The article - covers following Architecture based threats in the system of 5G Network Slicing which are potentially increasing as we adapt to the 5G technologies that are implied in regular business applications. The 5G Network Slicing typically has following areas of concern -

1. Life Cycle of a Slice
2. Inter Slicing
3. Intra-slicing

The research paper covers lifecycle of a 5G Network Slice from its preparation, installation, configuration, runtime and decommissioning of the service. Along with each stage there are certain of risks and security threats to mitigate at respective levels. The Paper briefly expose them and share the mitigation tactics required as a part of security of building a 5G slice in actual user use.

The 3GPP i.e. Third Generation Partnership Project established the fundamentals of 5G network slicing. The Network slicing is in category of virtualisation networking paradigm that deals with logical partitioning of the network. It can be counted along with SDN and NFV but is an independent technology altogether. The Network slicing enables flexible and efficient creation of logical networks on top of shared network infrastructure. Each logical network serves different type of service with different heterogenous requirements to facilitate vertical industry. 5G slicing is characterized in 5 categories – enhanced mobile broadband, ultra-reliable low latency communication, massive machine type communication

They Key findings of this paper is necessity of having a good, secured network with advancement of 5G slicing, its threats and mitigation strategies. Since 5G is an evolving field, it is recommended to have identify the plausible threats and have mitigation plan to avoid any serious security attack.

To Conclude on the security threats and plans to mitigate the same while considering the 5G network slicing we need to have additional considerations of facts and figures which should be more robust and optimized way to tackle the security threats to avoid any possible security breach in the network.

Shortcomings of research article –

The research paper mainly deals with –

* 5G Architecture
* A Slice Lifecycle
* Security Threats in slice lifecycle, interslice and interslice

In real life application of 5G Network Slicing there are more major areas of threats and challenges which 5g Slicing Architecture need to be configured for. The research article is quite confined to what is already given and the basis of which the things are derived and noted. Instead there should be more practical approach to tackle the current Security challenges directly by consulting the customers. Otherwise it is advisable to have more deep research on threats with the current system and finding out all the flaws in rules and regulations set for G network Slciing. Since it is quite new there are a lot more possible flaws in the model and needs to be improved. This initial research will help for long term and larger part of the network community in coming years to avoid any huge losses in case of compromised system.The current research article can be evolving, 5G Network Slicing is taking time to evolve and adapt in incoming network changes, it is necessary to consider all aspects and its outreach in security threats.

The article rightly cover up the Architecture and Network slicing layers the way they are communicating between themselves and how it would affect the upcoming challenges in the field of network utilization. There are innumerable threats which are opened up with the introduction of new technologies. And one must consider all aspects of these threats to overcome and plan accordingly to avoid them. This gives immense regularity to build a threat free network slicing for the future

Firstly, the 5G Network slicing Architecture consist of following main Domains –

Core Networks and Radio Access Network. A single slice instance also known as single logical network instance are combined to form a one or more network slice subnet also called as Sub slice.

When multiple sub slices combine it forms a single network slice instance also called as Slice. The resource layer, network Slice instance and Service Instance layer comprise of servers catering one or more network slice instances. Network slice instance layer need to have network compatibility in order to service to various equipment’s and devices

And the Service instance layer helps to serve the end equipment.

For the Slice Life Cycle- there are major 4 stages – preparation, installation, runtime and decommissioning of the server.

Based on these factors the security threats are classified as follows –

Slice Life Cycle Security

Preparation –

Installation & Configuration  
Runtime

Decommissioning

Intra slice Security has

* 5G customer Devices which are inter connected within a system of Networks

supporting capabilities as dynamic auto-scaling as well as high availability to address the performance requirements of mission critical applications.

Org & Development of Ideas – Logical development of ideas through well developed paragraphs good use of transition

Mechanics – length requirement, grammatical & punctuation errors. APA MLA Guidelines are meticulously followed adhers to font spacing guidelines