www.ijecs.in
International Journal Of Engineering And Computer Science
Volume 10 Issue 12 December 2021, Page No. 25606-25630
ISSN: 2319-7242 DOI: 10.18535/ijecs/v10i12.4668

Enhancing Telecom Security Through Big Data Analytics and Cloud-Based Threat Intelligence

Venkata Bhardwaj Komaragiri
Lead Data Engineer, ORCID ID : 0009-0002-4530-3075

Abstract
Negative effects of cyber-attacks against telecom operators are imposed not only on the telecom operators but also on their users. Even worse, negative effects could be imposed on national economies and on public safety. This situation happens because telecom operators are the primary communications infrastructure providers used by enterprises and people for their day-to-day operations. In the network-cloud era, telecom operators face cyber threats from both established and new attack sources. In addition, telecom operators deliver numerous services over general-purpose COTS hardware and software for lower COST, which ultimately results in larger surfaces of attack. These challenges require enhanced telecom security that can effectively improve detection, prevention, response, and recovery capabilities against advanced, massive, and patchy threats targeting telecom networks and services.
Although real-time threat detection and forensic investigation can be efficiently performed using state-of-the-art techniques such as big data analytics based on statistics or machine learning models, it is challenging to understand unknown threats. This results in having to deal with an unknown threat, which is more costly than known threats. The recently proposed cloud-based threat intelligence service can fill this gap by providing threat information regarding new attack sources, tactics, methods used, signatures, and patch solutions. Such service can leverage a large telecom security consortium where a group of telecom operators share the information of their security logs and shares the cost of the threat intelligence service, which usually charges COSTs based on the size of ingested logs. The consortium must protect its ingested logs and extracted intelligence in the service from being compromised by users in the cloud.

Keywords: Telecom security, big data analytics, cloud-based threat intelligence, cybersecurity, network protection, real-time threat detection, intrusion detection systems (IDS), anomaly detection, predictive analytics, data-driven security, cloud computing, scalable security solutions, advanced persistent threats (APT), threat intelligence platforms, security analytics, SIEM, telecommunications infrastructure, cyber threat mitigation, proactive security, data protection.

1. Introduction

Telecommunications (telecom) service providers, such as mobile network operators, landline telephone service providers, and internet service providers, play an vital role in the critical infrastructure of a nation [1]. Telecom service providers experience cybersecurity incidents, which are either resolved or linger undetected. Cyberbad actors take advantage of previously hidden incidents, and despite strong security controls and

vigilance, incidents can still remain hidden. A glaring flaw in the current practices and processes of telecom service providers is that correlation and analysis of critical event information from many sources is lacking. Governments often spearhead regulatory compliance aimed at telecom service providers, which requires telecom service providers to engage law enforcement agencies with access to critical network and telecommunications infrastructure. No prior steps existed to ensure that law enforcement agencies were not cybersecurity bad actors themselves. Acceptance of responsibility aligned with legislation serves to create an environment of mutual trust and respect between telecom service providers and law enforcement agencies, with the intention of safeguarding the security of critical national infrastructure. However, without advanced security controls and precautions, this responsibility, coupled with the lack of oversight and auditability, creates an opportunity for harm from unprecedented powers over the networks of telecom service providers. Even with the best intentions, lawful hacking can still infiltrate and compromise networks, systems, infrastructure, and intelligence collection. The big data creation trend poses strict requirements on the architecture of IT systems across the Telecommunications industry. Real-time data movement, pipelined data processing, and archived data retrieval are required measurements to take on data streams, which are huge volumes of data flow in a continuous manner. In a real-time detection scenario, it is required to ingest, analyze, and take action on incoming data in real-time or near real-time. The solution must be saturated horizontally by deploying additional commodity servers. Furthermore, some kind of orchestration service is needed for data transmission handling, analysis task scheduling, and aggregate result storing mechanism. Either off-the-shelf products or cloud-based platforms can be used to build a sophisticated ecosystem for such a purpose.

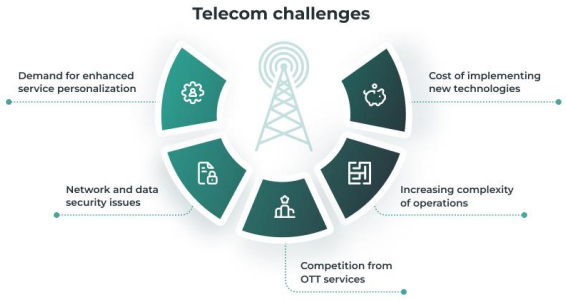

Fig 1 : Cloud Computing in Telecom: Benefits and Challenges

2. The Telecom Security Landscape

Telecommunication networks are not immune to emerging threats. Recent attacks on telecommunication service providers show how critical communication infrastructures can be harmed. Hackers have utilized telecom provider zero-day vulnerabilities to listen to calls and read customers' text messages. Another world-scale compromise of the products of a telecommunication infrastructure vendor invoked U.S. sanctions against a major European mobile services provider. These attacks illustrate the chic yet dangerous tendency of hackers to target TSPs, as customers' consequences from telecom cybersecurity breaches can far exceed breaches of typical IT firms' systems.

To threat actors, the raw amount of telecommunication technologies' easy-pickings in the detection area is evident. Consequently, TSPs need to enhance their network infrastructure defenses and harden detection systems. Context-aware detection parameters around the 5G telemetry signals should be tightened and augmented, with implementation of big data analytics and cloud-based threat intelligence based on lodger analytics. Such systems would enhance the coverage and searching space of behavior intelligence detection over machine learning features in the 5G networks with warning metrics and detection metrics, improving day-0 and day-1 responses against novel attacks.

A new user equipment is booting to the evolved packet core of the telecommunication company. The user equipment transmits a attach request to the

evolved node-b for 5G telecommunication services over the new radio. The user equipment attaches to the next-generation packet core with 'shut eye' in the 'sleeping' message. This transmission sits in the middle of the security handshake with invalid authentication vectors, but was unapproved due to guessed behavior analytics. An adherent attack could have dropped the user equipment out of sight from 5G signal detectors and monitoring suites, using legit identifiers to seize services within a telecommunication infrastructure.

3. Big Data Analytics in Telecom

Telecom service providers are facing challenges in continuous operation and updating. With the explosive growth of operation data, big data analytics is being introduced using data from different sources related to telecom infrastructure. By combining different views of data with respect to resources, alarms, performance, and logs, data can be analyzed faster and closer to real-time data due to limitations in the ability to analyze big data. framework integrates established tools and platforms using matured algorithms and predictive models to cover key data types from telecom infrastructure. Providing a user-friendly interface for data exploration and customization of dashboards and alerts helps solve multiple customer use cases.

Mobile networks possess information about the users as well as the network. On a high level, big data analytics can efficiently analyze user and network information, unearth meaningful insights with the help of machine learning tools, and correlate different factors with a user's experience, service quality, and traffic distribution. Telecom service providers need to design and upgrade their network based on these insights in order to provide user satisfaction .

Telecom service providers need to improve call drop rates, as well as reduce fake calls and traffic. To detect anomalies in the network, Call Detail Records data is used. To make the detection even more efficient, authentication and verification of anomalies is used, along with clustering to identify the location of clusters and fit back centre points using an unsupervised machine learning algorithm . By focusing on the count of call detail records, the mean and standard deviation of the number of calls in normal situations can be calculated for different zones. Once the number of calls in a zone exceeds the external threshold range, it is flagged as an anomaly zone.

3.1. Overview of Big Data in Telecom

Since 2010, the term "Big Data" has emerged and become a trendy catchphrase in IT, scientific research, finance, and government organizations. In the telecommunication industry, big data can be seen in more powerful switches, higher-speed border gateways, more subscribers, fixed devices and mobile terminals (with different levels of usage), and multilib technology. The emergence of these factors is accompanied by the increase in data volume, data velocity, and data variety. Big data brings new opportunities and challenges to the industry. Telecommunications can create value from Big Data in: (a) Real-time operations (high velocity) - monitoring alarm messages, detecting service, network and system performance issues and extracting information, and extracting knowledge from social media, port monitoring, log records, infrastructure, probes, and sensor networks to improve operations quality; (b) Analyzing Entire Historical Records (high volume) - discovering important spatiotemporal patterns in telecom taxi/fleet data and analyzing performance by improving stochastic approximation methods; (c) Adding New Data Types (high variety) - analyzing unstructured and semi-structured text data to extract service and user content sentiment .

Telecam uses data collected from fixed assets, probes, and sensors to manage the oil pipeline layer and the production resources equipment layer of the oil industry using rule simulation, failure prediction models, and simulated Annealing algorithm optimization. Telecom traditionally models and analyses complex networks with mere mathematical

and logarithmic tools using the existing processed/purified data for network evolution, growth, topology change, performance deteriorate, and stability. Recently Latent Tree Model (LTM), which learns the structured representation of data, and nonparametric Bayesian-network discovery methods are used for network topology discovery are employed to detect 4G base-station behavior events with multi-dimensional complexity through censoring the queuing process observed in an event/time series. A P2P Live Video streaming network is analyzed using the concept of Local Area Network; a small World Network modeling algorithm-based discovery method is introduced for telecom SNS to discover friendship circle structure patterns and their impact on User Generated Content (UGC) accessing pathway.

In the telecommunication industry, sensor and distributed monitoring for upcoming 4G networks development is used; applications of multi-level monitoring of real-time alarms triggered by different devices are mentioned; ATTRA must be augmented with new types of scripts for detection of atomic fragments due to multi-level distributed monitoring and be extended to take full advantage of big data techniques; presentation on key roles; conference proceedings filtering engine was demonstrated; compared with telecom OSS, Dimension Data focuses on telecom bouquet at an enterprise level; and, on video delivery industry leveraging telecom resource with IT big data analytics.

3.2. Data Sources and Types

The common roadside installations of mobile networks (like antennas, radio base stations or BSCs) are often situated in remote locations and regularly monitored and taken care of by Outsourcing IT companies by obtaining access to the management systems of Carrier Telecom Operators (CTOs). After a proper analysis of the CCS Threats, several possible attacks can be foreseen on the CCS. A classification of possible attacks on CTI networks can be seen below. It is easy to see that a breach in the CCS via an attack on Cloud Metadata could gain access to signalling, and audio streams. It is also important to mention that breaches via Cloud Management, Cloud Analytics, or Cloud-hosted databases can also obtain access to the targeted SS7 and STP entities.

In terms of implementation, the impact of transitioning existing CTI systems from on-premise operation to cloud-based architecture on users' privacy is more profound than merely adding new functionalities on top of implied pre-existing architecture. Transitioning to a cloud-based architecture fundamentally changes how CTI data are hosted, and so also how they can be accessed by malware. It transforms CTI data from being entirely under the control of a group of trusted users, into being hosted on publicly accessible cloud servers, where trusted user control would have to be completely redefined and Minimum Viable Security should be redesigned and reimplemented accordingly. On that account, the feasible abstraction and architecture of privacy preserving frameworks for cloud-based CTI would have to be different than those proposed in modern on-premise systems.

The factors affecting the change of attack surface due to transition to a cloud-based architecture should be better quantified. Analysis should be conducted to explore what CTI, on what CTI hosting architecture types, will be exposed to what malware capabilities, i.e. which phenomena vacuums in terms of knowledge are created amidst migration of existing data to the cloud, and what inputs would such for adversaries? Potential consequences of such knowledge vacuums should be analysed with cost-benefit analysis of possible prevention mechanisms.

3.3. Analytical Techniques Used

To accomplish the aforementioned objectives, various data analytics techniques were employed. The details of the data, its preprocessing and cleansing, and the big data analytics techniques used are described in the following sections.

Anonymized detection center to customer (D2C) log data was obtained from an Indian telecom service provider for August and September 2021. The log data consisted of around 49 million records, and the relevant attributes include response_time_categories, su_id, detection_id, alarm_type, detection_date, customer_id, and signal_ind, among others. The detection_id refers to the type of detection initiated by the detection center. Each detection can have multiple alarms aggregated based on the alarm_type attribute. The detection timestamp was converted from UTC to Ist.

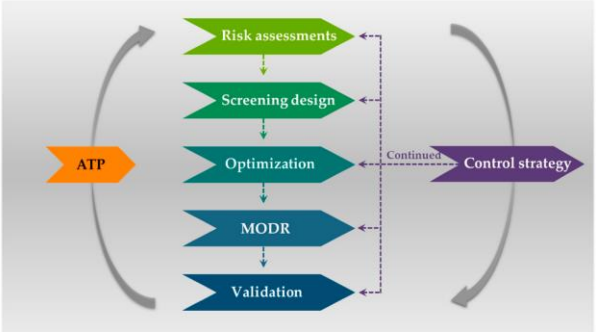

Fig 2 : Analytical procedure lifecycle

This data was structured un-sanitized data, which was cleaned to become analysis-ready. A lot of effort went into understanding the data and modeling it properly for analysis. The resulting clean data includes the same attributes apart from customer and su_ids encoded to reduce the cardinality to improve storage and processing times, alarm aggregation, and finding a meaningful time interval for data aggregation.

The resultant dataset is a balanced anonymized D2C log data of about 1.3 million records. On analyzing the cleansed D2C data, close to 470 (detection, timestamp interval) combinations with a minimum number of instances of 20, most having a few hundred instances, were observed. Each (detection, time interval) is treated as a single event in time partitioned data format.

Powerful big data analytics techniques available with the cloud solution based big data platform are used for data analysis. In this context, descriptive and predictive analysis techniques provided by the platform are implemented. Two analysis scenarios—anomaly detection on the unscratched model and detection on scratch model—were implemented, of which the first scenario is described.

Detecting anomalies (outliers) in the number of alarms is an interesting descriptive analysis that is vital to telecom network monitoring. Anomalies within a short time interval possibly indicate a sudden surge of alarms, which can be used to issue alerts to all stakeholders, operators, and D2C customers. Detecting anomalies is a non-standard yet interesting problem because it is a univariate time-series-like sequence of event counts .

The above problem takes a count-based prevention approach, where the number of alarms over sliding time intervals is surfaced as a series of events with varying granularity. Increasing the sliding interval improves the recall of anomalies but with reduced precision. On the top of the above static event processing, different types of visualization techniques are used for anomaly detection, and logging event-based statistical trackers maintain the status of available resources.

4. Threat Intelligence in Telecom

Telecom Systems wishing to be effective and competitive in modern environment necessitates the capacity to use technology and efficient organizations. Generally, these institutions are more trustworthy than their rivals. Therefore, the unbelievably colossal amount of precious data that is integrated daily in Telecom, Telecommunications companies are invaluable. They need understanding of client demand in order to fix the future investment on capacity. Clients are introducing new techs, interactions and devices in their lives and industries.

Equation 1 : Threat Propagation in Networks (Graph Theory)

$$P_{infected}(v) = 1 - \prod_{u \in N(v)} (1 - p_{uv})$$

- $P_{infected}(v)$: Probability that node v is infected
- $N(v)$: Neighbors of node v
- p_{uv}: Probability of threat transmission from node u to v

Big Data can actually "answer" in real time queries and situations that are in importance for Telecommunication organizations in their planning. Mostly those demands can deeply change entities, their profit and expense structure and the competition. That is why responsive and expert understanding of those queries need highly educated data miners with thorough knowledge of the company and its markets. Moreover, sometimes fraudulent behaviours can generate commitments for Telecom companies bringing them in risks of license break and govern approach; and stemming the reputation or the credit of the firm. Data Mining Process is to select proper data describing the object; and transform the data in a suitable form for DM. Data mining is to find proper vultures and patterns in the object.

Different statistics and models can generate different best selection of quarrying data so the Discovery of Knowledge in Databases (KDD) processes is completely on the data analysis side. Then the information of interest can be treated. It is used to decide rules or to classify a situation. In Final phase, Evaluation, this results are verified and justified bringing to the application of the knowledge in a larger context and producing other ways of acquiring further information. At last potential testament, benefits, costs and the procedure needed to exploit the knowledge is detailed.

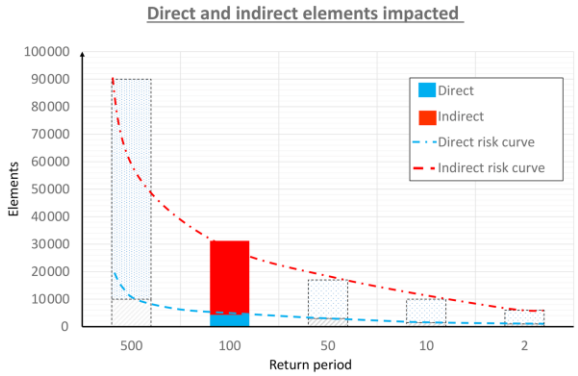

Fig : Direct and Indirect elements Impacted

Generation of supervision telecommunication systems is described. This is a concrete data mining architecture for monitoring fixed line and GSM origin telephone calls. On the first basis some analyses, useful to understanding the "dangerous behaviours" or not of one client calling from a determined number, is discussed with related studies on the to be expected behaviours of a telecommunications customer [1] Evolution of telecommunications firms, necessary steps to implement a Lawful Interception babm, swish provision of Li as a Service (LaaS) and, in general, the introduction of an internal "Information is Gold" policy are discussed.

4.1. Definition and Importance

The objective of this text is to increase the understanding of how to utilize cloud and Big Data technologies to enhance telecom security solutions by creating a cloud-based threat intelligence platform. This platform would serve as a service that could gather big data intelligence from different telecom CSPs to enhance proactive defense systems. A proof-of-concept prototype model is presented and evaluated with positive results. It is concluded that threat intelligence sharing, cloud, and big data technologies as well as telecom big data sources have a great potential to enhance security analytics and give rise to sophisticated proactive defense systems for telecom network security.

The event of cyber-threats has drastically increased in recent years. Different organizations apply some

security solutions to protect their computers and network infrastructures against various attacks and infiltrations. Threat intelligence refers to data that can help an organization identify the attack patterns, create up-to-date threats profiles, alter the detection patterns of current security solutions, apply mitigation actions against known threats, and that can be more generically categorized into tactical, operational, and strategic types. Many organizations open up various types of threat intelligence sources to share their analytical findings about an updated threat on a server or an IP address with other users to increase the general knowledge of the cyber-threats. But there are also a number of private capability threat intelligence sources, which operate closed API, that are only available for their customers that refer to the customers of the security service providers.

Telecommunication Service Providers (TSPs) also face some heavy challenges such as a very special type of cyber-attack that is problematic to secure their infrastructures and a heavy reliance on third-party applications that exposes them to various security risks. Different telecom-based security vendors provide telecom security solutions to combat the upcoming cyber-threats such as DDoS attack detection and mitigation solutions for maintaining the Quality of Service of the telecom users, unauthorized IP reputation and malware traffic filtering solutions for preventing botnets, Big Data Intelligence Platform for telecom data analytics to prevent true positive detection and no-delay mitigation solutions, etc. These solutions already contain some good capabilities, processes, and algorithms to mitigate such attacks but on a smaller detection coverage scope than the whole telecom infrastructure.

4.2. Sources of Threat Intelligence

Despite the emergence of new information technologies that capitalize on the needs and challenges of digital transformation, the market demand for cyber threat intelligence and data analytics in various sizes and domains continues to grow across public and private sectors. Continuous improvement of conventional telecommunication networks toward high-speed and flexible 5G and subsequent generations poses new opportunities and novel challenges in many domains, including security. Security technologies for telecommunications have evolved over time with regards to unique capabilities and scalability. The promotion of the cybersecurity mesh architecture (CSMA) emphasizes standardizing security models across disparate systems, while the telecommunication industry has established its own security standards and models. Such large-scale networks contain abundant heterogeneous telemetry data generated by traffic and computing resources in data centers, which can be analyzed to understand suspicious activities and incidents in order to protect the integrity and confidentiality of the networks.

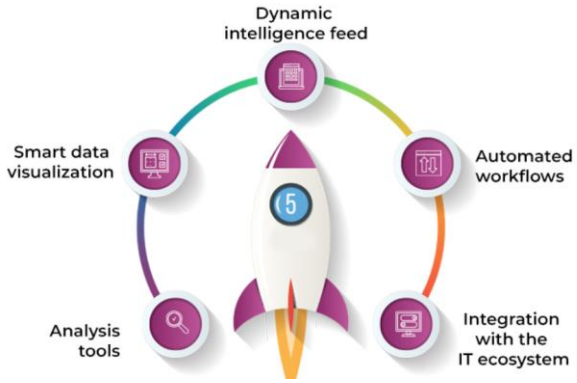

Fig 3 : 5 Must-Have Features of Threat Intelligence Platforms

In addition to localized response behavior, effective proactive prevention, detection, and response measures need a holistic view of network telemetry data from disparate systems in or behind the network perimeter. It is not a rare case for a single piece of telemetry data, when viewed in a small context with its own scope, to seem unintelligible or problematic, but when looked at holistically with surrounding data from different sources and domains, it could be evidence of malicious activities. Thus, the rapidly increasing volume, variety, and velocity of telemetry data require efficient systems for collecting and correlating telemetry data across the attack surface. Cyber

threat intelligence (CTI) is defined as the material that reduces the uncertainty in decision-making processes regarding cyberspace. Based on profiling and understanding the threat actors, their objectives, tactics, techniques, and procedures, better prevention, detection, and response measures can be applied to the attack surface.

4.3. Integration with Existing Systems

Telecom companies must increasingly work together to identify and understand new threats. This requires a bottom-up approach where incidents and indicators related to threats are shared first. Anonymisation and encryption of threat indicators is therefore crucial. Using CANs as a communication network between companies introduces the awareness that information systems should not be compromised. To comply with the requirements of the telecom industry, some parts of C3ISP need adjustments, most notably on the issue of intermediary parties alongside information sharing routes. SLA guarantees and accountability need to be taken into account. The C3ISP architecture must therefore first be refined, after which its functionality can be prototyped.

Privacy-preserving sharing of Cyber Threat Information (CTI) involves many parties exchanging CTI which they want to keep confidential. Countries cooperate by sharing CTI through alliances on a national level. Telecom companies share threat intelligence with peers using Computer Security Incident Response Teams. Threat intelligence platforms are built around sharing CTI from many sources. In many projects it becomes apparent that a dedicated anonymisation service is crucial for end-user groups because threat indicators are sensitive information. Telecom companies focus mainly on detecting small scale attack activities. To ensure a timely intervention these activities have to be identified very early. Many telecom companies therefore built or are building in-house tools that notice their systems. A special implementation of C3ISP must be able to automatically handle analysis requests on CTI.

Equation 2 : System Compatibility Index (SCI)

$$SCI = \frac{\sum_{i=1}^{n} C_i \cdot W_i}{\sum_{i=1}^{n} W_i}$$

- C_i: Compatibility score for component i (0 to 1)
- W_i: Weight or importance of component i
- n: Number of integration points
- SCI: Ranges from 0 (incompatible) to 1 (fully compatible)

Telecom companies have a special interest in threat information about outgoing telecom equipment, which often has unknown and untrustable origins. Even free of charge the equipment might influence the future of the telecom company. Because of the evident high stakes involved anonymous threat intelligence sharing is paramount. Anonymisation and encryption must therefore happen at their gateways. The proposed service focuses on CTI provisioning and sharing, only. Enrichment, deduplication and alert submission account for the rest of its functionality and will possibly be in the scope of follow-up projects. The indivisible need of outside analysis requires the collaborative CTI sharing service to provide an online, transparent and privacy preserving service for all telecom companies wishing to participate on the initiative. Those requirements imply that sharing broadly across telecom companies must be a one way street from an internal perspective. Leaving shaping to the analysis provider completely abstracts from all the details of information sharing to prevent any information leakage. The proposed service focuses on provisioning and sharing CTI only. Anonymisation and encryption must however be done at the telecom companies' gateways to prevent any information leakage.

5. Cloud-Based Solutions

As digital technology and the Internet have advanced, the Communication Technology industry has increased its global significance and popularity. However, threats to the private sector, national economy, and state security have also increased in

this advanced view. These events demand that mobile network operators take necessary protective measures to safeguard their businesses and subscribers.

Traditional security mechanisms are inadequate to deal with contemporary cyber threats. The increasing complexity and massive number of new threats make it impossible to deliver effective detection strategies solely within a telecommunication operator's network. The traditional security defense models that rely on defenses at the perimeter only are no longer effective against cyber-attacks. They must be combined with advanced analytics and enhanced situational awareness for professional incident detection, analysis, and response against emerging sophisticated attacks. The goal of advanced analytics is to generate actionable intelligence from the ever-enlarging volumes of raw data. To meet such performance demands, scalable and high-performance computing can only be built in cloud-based environments.

Equation 3 : Service Availability (A)

$$A = \left(1 - \frac{D}{T}\right) \times 100$$

- D: Downtime during the period
- T: Total time
- Availability is usually expressed as a percentage (e.g., 99.9%)

The threat data can be shared with a threat-intelligence database, improving the broader environment's threat-awareness and giving early warnings to network operators. However, storing a significant amount of activity log and monitoring data presents a big query challenge. As a result, intrinsic data from network devices and pure data of packet flows during traffic capture are sent to remote analysis servers, freeing up storage and improving efficiency. Cloud-based systems provide sufficient performance and lower deployment costs. The international-wide renowned big data analytic method could empower an effective and efficient intelligence analysis engine for a telecommunication operator's lower-level security tier, handling massively big data at one time. Since activity logs must be shared with a server from various Data Generators, a scalable and highly distributed communication protocol has to be designed.

Moreover, cloud-based analysis servers are considered not merely as data processors and higher-layer analysis engines; they are also viewed as trusted service providers. A core trust mechanism must be secured to avoid possible adopted attacks from these analysis servers and false reply results which could lead to serious financial and reputational losses.

5.1. Benefits of Cloud Computing

Cloud computing can be defined as a computing model that proposes a specific set of capabilities of on-demand networks to networks through the internet. In this computing model, the capability of a user can be pursued by almost any possible geographical location regardless of his/her device. Cloud has the same meaning in computing as it is in the telecommunication field which refers to a non-confined and limitless network providing services in a fixed unit of services such as electricity, telegraphy and so on. Building a telecommunication system is extremely expensive. Information is transferred inexhaustibly through fiber optic cables and satellites which are temporal and spatially dispersed. For such networks, maintaining is extremely expensive. Once the infrastructure is put in place information can be distributed across a huge geographic area in extremely short time and at too low a cost that economies and prophecies are unaware of mathematical ways of preventing it [9]. Besides providing a rapid-growth network, distributed systems introduce additional difficulties. First and foremost, the first hurdle of large system design is the communication and distribution problem. A protocol for communication will be needed for synchronous or asynchronous computation as expected. The key is to choose

negligible-time period of computation, negligible probability of failure and negligible range of uncertainty about the current stage. Another trouble of cloud computing is privacy and security of data. When a user's data are stored and processed on someone else's computer, they may be corrupted or compromised. Some means must be formed to ensure that cloud customers' privacy holds. Additionally, minimal capability of a cloud service relies on non-redundant software and hardware not in possession of customers. Some mechanism must be proposed to make sure that their incapacity cannot be used to harm other users or the cloud cash. Designing must be efficient because searching for, processing, or even communicating information in a cloud is pallet of its deployment. A cloud should not be faster on its Client Machine than on its Server Machines.

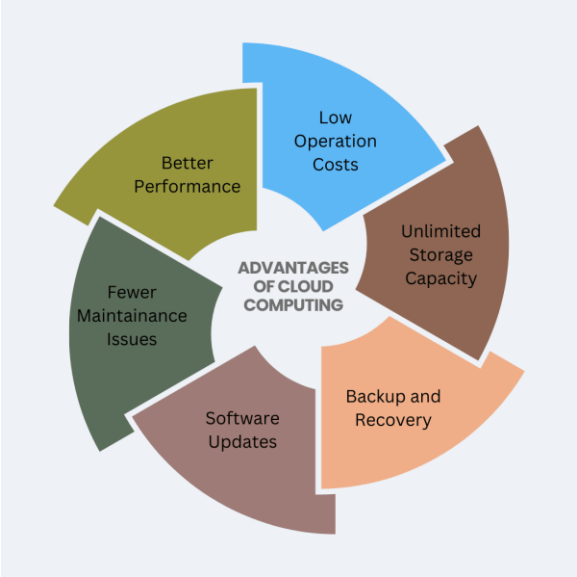

Fig 4 : Advantages of Cloud Computing

5.2. Challenges and Risks

The world of data hosting and processing has experienced a radical evolution over the past two decades. In the past, most organizations maintained thousands of on-premise servers to process and host their data. Recently, however, many organizations opted for co-location facilities or, more recently, adopted infrastructure as a service (IaaS) models in the cloud. The data hosting landscape has transformed from an on-premise architecture process involving several layers of physical and virtual security setups to a cloud process with a shrunken security perimeter. One of the biggest misconceptions is mistakenly considering that utilizing cloud services automatically means gaining improved security]. This 'better security = cloud' myth blinds the cloud customer to the inherent risks residing in the cloud environment, such as lack of control over the infrastructure housing the data, threats toward multi-tenancy environments, or privacy concerns affecting the data stored and processed in a cloud service. Moreover, the threats and vulnerabilities against cloud services can be classified into different areas, including logical security vulnerabilities, risk of data and service obstruction and loss, compliance vulnerabilities, risk of privacy, confidentiality and ownership (the most sensitive area), and vulnerability of dependence on the cloud provider. The cloud environment itself consists of several layers, usually categorizing them as infrastructure layer, platform layer, and software layer, each with its own set of challenges. For the governance of this landscape, the Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR) is the cloud industry's continuously updated directory of cloud computing providers and security assurance. Besides several advantages generally attributed to cloud computing technologies when utilized by modern organizations, a number of challenges are suggested as a response to the growing concern and uncertainty toward security, privacy, and adoption of cloud services all over the world. Modern organizations have to cope with two opposing goals: on the one hand, they are required to increase their competitiveness and efficiency in order to survive in the dynamic business environment by taking advantage of the opportunities that continuous rapid development of technology has brought, including cloud computing technologies; on the other hand, they are faced with the growing risk of cyber crimes that threaten their security and survival. One possibility to satisfy these opposing goals is to utilize cloud-based

security monitoring systems that increase the affordability of security systems by clouding the economy of the service while providing the customers comprehensive security monitoring systems. The major challenges regarding cloud computing application from the security aspect relate to three distinctive phases in the implementation cycle: pre-cloud phase, on-cloud phase, and the post-cloud phase. The pre-cloud phase relates to the risk of transferring the organization's data and their specific characteristics and protection needs to a cloud environment. The on-cloud phase relates to compliance with security and privacy regulations and expectations for personal data handling in the cloud environment. Finally, the post-cloud phase refers to the possibility of cloud service provider termination and the subsequent data transfer or loss.

5.3. Case Studies of Cloud Implementation

The implementation of cloud infrastructure in telecom networks is already happening. It is usually carried out in phases, starting with migration of a single use case of a telecom service. These are usually virtual network functions that can be classified as service functions or infrastructure functions. Space is then created for other functions, potentially owned by third parties. The telecom operator agrees to the standard model so that bookkeeping of the resources can be facilitated by the controller. It also means that every component of the service chain will declare its subscriptions to the controller and the controller forwards this information as advertisements to the broker. Other components only receive this information, without acting upon it, when a service chain is instantiated and service functions need to be connected. Thus there's no chaining yet and would ensure that the service functions are independent. Cloud infrastructure can only take service functions of the initial subscribers. Third-party functions can also be hosted here, but first, they need to be connected to the existing service chain.

The turning point in the design came with the notion of the testing environment. An approach formerly adopted during tests would be to physically copy the cloud infrastructure to another site, including the configuration and its functions. Instead of letting all the installations follow suit, components would be created with no other deployments than a DSS of themselves. All functions would be deployed as single-node instantiations and chained to create the whole operation. Thus the cloud infrastructure remained intact and furthermore, the test run could be switched off and reviewed in the presence of all scripts, simulation nodes, logs, and configuration files. Cloud infrastructure can be put under scrutiny and its functionalities stressed, so it cannot afford to be blind.

The biggest factor fostering management of cloud dilemmas for all parties concerned is likely to be some kind of command and control infrastructure. Such organization does not exist at present nor are companies or any actors willing to found a new one. The idea is that all the potential cloud hosts and consumers could in reality be appointed a reception control tower that moderated information, operation, and integration among these parties so there could be no abuse or fraud. But such organization would likely be both overly expensive and a burden on both parties. Moreover, it would require preemptive decree powers far beyond existing organizations. Thus from a cloud consumer point of view, the control tower may also be pursued as a part of the desire to establish cloud computing in-house.

6. Combining Big Data and Cloud Threat Intelligence

Attack Intelligence is the first sort of threat intelligence classified according to the source of threat. It refers to the indicators and patterns of security threats collected from an information source through intelligence monitoring. The analysis includes collecting, describing, and depicting relevant information,

aggregation/integration of threat intelligence, construction of service interfaces, bi-direction communication with endpoint devices and comprehensive collaboration with general security operation systems in order to control the entire operation process.

Most legacy systems analyze internal log information, such as net flow data or access logs. The information obtained by traditional security monitoring systems, such as IDS, Firewall, Logs and Non-intrusive Analysis, has a deepfulness of days to months, but a breadth of hours to days, and is dispersed by different machines. Neither passive nor active heuristic methods can be applied to the detection of obfuscated attacks. Consequently, with the sophistication and unintelligibility of attacks, the traditional monitoring tools may miss the chance to react. In contrast, Threat Intelligence offers information of not only the target systems, but also of the lifelong experience of attackers. Unlike the traditional monitoring tools, which only provide internal security knowledge, threat intelligence gathers knowledge that is global. Therefore, it can be used at the first time when a new attack is discovered regardless of the target devices, system or type of attack.

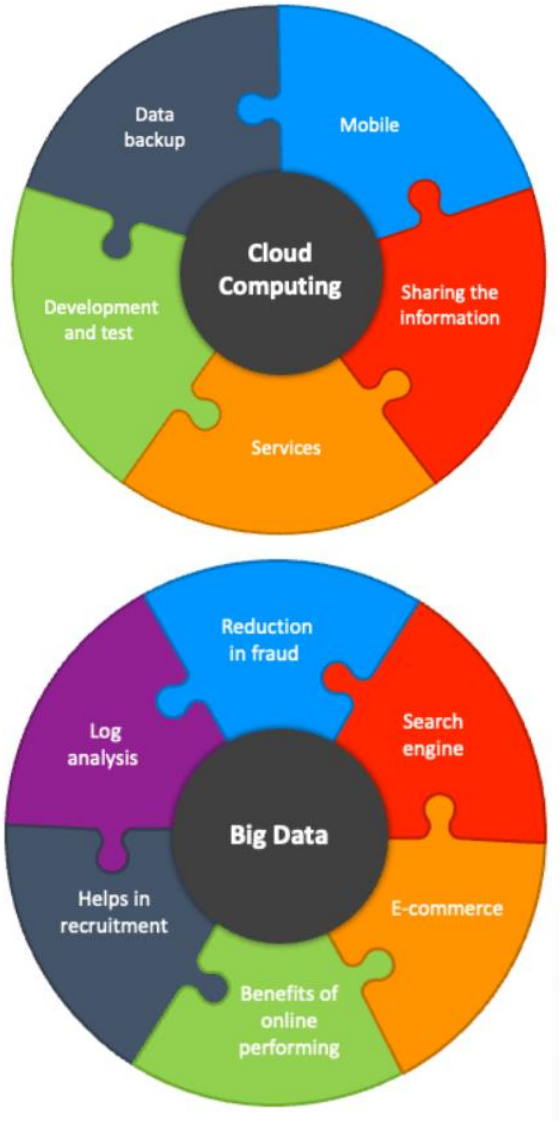

Fig 5 : Big data and Cloud computing

Cloud-based threat intelligence provides a platform for client organizations to share attack intelligence. This architecture proposes three parts of cloud services: an IOC cloud, a content service cloud and a search API cloud. Stateful and stateless log management, as well as plug and play security tool integration, are available to convert relevant history and current logs to IOCs and persistent objects. These convert service blocks are scalable and can also be used to structure and preprocess the local attack intelligence. The cloud vendors have the responsibility to protect the threat intelligence from being exploited by illegal users/clients except for the cooperative parties during the attack intelligence interactions.

6.1. Framework for Integration

The proposed framework can be considered in two levels. At the lower level, an enterprise network control block applied to a single SME's network can be developed, fulfilling the requirements of data collection, storage, and analysis for supporting the decision-making process of that SME. At the higher level, a cloud-based or other third-party control block can be developed. This block will connect several analysis services to cooperative SMEs who will share the CTI data and will receive back processed and more informative intelligence data, for instance correlated with data from other SMEs. To indicate data flow in the proposed framework, two illustrative assignments of possible system architecture scenarios between control blocks were designed. At the lower level, on any SME's premises, data collection and filtering will be executed in real-time inside a dedicated appliance called Threat Data Collector, usually implemented as a dedicated computer or a computer appliance in a more advanced security architecture. The CTI data collected by the dedicated appliances inside the SME's networks are aggregated and processed in IEC blocks that are usually located on a private and secure cloud. It will be acceptable to use an internal SMEs' private cloud but would be recommendable to deploy the system on a public cloud where enhanced external analysis and correlation could be performed. The resulting intelligence data will be sent to other SMEs through a secure PaaS capable of implementing the policy-based information sharing mechanisms designed in the framework. At the higher level, IoT-enabled driven enterprises could utilize the basic features of the framework. Data collection could be performed by several types of harvesters and then forwarded to SME's network control blocks through similar transport network appliances connected as an Internet gateway to the SME's enterprise LAN. The analysis services could also be implemented, one on the enterprise-side at the SME's premises, one in an internal SMEs private cloud, and more advanced in a public cloud where state-of-the-art security analytics could be performed. Thus, SMEs in exchange for their intelligence data could receive enhanced protection strategies and possibly forensic investigations using this shared information. The intelligence data generated by one enterprise could be used to protect others from similar attacks and would implement the concept of global protection.

6.2. Real-Time Analytics

The communications infrastructure has been attacked at an alarming rate in recent years. Security teams have to work at a frenetic pace to keep up with bad actors, leading to a massive overspend and faster-than-expected losses. Telecom companies are collecting tons of data and need to speed up their ability to analyze it. They also need to leverage external insights and analyses. To speed up their understanding of events and flow of insights, telecom security teams need two things: First and foremost, they need data gathering relief – everyday operations that require underlying machine learning that can be customized-endlessly and done in minutes; Second, they need a new way of consuming threats – From point tools that do one thing, they need an unrivalled analyst tool that marries the myriad of insights into one source.

Data protection is necessary more than ever today, especially for telecommunications companies. The telecom sector is a central piece of the ecosystem for IT services, making it a target for many attacks, as well as the first to become aware of most incidents. Attacks targeting telecom datacenter environments have risen by over 80 % in four years. These attacks are usually targeted, leveraging human intelligence, personal contacts, or social engineering to trick security guards, network admins, and other key players into providing access. Exploits also tend to be advanced, as specialized and sophisticated technologies are usually needed to breach telecommunications systems. Even with proper logging and monitoring in place, detection of these events is very difficult. Oftentimes, attackers use the compromised account and become

"indispensable" actors in the network, making it even harder to detect suspicious actions.

Telecom logs and events are also vastly different from conventional IT logs. They can comprise hundreds of attributes that change over time. Events may take seconds, minutes, hours, or years, and new data models and structures may be generated in the meantime. Such rich datasets make the pre-processing of victims a willingness to cooperate a very complex task. Data pre-processing, especially the conversion of proprietary formats, is currently a manual task on a case-by-case basis, making it a lumbering mechanism. As events unfold, it becomes increasingly difficult to keep track of bits gathering data from varied formats. And although these working documents, usually Excel sheets, are vastly useful and insightful, they are usually consumed statically. In the current age, data needs to be visualized as it unfolds. All businesses today need transparency over their assets and chains, and the telecom landscape is no different.

6.3. Predictive Threat Modeling

Security is becoming an increasing challenge in Information Technology (IT), Mobile Communication, Internet of Things (IoT), and Cloud Computing. The Cloud brings several benefits to industries. However, it also becomes a target for exploit by hackers. Security breaches involving top cloud providers' infrastructures impact numerous trickle down industries, and compromise huge datasets. As the attacks become extremely sophisticated and exponentially many, increased complexity of the cloud infrastructure and diverse attacks, defensive means cannot be purely reactive anymore. Instead, it is paramount to develop intelligent cyber security approaches that can proactively predict the risks and better protect the critical cloud infrastructure. Predicting a targeted service compromise is paramount due to its serious and trickle-down consequences, from an estimated 40 million data accounts stolen from a service provider in the United States triggering Facebook's loss of at least $120 billion in healthy share price, to myriad firm closure. Statistically accurate models can provide insights on when to strengthen the preventive countermeasures and informative perspective to the decision makers regarding the most desirable investment on resources in the long term across the infrastructure. Probabilistically modeling a targeted service compromise with the service requests on critical cloud providers is achieved. The historic logs and the network topology are employed to automate critical cloud infrastructures modeling. Random processes for each service influence the requests towards the cloud services modeled in a reactive manner. Coupled with a proposed game theoretic prediction algorithm, prediction of the cloud service risks to be compromised, based on its receipt request distribution and the requests to other services, is made in a proactive manner.

Intelligence based cyber security approaches with predictive ability are vital to creating resilient critical cloud infrastructures. To this end, statistical and probabilistic approaches for predictive threat modeling without human intervention to combat the sophisticated attacks are tailored. These proactive approaches can mitigate risks in the intelligent cyber security systems via guiding and optimizing investments on the defensive controls and countermeasures among candidates based on their predicted impacts on mitigating the risks. Probabilistic modeling of both historical and present observations and pivotal knowledge reasoning on predictions can also be conducted. Potential loss of valuable services and customer credibility can grow dramatically and rapidly, resulting in more severe cascading losses. If intellectual property data such as corporate emails, product plans or employee records are targeted, ramifications on a firm may be catastrophic and insurmountable.

7. Regulatory and Compliance Considerations

In telco cloud environments, there is a need to closely consider regulatory and compliance requirements. Telecom operators and service providers in various industry verticals must meet

complex mandates set by regulatory organizations. These mandates specify safety, reliability, and privacy requirements for public safety, health, and critical infrastructure operators, whereas compliance with such mandates depends not only on operations but also on the underlying infrastructure. In the quest of embracing cloud for implementing applications and services, telecom operators must address a set of new compliance requirements related to the distributed approach of cloud implementations.

Additionally, telecom operators may face several regulatory requirements related to Data Protection Laws, Traffic Monitoring Regulations, Network and Service Security Regulations, specific to-to-customer obligations, Information Security Obligations, and more operational aspects of the network. A majority of telecom regulatory requirements (i.e., 8 out of 13 compliance requirements) are related to communications networks and data centers and are well within the scope of cloud software. By providing a common cloud platform for the telecom veracity cloud along with big data analytic and threat intelligence capabilities, telecom operators can and must support their vertical customers reachable to mandate compliance with regulatory requirements related to cloud infrastructure, proactive security incident monitoring and reporting, and some operational compliance requirements.

It would be a compelling value proposition for a telecom operator to take full responsibility for satisfying Customer Telecommunication Regulatory Requirements through regulated cloud offerings. Through cloud-based Security and Compliance as a Service offerings, telecom operators can serve as defence partners to eliminate or minimize the risks of compliance missteps to financial or reputational losses. Service Level Agreements offered by telecom operators need to go beyond the well studied availability, reliability, and performance metrics and include regulatory compliance. Solution providers operating in the telco cloud environment will also need to consider regulatory compliance requirements for meeting expected services as well as directing lawful access demands.

7.1. Overview of Telecom Regulations

In modern times, telecommunication growth is so rapid that it has created many regulatory frameworks for its governance, in parallel with its growth. Telecommunication Regulation comes into existence to protect the welfare of both the companies and the consumers. Telecom Regulation is the body of Volume, rules or guidelines that control or govern. These guidelines usually compose regulations, commission standards, policies, protocol etc. They help telecom service providers, operators and government to protect their own interest while providing services. As Telecommunication industry is a rapidly growing industry over the last two decades, many Telecommunication Regulatory Authorities have been established worldwide. While some authorities have been established to govern such highly regulated operators, there are many private service providers, which require separate regulations for their proper monitoring. Ministry of Communications & Information Technology out sourced some of its functions of the Department of Telecom to TRAI, which was established as a regulator for the telecom industry similar to the Regulators for Broadcasting, Stock Market and Housing. Telecom Regulatory Authority of India Act was passed on 28 March, 1997 with a comprehensive framework of policies and guidelines for regulation of services. Telecom Regulatory Authority of India has the authority to make laws and regulations for implementing provisions of the Telecom Regulatory Act. Activities of TRAI can be enforced through summary trial procedures. There are provisions of penalties for violation of the decisions or directions of the Authority also. There may be a reference of disagreements or conflict of interest between the service providers and consumers. There are many standard complaints and grievances but all of them cannot be cited here. Some of important keywords

to be included in GRIEVANCE REDRESSAL are Performance Monitoring, Quality of Service Regulation, Service Quality, Naturally Monopolistic, Traffic Regulation, Licensing Policy Basic Service, Value Added Services, were briefly defined. There is a great responsibility on the service providers to maintain service quality and proper grievance redressal mechanisms. In making such rules there is uniformity in the licensing for competitive telecom service. Performance standards are designed by TRAI and they are expected to comply with it. In addition to that, a layman interpretation is expected on the complaints and the judgments provided by the regulatory authorities.

7.2. Impact of GDPR and Other Laws

The European Union's General Data Protection Regulation (GDPR) has adopted a comprehensive view of citizens' data by agreeing on a regulation that would serve as an umbrella under which the various data privacy laws of the member states would come under. GDPR is designed to protect citizens' data privacy and thus impose restrictions on organizations on the use of citizens' data. The GDPR imposes strict penalties on organizations that handle citizens' data and go afoul of the regulations. The regulations must be declared before a contravention occurs, and guidelines must be established on how and when it becomes illegal to collect and use citizens' data . The regulation on the processing of personal data presents a challenge to companies who desire to share cyber threat intelligence. The sharing of cyber threat intelligence (TTPs, indicators, and events) is a widely agreed upon measure for building better cyber defense and helps organizations to understand existing cyber attacks and to react against them. However, threat intelligence very often contains sensitive and identifying information such as IP addresses, email addresses, etc. Persons want to know of threats, but service providers cannot reveal them due to unclear regulations. The challenge for managers of cyber threat intelligence datasets is to comply with GDPR and to avoid GDPR infringements when sharing intelligence.

On May 25, 2018, the European parliament adopted the General Data Protection Regulation (GDPR), the first comprehensive cross-national data privacy law. GDPR takes a comprehensive view by defining personal data as any information relating to an identifiable natural person. GDPR defines three entities that interact with personal data: the data subject, a natural person whose personal data is collected, the data controller, the entity that collects and uses personal data, and the data processor, an entity that processes personal data on behalf of a data controller [20]. Under GDPR, the data controller is primarily responsible for compliance with GDPR, but can appoint a data processor to handle personal data. GDPR has limited exceptions and can only be modified in a more permissive form. GDPR specifies jurisdictional details such as which entities are affected by the regulation and who the regulators are. GDPR enables a range of rights such as the right to access information collected, the right to have information erased, and the right to data portability. GDPR dictates various constraints on how organizations must store and use personal data.

8. Future Trends in Telecom Security

The current telecom security landscape is defined by significant evolution from mostly perimeter- and device-centric with efforts focused on firewalls and upstream filtering to a radically different posture that is inherently cloud and data driven. In this model, device and network security devices provide intelligence and actuators, creating a richly instrumented data ecosystem, and CSPs power the security data lakes, delivered as a service, off which tooling and analysis can be created. Unfortunately, the current telecom landscape has many challenges including multitenancy and siloing in data lakes, small and non-collaborative black holes in cloud security, substantial cloud computing costs for analyses, data drift in analyses and models, persistent disadvantage from near real-time threat

intelligence relevance, hurdle of non-standardized vendor APIs, alarm fatigue from lack of relevance and enrichment, lack of reliable asset exposure from inaccurate management information databases, effective but insustainable manual investigations of black hole detections, and lack of inter-domain visibility. Threat data is one of the most important sources of improving detection and analysis effectiveness to increase the chances of identifying an attack in a vast data set.

The telecom security landscape is anticipated to continue far into the future. Customer-managed RTLs with service-oriented architecture or analytics and visualization as a service may come to fruition or alternatively there may be collaborative data lakes where customer and vendor security intelligence merge and wholesomely analyzed. There may be a strict demarcation between the black box feeds of big tech near real-time machine learning anomaly detection systems and vendor feeds that are enriched with analysis specificity and cooperation with domain experts, investigators, and other stakeholders that act on them. Cloud security analytics is likely to become a service in itself—far removed from data lakes, preprocessing storage, and analysis ones and stressing the applied mathematics of analyses, their computational efficiency, and productizing molds for situational awareness and investigation.

8.1. Emerging Technologies

Emerging technologies include Big Data, Cloud Computing, and Artificial Intelligence. Big Data analytics can satisfy intensive telecom security analytics requirements, while Cloud-based threat intelligence can aggregate, correlate, and analyze massive intelligence data in real-time over large-scale systems. Security as a service can be easily integrated into the existing telco security systems. A novel architecture of telecom security, which consists of an Integrated Data Lake, a Big Data Platform and a Cloud Security Marketplace, can help to elevate telco security to a new level.

Security becomes one of the major concerns of operators as they are undergoing digital transformation. The security requirements increase significantly. Globalization and rapid technological advancements boost the adoption of digital services by consumers and enterprises. Meanwhile, this change poses a risk to the security of the business ecosystem as cyber assaults exploit Connected-Device Vulnerabilities. Therefore, there is a higher demand for telco security. It requires protecting potential threats from various layers of services. Broad Telecom Security covering across services, namely network security, cloud security, data security and end-point security is required to fortify and detect the associated Potential Threats. Security as a core competency is needed for operators as leading telecom security players. Telecommunication operators, as the main providers of network infrastructure for governments, enterprises, and public-owned organizations, play a key role firstly to secure the country. It is reported that 5G would theoretically come with new potential threats to the telecom security landscape. Advancements in AI would simultaneously improve the effectiveness of cyber-attack tools.

To cope with massive data volumes, Big Data and AI are either adopted by security vendors or advanced criminals in threat detection and identification (TDI). With state-of-the-art technologies, Security Information and Event Management (SIEM) and analysis tools can be provided to Security Operation Centers (SOC) to monitor signals, check compliance, perform incident investigation and threat hunting (TH), etc. Telcos have been providing these security analytics products for a decade with a focus on the telecom domain. However, due to the increasing attacks targeting telecom operators, the defensive capabilities based on intensive analytic requirements have been weakened due to high resource consumption.

8.2. The Role of AI and Machine Learning

Artificial Intelligence (AI) and Machine Learning (ML) applications have shown great promise in various fields. Telecom operators have turned to these technologies to defend their networks and minimize potential risks. On the one hand, due to the variety of data and the multitude of incidents to detect, ML has been considered as the most suitable solution. On the other hand, Telecom operators have been trying to centralize the security datasets, events, and alerts they receive from their various systems in a common SIEM (Security Incident and Event Management) system. As a consequence, Threat Intelligence Companies suddenly appeared on the market, proposing cloud services to analyze behavioral data from different networks and share the results with various incidents detected on multiple customers' networks. The combination of telecom operators' decision to centralize their security data and the promises of these new cloud-based services have led most of the operators to massively outsource their threat detection platform.

The integration of AI/ML applications for cybersecurity in a digital ecosystem at the enterprise level is a complex undertaking. This is a key challenge in the effort to secure Smart Infrastructures and Digital Industries by utilizing the advantages of AI/ML tools. The industrial information integration concepts and techniques developed over the past decades could help to effectively integrate AI-enabled cybersecurity models into complex enterprise systems. However, even if data-driven ML models have demonstrated great performance in cybersecurity domains, the application of ML in cybersecurity consideration still raises many challenges. First, ML models generally require large volumes of high-quality data to be effective, while datasets on cybersecurity are often small with respect to the required data volumes. Even when large volumes of data are available, security datasets are often imbalanced, with many more examples of normal behavior than of attacks. It is very difficult to obtain a well-distributed dataset containing examples of all existing attacks. In addition, ML models need to be able to interact effectively with various different applications and systems in an enterprise. The integration of AI-enabled security solutions in practice is further challenged by the dynamic and complex nature of modern network environments, where traffic patterns and attacks change continuously over time. The large amounts of network flow data in modern networks necessitate the use of ML models at the edge of the network for effective and efficient graph processing of data.

9. Challenges in Implementation

Telecommunication Systems have several Security Mechanisms to provide Integrity, Confidentiality, Authentication, and Data Availability in 5G and Before versions but at the same time, they are become large Data sources. Data exchange, Mobility and Volume growth become a challenge for Telcos as well as Authorities. With the Views and Statistics provided, ATS and GSOC Officers become frequent report generators, and the big challenge is to extract useful information in rapid time. All these problems exist due to the proliferation of 'Big Data'. A combination of Big Data Analytics and Cloud Based Threat Intelligence Solutions can provide a good security posture for Telecom Operators. Presenting an action plan would enlighten how all these Security Collaboration Platforms (SCP) and Security Analytics Systems can be implemented.

Telecom Operators, Telecom Equipment Manufacturers and Cloud Providers are key stakeholders for the implementation of the security analytics systems. In Pre-requisite phase, all the precautions like Security Compliance, Conformance Testing, Network Hardening, Pre-emptive Actions, Scripting controls, and Fletcher checks would be put in place so that there would be no risk of Attack and Security Incidents. After that, Data Extraction, Data Validation and DLT would take place for long term retention, followed by the deployment of Header Extraction Tools and Development of Parsing Loggers for Real Time Extraction of the logs, which send the logs to Target Servers and

Store Logs in Locally . All the Action would take place at Network Operation Centre (NOC) level. Next, Security Analytics & Correlation would be implemented. Here, the verification and validation of Common Event Format (CEF), JSON and Syslog Forwarders would take place with Elucidation of Storage Architecture and in-house Reporting Solutions. Design & Development of On-Premises Security Analytics Systems would happen in Development Phase. Parsing Engines, Analytic Processing Scheduler and Third party Query Handler Life Cycle would be developed before Deployment & Migration (Cloud & On-Premises Setup). These Cloud Based Security Intelligence Systems for Cloud Log Views, Security Posture Indicators & Third Party Threat Intelligence would be leveraged by Telcos.

Federating Security Features using the Cloud to share Threat Intelligence between Telcos in a Secure manner without Loosing the Privacy and Confidentiality is a challenge for Cloud and ACT Officers. Security features from multiple Telecom Operators, Telecom Equipment manufacturers, and Cloud Providers can help to detect a threat in near real time and mitigate the damage. Besides that DumPede Forms, CTI feeds, and Information sharing is a challenge for Telcos as the only telecom data feeds may not help to identify the Threats better.

9.1. Technical Barriers

Huge volumes of data on all types of network entities can be collected and efficiently analyzed using advanced Big Data analytics technologies to gain insights for intelligent decision making. It includes security analytics around identify deception issues like DDOS, XSS, HLS vulnerabilities and fraud detections [24]. Cloud-based threat intelligence services provide security knowledge on a subscription basis to organizations. Focus areas of such services include domain name system (DNS) reputation, IP reputation, URL reputation, malware variant intelligence, real-time domain generation algorithm detection, threat actor intelligence and other sources. These external threat intelligence services can be applied using web services/APIs to enhance security monitoring and analysis.

Key challenges include the inability of many current products to accept Big Data analytic-driven intelligence (compared to simpler SIEM-driven intelligence); the lack of industry standards on how intelligence is structured; real-time usage of intelligence (i.e. creating and sharing effective responses); the ability to operationalize intelligence sharing (i.e., moving from a sandbox to an operational environment and consistently generating useful insights); the maturity of threat intelligence; untrustworthy sources and the ability to distinguish “real” threats from fabrication and FUD; incomplete or non-standardized intelligence; sharing platforms; ignorant analysts; determining value generated from intelligence usage and sharing; and lack of external validation. Cybersecurity strategy management, a top-down approach for cyber vulnerability risk assessment and remediation, is essential for any organization that is seriously involved networking. It involves identifying potential hackers, estimating their capabilities, understanding critical assets within the topology and estimating risk metrics.

The analysis uses graph theory to formulate the topological problem, and a generalized Peters-MacMillan iterative approach to solving it. Technically, existing products lack the capabilities and infrastructure to ingest raw threat intelligence from online threat sharing communities, a true Big Data problem. The volume and velocity of MITRE’s LIST and STIX threat intelligence formats are significant challenges for many incumbent industry players. Those who cannot keep pace with the rapid evolvement of the threat intelligence space will be heavily disadvantaged within five years.

9.2. Organizational Resistance

When confronting the prospective cognitive consequences of such proposals or risk actions, engineering managers encounter resistance from

various organizational horizons. The first proposed option is regarded as an opportunity-loss barrier, or a realist or more adequately a realist-investment scenario. It is likely that a real the 5G intelligent network architecture platform investment situation, the other service provision opportunities would attract strong advocacy to gain corporate or business unit approval. The second proposed option enables overt gains of value from acceptance of the risk governance effort. However, resistance can rather likely arise from counter interests with other analytic related functions. The responses to counter opportunity loss and governance resistance on risk action proposal options are conceptually summarized in Table 26. Risk-assessment criticism responses are adapted from the analysis of the social and demographic biases, human heuristics, the human cognitive limitation impact on technical predictions, and risks scenarios belief contagion modelling analysis. On the other hand, the practical suggestions are developed from meta-cognitive processes and operating principles from deliberation and cognitive reflection studies, and practical settings observations on the AI requirement analysis case study.

There remains practical challenges in offering the obtained suggestions. Currently, the existing conception of audit and visors used for technology impact understanding and governance only focused on unfolding the implicative and prospective impacts of artifacts being employed or their scenarios being considered but not the pre-built understanding or design patterns and properties perspectives to understand the artifact being considered for the risk action proposal. Quite likely, cognitive assistance by an external resource is required. Besides, there can be cognitive assisters available to offer this.

10. Best Practices for Telecom Security

Telecom operators should adopt an Industry-wide risk and threat assessment framework, including guidelines for risk assessment and outlining the actions the telecom operator should take in response to specified risks . This framework can be used in a generic manner by telecom operators across the world and will encourage them to invest in security and build appropriate cybersecurity measures. Telecom operators should adopt an Industry-wide Architecture for Security Operation Centers, outlining best practices for the monitoring, detection, investigation, and mitigation of security incidents. This generic architecture can be used continuously by all telecom operators to materialize the Measurement and Response phase and drive maturity improvement of their monitoring and detection, investigation, and mitigation capabilities. Telecom operators should adopt an international Industry Forum on Cybersecurity with the mission to share threat intelligence and best practices.

Using Open-Source Software and Hardware for cybersecurity applications will significantly improve MTTR and TCO for detection and mitigation applications. Telecom operators should adopt industry standards for Security Patch Management, describing the processes and the products that need to be patched within what timeframe. Telecom operators should introduce Security Risk Management by establishing an Asset Risk Register, a 24/7 security incident detection and monitoring organization, a Security Incident Response Plan, Security Incident Response Teams with all needed roles, a Security Organization with necessary expertise, and disclosing recommendations and threats to the internal organization and telecom industry organizations. Telecom operators are necessary to set-up security management for compliance with laws and regulations. It includes certification for Audit Companies, Security Policies, IRP and DRP procedures, Security Awareness training for employees, Knowledge sharing and using Multi-Level Security education test environments, Security Requirements for products and processes, and a Risk and Threat Assessment methodology for suppliers.

10.1. Developing a Security Culture

The necessity for a strong security culture continues to increase as organizations become fully aware of the risk presented by employees and contractors. Cyberthreats utilizing various social engineering techniques are consistently mentioned in the daily news. Insider threats were cited as a concern by nearly half of the respondents in an online survey conducted. The computing view of enterprise security provides a clear introduction to security considerations that need to be made as technology is introduced. However, this view is not sufficient to provide a comprehensive business or organizational view of security culture. detailed a thorough analysis of a specific organization's security culture and concluded with recommendations for managerial actions that would strengthen the organization's security culture. To determine the managerial actions that can be taken by any organization in any sector to develop, promote and sustain a positive security culture, and subsequently measure the impact of these actions, a series of investigations were undertaken.

This work highlights six levers for managers to use such as building cybersecurity expectations in performance evaluations and reward systems, enforcing consequences for insecure performance, creating strong communications plans, and providing ongoing training and updated opportunities for learning about increased cybersecurity activities. All are actions any manager in an organization can take to strengthen cyber resiliency. Further, when management creates a position specifically dedicated to creating a cybersecurity culture, they can expect to see results that increase resilience in the organization. Increasing cyber-resilience is on every executive agenda, and this project will help leadership teams and all levels of management identify specific ways they can aid their organization in achieving this objective. Cyber-resilience is a multi-faceted challenge that requires techniques and technologies from a variety of different sectors.

10.2. Continuous Monitoring and Improvement

The threat landscape is constantly evolving and TLP monitoring implementations must continuously adapt, monitor and improve the underlying platform architecture and analysis algorithms in order to counter that threat landscape with relevance. TLP should consider identifying and classifying the verification and monitoring events that should take place. TLP may benefit from using a n-tier approach to verification and monitoring. Similarly to the development of analysis algorithms, the architecture monitoring infrastructure may be realized in two overarching building blocks: a detection engine and a visualization/workflow engine. The detection engine is responsible for receiving events related to the system being monitored, and for continuously updating the knowledge base. The visualization and monitoring engine is responsible for the visualization and notification of detected issues, and to allow user interaction with the knowledge base and event log. The work on TLP technology enhancement would likely benefit by recognizing performance issues and code flaws in existing TLP implementations.

The target audience for expected outcomes includes both enterprise and vendor telecommunications network operators. The envisaged technical platform could be directly implemented by large operators, leveraging their extensive in-house expertise in security related fields. Smaller operators often lack such capabilities, which makes definitive analyses inaccessible to them. For this audience, TLP technologies would be incorporated into implementation of security tools, highlighted as innovations and supplying a competitive advantage. A secondary audience includes academic researchers with an interest in cybersecurity, telecommunications security, and natural language understanding. They may benefit from the research component of the outcomes and be encouraged to continue research along similar lines. This added benefit may also account for the selection of certain prototypes. Select outreach to public bodies, industry organizations, and vendor neutral industry engagements could also be considered in order to

ensure the technical platform is disseminated to a wider audience than operators alone.

TLP products with presence in wide-scale use are a viable product entry point into the telecommunications domain. Commercializing TLP products would not only potentially off-set significant funding, thus allowing for further investment into refining and enhancing their capabilities and performance, but also for exposing TLP technologies in places where they can do the most good. Namely where they may be most relevant to read and combat Telecom-targeted threats. This is an area of shared-market interest between privately funded initiatives, who wish to limit unregulated exploitation of their TLP technologies, and government funded initiatives who wish to protect the telecommunications domain from potentially catastrophic consequences.

11. Case Studies

In recent years, a number of cyber case studies have been investigated to illustrate the threat landscape endured by telecom operators worldwide. Moreover, some of such events have been studied to better understand aspects such as how large scale attacks work, their impact on the infrastructure and how the involved operators managed to recover their services.

Telecom service providers are increasingly targeted by hackers. While attention may be diverted to the growing frequency of sophisticated distributed denial of service (DDoS) attacks, attacks exploiting a telco's internal operations have the potential for far greater damage and disruption.

Not only are telcos responsible for the routing of voice calls and other communications between people, they have complete visibility of the relationships between mobile phone subscribers. Equally important is the mobile IP network where subscribers access the internet and interact with TV, sport, e-commerce, financial and other services. Attacking the telecom operator in its situation function means increasing the global yield of an attack.

The more sophisticated attacks can’t be diffused or filtered using out-of-path mitigation services or even in-path appliances. These attacks, instead, are only spread in a limited area, where they are in-path.

11.1. Successful Implementations

There are many examples of cloud-based CTI systems that are commercially available: some have a proven track record and others are still testing their technology with beta clients. Technical capability is not necessarily the most relevant factor in selecting a vendor; when looking for third-party CTI analysis capabilities, a client organization will weigh other criteria as seriously, if not more seriously. The quality of service offerings, how responsive the vendor is, the climate of collaboration and partnership, the vendor's financial viability, and whether or not any sanctions are against the vendor organization will weigh heavily on the decision.

A client will appoint a clear Account Management lead, who will act as the main point of contact for the vendor(s), coordinating communication, priority resolution, and managing the settings and accessibility of cases. The vendor will also appoint a dedicated vendor side Account Management lead, who will be fully versed in the client’s work. To aid in uptake and improvement of service, it is important to appoint a well-motivated and engaged internal core user group that can advocate for how the service can enhance and evolve over time with user feedback. It is important to have a small, well-defined scope of work that is achievable within the time and budget constraints of the pilot period.

Focus on case types that would typically take a long time for the client to resolve themselves. Specify desired outcomes and ways of measuring them. During negotiations, it is helpful to normalize costs and expectations based on the scope of work offered, the prices paid for alternative techniques, and the expected return on short- and long-term investments. Identify a single dedicated source of

CTI consumption and regular reporting for the client organization to acknowledge.

11.2. Lessons Learned from Failures

The dilemma faced by an information administrator in providing assurance to external users, who might demand absolute confidentiality, integrity and availability of information, is a very delicate balancing act - one that very often does not end well. It is important to remember that information risk does not arise because the information administrator has done something wrong. No information manager makes an intentional default with any of the required precautions in protecting information assets. New accounts of information breaches appear almost daily in the news about unreputable actors gaining unauthorized access to sensitive information and data. Similarly, reports of federal security breaches almost doubled in just four months, rising from 26 to 55 incidents from July to November 2010. Twelve organizations suffered large personal data incidents, exposing over 30 million records.

Target Corp's breach of data security exemplifies a scandalous breach event]. Beginning on Black Friday; and once the investigation was conducted, it was revealed that the data security breach began weeks prior using a vendor compromise - malware was installed in-store point of sale card swipes - data was exfiltrated - the breach was not contained for 6 days, - 40 million credit card records in terms of security exposures. In its wake, Target lost a staggering $1 billion in costs associated with the breach, and the company, now reborn as a fully new form of organization, and its CEO along with the CTO lost their jobs.

Inappropriate information dissemination, transmission, transmittal or sharing can be damaging to individuals, corporate organizations and nations. Publicity surrounding the reputation of institutions, governments and even whole countries can be seriously damaged by misinformed/incorrect information. The credit rating of a firm may drop, the bankability of a country to secure loans from an otherwise charitable benefactor may be endangered. On a more micro-level, improperly shared detailed personal information can endanger the life of an individual. Business may be detrimentally compromised by security breaches involving phishing attacks for donor cards/credit cards - the unsuccessful exploitation of a financial services vendor file containing personally identifiable information or even payment-related outputs that reached the public domain.

12. Conclusion

In the next ten years, the telecoms market will see a dramatic increase in the amount of data it collects. Big data could enhance data network traffic classification and provide a clear unfair use of a Subscriber Identification Modules (SIM) card in the telecom sector. In terms of next-generation networks, operators must adapt to various standards and support or negotiate users' mobile handovers for real-time seamless service continuity]. Telecoms need to rethink how to efficiently manage and analyze different types of cloud, signal, application, user, and devices data to improve predictive maintenance. Digital signal-based data from cloud radio access networks offers possibilities for radio pattern anomaly detection. In contrast, application service-affiliated data can optimally allocate server resources and achieve efficient delivery in service-based devices relying on cloud or edge computing platforms. During the last ten years, everything has shifted towards a cloud future, in which telecom companies are in the weightless ICT service business in this new environment. The telecommunications industry continues to focus on the deployment of cloud-based core networks and have matured moving application, user, and network functions to public, edge, and private cloud servers. The virtualization of reactive, adaptive, and proactive workload management properties unlocks telecom companies' potentials in machine learning-driven next-generation cloud intelligence. Open-RAN-based approaches are also paving the way for operators in control of the accessibility of relevant

radio data collection and analysis. These technological upgrades and paradigm shifts allow companies to use bigger data and diverse sensing arrays for monetizing telecom network services and developing new cybersecurity and privacy protection solutions. While the telecom network edge needs to be controlled and protection-focused, the bigger opportunities lie in how companies share intelligent telecom cloud services.

References:

1. Chava, K., Chakilam, C., Suura, S. R., & Recharla, M. (2021). Advancing Healthcare Innovation in 2021: Integrating AI, Digital Health Technologies, and Precision Medicine for Improved Patient Outcomes. Global Journal of Medical Case Reports, 1(1), 29–41. Retrieved from https://www.scipublications.com/journal/index.php/gjmcr/article/view/1294
2. Nuka, S. T., Annapareddy, V. N., Koppolu, H. K. R., & Kannan, S. (2021). Advancements in Smart Medical and Industrial Devices: Enhancing Efficiency and Connectivity with High-Speed Telecom Networks. Open Journal of Medical Sciences, 1(1), 55–72. Retrieved from https://www.scipublications.com/journal/index.php/ojms/article/view/1295
3. Avinash Pamisetty. (2021). A comparative study of cloud platforms for scalable infrastructure in food distribution supply chains. Journal of International Crisis and Risk Communication Research , 68–86. Retrieved from https://jicrcr.com/index.php/jicrcr/article/view/2980
4. Anil Lokesh Gadi. (2021). The Future of Automotive Mobility: Integrating Cloud-Based Connected Services for Sustainable and Autonomous Transportation. International Journal on Recent and Innovation Trends in Computing and Communication, 9(12), 179–187. Retrieved from https://ijritcc.org/index.php/ijritcc/article/view/11557
5. Balaji Adusupalli. (2021). Multi-Agent Advisory Networks: Redefining Insurance Consulting with Collaborative Agentic AI Systems. Journal of International Crisis and Risk Communication Research , 45–67. Retrieved from https://jicrcr.com/index.php/jicrcr/article/view/2969
6. Singireddy, J., Dodda, A., Burugulla, J. K. R., Paleti, S., & Challa, K. (2021). Innovative Financial Technologies: Strengthening Compliance, Secure Transactions, and Intelligent Advisory Systems Through AI-Driven Automation and Scalable Data Architectures. Universal Journal of Finance and Economics, 1(1), 123–143. Retrieved from https://www.scipublications.com/journal/index.php/ujfe/article/view/1298
7. Adusupalli, B., Singireddy, S., Sriram, H. K., Kaulwar, P. K., & Malempati, M. (2021). Revolutionizing Risk Assessment and Financial Ecosystems with Smart Automation, Secure Digital Solutions, and Advanced Analytical Frameworks. Universal Journal of Finance and Economics, 1(1), 101–122. Retrieved from https://www.scipublications.com/journal/index.php/ujfe/article/view/1297
8. Gadi, A. L., Kannan, S., Nandan, B. P., Komaragiri, V. B., & Singireddy, S. (2021). Advanced Computational Technologies in Vehicle Production, Digital Connectivity, and Sustainable Transportation: Innovations in Intelligent Systems, Eco-Friendly Manufacturing, and Financial Optimization. Universal Journal of Finance and Economics, 1(1), 87–100. Retrieved from https://www.scipublications.com/journal/index.php/ujfe/article/view/1296

9. Cloud Native Architecture for Scalable Fintech Applications with Real Time Payments. (2021). International Journal of Engineering and Computer Science, 10(12), 25501-25515. https://doi.org/10.18535/ijecs.v10i12.4654
10. Pallav Kumar Kaulwar. (2021). From Code to Counsel: Deep Learning and Data Engineering Synergy for Intelligent Tax Strategy Generation. Journal of International Crisis and Risk Communication Research , 1–20. Retrieved from https://jicrcr.com/index.php/jicrcr/article/view/2967
11. Chinta, P. C. R., & Katnapally, N. (2021). Neural Network-Based Risk Assessment for Cybersecurity in Big Data-Oriented ERP Infrastructures. Neural Network-Based Risk Assessment for Cybersecurity in Big Data-Oriented ERP Infrastructures.
12. Katnapally, N., Chinta, P. C. R., Routhu, K. K., Velaga, V., Bodepudi, V., & Karaka, L. M. (2021). Leveraging Big Data Analytics and Machine Learning Techniques for Sentiment Analysis of Amazon Product Reviews in Business Insights. American Journal of Computing and Engineering, 4(2), 35-51.
13. Routhu, K., Bodepudi, V., Jha, K. M., & Chinta, P. C. R. (2020). A Deep Learning Architectures for Enhancing Cyber Security Protocols in Big Data Integrated ERP Systems. Available at SSRN 5102662.
14. Chinta, P. C. R., & Karaka, L. M.(2020). AGENTIC AI AND REINFORCEMENT LEARNING: TOWARDS MORE AUTONOMOUS AND ADAPTIVE AI SYSTEMS.