the same physical server can be used to switch the traffic between the virtual machines (VMs) and aggregate the traffic for connection to the external physical switch. The virtual switch is often implemented as a plug-in to the hypervisor. The VMs have virtual Ethernet adapters that connect to the virtual switch, which in turn connects to the physical Ethernet adapter on the server and to the external Ethernet switch. Unlike physical switches, the virtual switch does not necessarily have to run network protocols for its operation; nor does it need to treat all its ports the same because it knows that some of them are connected to virtual Ethernet ports. It can function through appropriate configuration from an external management entity.

Network architecture is one of the key building blocks of cloud computing. A cloud user connects to the network to access the cloud resources. The cloud is accessible through a public network (the Internet) or through a private network infrastructure (e.g., multiprotocol label switching, MPLS, or dedicated links). The most significant effect of cloud computing on a network is in the data centre.

The data center consists mainly of servers in the racks interconnected through a top-of-rack (TOR) Ethernet switch, which in turn connects to an aggregation switch, also known as an end-of-rack (EOR) switch. The aggregation switch connects to other aggregation switches and through these switches to other servers in the data center. A core switch connects to the various aggregation switches and provides connectivity to the outside world, typically through layer 3 (IP). Since most intra-datacenter traffic traverses only the TOR and the aggregation switches, a fat-tree.

VI. SYSTEM ARCHITECTURE



NIST (National Institute of Standards and Technology) is a well-accepted institution all over the world for their work in the field of Information Technology. I shall present the working definition provided by NIST of Cloud Computing. NIST defines the Cloud Computing architecture by describing five essential characteristics, three cloud services models and four cloud deployment models (Cloud Security Alliance).

NIST (National Institute of Standards and Technology) is a well-accepted institution all over the world for their work in the field of Information Technology. I shall present the working definition provided by NIST of Cloud Computing. NIST defines the Cloud Computing architecture by describing five essential characteristics, three cloud services models and four cloud deployment models (Cloud Security Alliance

Although we have worked out an accurate cloud architecture model, the model is not perfect. There are some challenges for establishment of this model. To overcome this problem, our future research can focus on various cloud architecture models.

The smart enterprises network for cloud computing architecture is designed to improve network performance, security, and reliability while enabling enterprises to deploy and manage their cloud resources in a more efficient and automated manner. The architecture is based on Software-Defined Networking (SDN) and Network Function Virtualization (NFV) principles, which allow the network to be more agile, programmable, and efficient.

The proposed architecture consists of three layers: the infrastructure layer, the control layer, and the application layer. The infrastructure layer comprises physical networking devices such as switches, routers, and servers, while the control layer includes the SDN controller and NFV orchestrator. The application layer consists of cloud-based applications and services that run on top of the network infrastructure.

Infrastructure Layer:

The infrastructure layer consists of physical networking devices such as switches, routers, and servers. These devices are responsible for forwarding network traffic between end-hosts and providing connectivity to the SDN controller and NFV orchestrator. The infrastructure layer is designed to be highly scalable and flexible, enabling enterprises to add or remove networking devices as required.

Control Layer:

The control layer includes the SDN controller and NFV orchestrator. The SDN controller is responsible for managing and controlling the network infrastructure. It communicates with the infrastructure layer devices to configure forwarding rules and manage network traffic. The NFV orchestrator is responsible for deploying and managing virtual network functions, such as firewalls, load balancers, and intrusion detection systems, on commodity hardware. The SDN controller and NFV orchestrator work together to enable network automation and orchestration. The SDN controller provides centralized network management and control, allowing administrators to configure and manage the network from a single location. The NFV orchestrator enables the deployment and management of virtual network functions, reducing the need for expensive and proprietary networking equipment.

Application Layer:

The application layer consists of cloud-based applications and services that run on top of the network infrastructure. This layer is where the enterprise's business applications and services are deployed. The applications can be hosted on public or private clouds, depending on the enterprise's requirements.

Benefits:

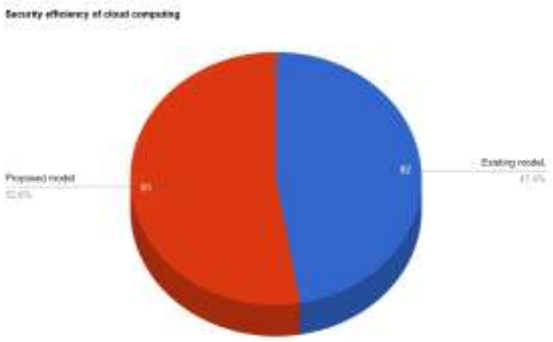
The smart enterprises network for cloud computing architecture provides several benefits for enterprises:

1. Efficient and automated network management: The architecture enables enterprises to deploy and manage their cloud resources in a more efficient and automated manner, reducing operational costs.
2. Improved network performance, security, and reliability: The architecture improves network performance, security, and reliability, ensuring that cloud-based applications and services are always available and responsive.
3. Scalable and flexible: The architecture is scalable and flexible, enabling enterprises to add or remove networking devices and cloud resources as required.

Overall, the architecture of a smart enterprise network for cloud computing is designed to provide secure and reliable connectivity between different cloud services and users. It is a combination of different technologies and layers that work together to ensure that the network infrastructure is scalable, manageable, and secure.

The architecture of a smart enterprise network for cloud computing typically consists of multiple layers that work together to provide secure and reliable connectivity between different cloud services and users**.**

VII. COMPARASION OF PROPESED MODEL



t in this matter as it is used for host authentication and data encryption. XML signature or XML encryption cannot be used by browser directly as data can be only encrypted through TLS and signatures are only used with the TLS handshake for security. Every file is encrypted on the sender side and each file individual separated key that was generated to decrypt the received file, The key for the file was sent to the receiver email address for each file to authenticate and verify the authorized user.

.

IX. CONCLUSIONANDFUTURE

ENHANCEMENT

The smart enterprises network for cloud computing architecture is designed to address the challenges of managing cloud-based environments. The architecture leverages advanced networking technologies such as SDN and NFV to improve network performance, security, and reliability. The architecture is designed to be efficient, automated, scalable, and flexible, enabling enterprises to deploy and manage their cloud resources in a more agile and responsive manner.

In conclusion, smart enterprise networks using cloud computing offer numerous benefits that can help businesses of all sizes become more agile, productive, and competitive. By leveraging cloud-based networking technologies, companies can take advantage of scalability, cost-effectiveness, accessibility, reliability, and security. This can enable businesses to scale up or down as needed, reduce costs, increase productivity, and collaborate more effectively. With the rapid pace of technological change and the increasing demand for flexible

and scalable IT infrastructure, adopting cloud-based networking solutions is becoming increasingly important for companies that want to stay ahead of the competition. By investing in smart enterprise networks using cloud computing, businesses can position themselves for success in the digital age.

X. REFERENCES

1. Adriana Mijuskovic, Rob Bemthuis, Adina Aldea, Paul Havinga, University o*f* Twenty. An Enterprise Architecture based on Cloud, Fog and Edge Computing for an Airfield Lightning Management System, 2020 IEEE 24th International Enterprise Distributed Object Computing Workshop (EDOCW).
2. Maziar Nekovee, Sachin Sharma, Navdeep Uniyal, Avishek Nag, Reza Nejabati, Dimitra Simeonidou University of Sussex, National College of Ireland, University of Bristol, University College Dublin, "Towards AI-enabled Microservice Architecture for Network Function Virtualization" ComNet'2020 1570600327
3. Ogechukwu M Okonor, Mo Adda, Oliver Spear and Alex Geogov School of Computing, University of Portsmouth, United Kingdom, "Mobile Agent Based-Approach for Enhancing Energy Efficient Cloud Data Centre Network", 2020 6th IEEE International Energy Conference (Energycon).
4. Srini Bhagavan, Praveen Rao, Thuan Ngo, University of Missouri-Kansas City IBM Corporation, "A Transparent Supply Chain for Multi-cloud and Hybrid Cloud Assets Powered by Blockchain", 2021 IEEE 37th International Conference on Data Engineering Workshops (ICDEW).
5. Hamada Alshaer, Navdeep Uniyal, Konstantinos Katsaros, Konstantinos Antonakoglou, Steven Simpson, Hanaa Abumarshoud, "The UK Programmable Fixed and Mobile Internet Infrastructure: Overview, capabilities and use cases deployment", IEEE Access (Volume: 8) 2020.
6. István Mezgár , Computer and Automation Research Institute Hungarian Academy of Sciences Hungary, Budapest and Department of Manufacturing Science and Technology Budapest University of Technology and Economics, "Cloud Computing Technology for Technology Enterprises", 18th IFAC World Congress.
7. Luis M. Camarinha-Matos New University of Lisbon, Quinta Da Torre 2829-516, Monte Caparica, Portugal Hamideh Afsarmanesh University of Amsterdam, The Netherlands, "Collaborative networks: a new scientific discipline", Journal of Intelligent Manufacturing.
8. Luis M. Camarinha-Matos a,Hamideh Afsarmanesh b, Nathalie Galeano c, "Collaborative networked organizations – Concepts and practice in manufacturing enterprises" Computer and Industrial Engineering Volume 57 2020.
9. Maryam Shabbir1, Ayesha Shabbir, Celestine Iwendi , (Senior Member, Ieee), Abdul Rehman Javed, Muhammad Rizwan, (Senior Member, Ieee) Na Partially Supported By The Western Norway University Of Applied Sciences, Bergen, Norway, "Enhancing Security of Health Information Using Modular Encryption Standard in Mobile Cloud Computing", IEEE Access 2020.
10. Mustafa Gamsiz And Al Haydar Özer, Department of Computer Engineering, Faculty of Engineering, Marmara University, Istanbul, Turkey Corresponding author Ali Haydar Özer, "An Energy-Aware Combinatorial Virtual Machine Allocation and Placement Model for Green Cloud Computing", IEEE Access 2021.