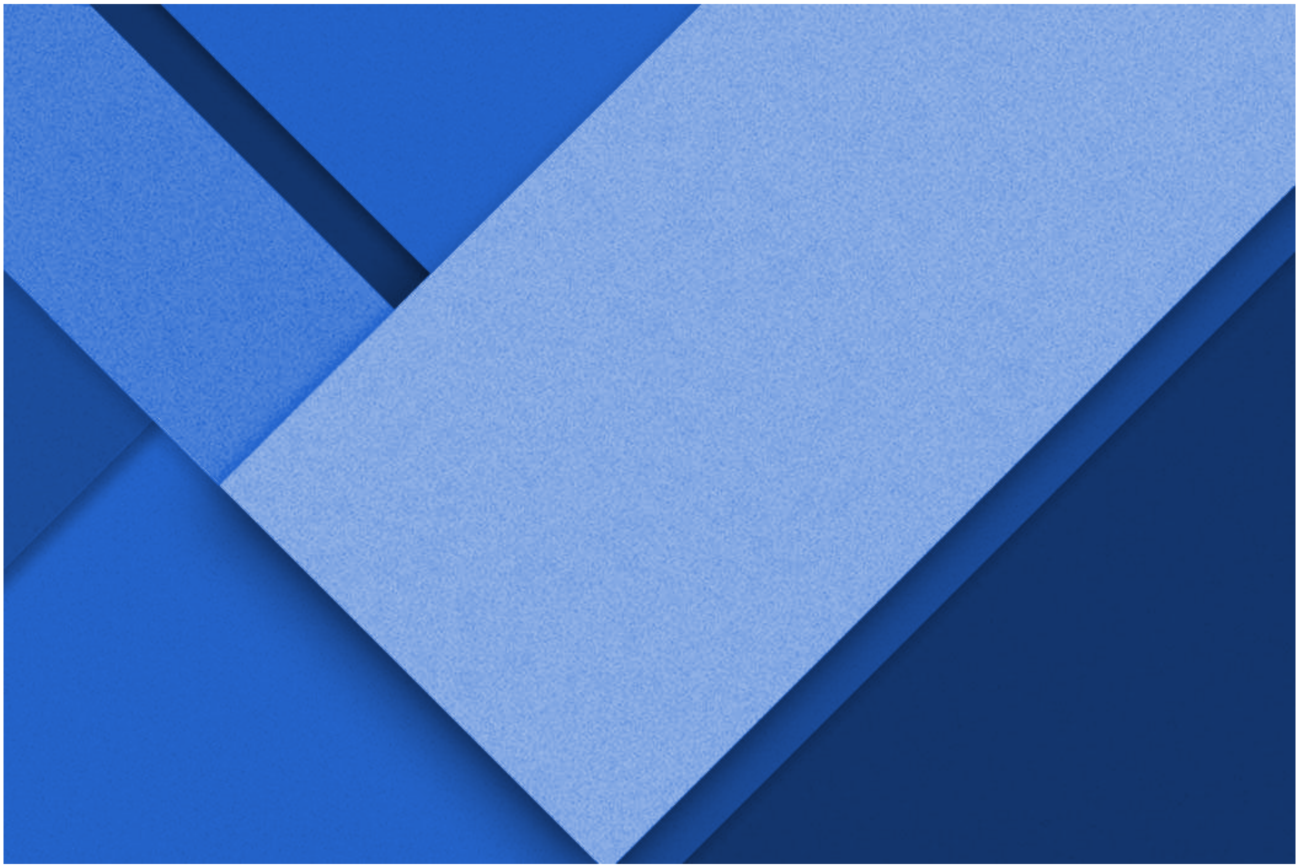


Final Project Report

A Survey on Trusted Computing In Mobile Networks

—

Submitted by Group 5
Christabelle Alvares (cda5542)
Shivangi Sharma (ss1695)
Shubham Verma (sv4168)

Date of Submission
Dec 13th 2022

Table of Contents

1. Introduction & Problem Statement

Mobile communication has entered our day-to-day life in almost every way we interact with the digital world. With continuous development in wireless cellular technology, we have come from the 1st generation of mobile networks to the fifth generation, which we now call 5G. Growing sophistication in technology subsequently demands a strong trust model to keep communications secure and efficient.

There is a need for trusted computing principles to be implemented in the domain of security for mobile network technologies. However, much more research into this field seems to be required as attack surfaces increase and there is no shortage of threats. Many of the works chosen for our survey deal with these problems using different security technologies and models such as blockchain, zero-knowledge proof, etc. in combination with TPMs (Trusted Platform Modules) and TEEs (Trusted Execution Environments) to secure the entire mobile architecture and network components. The main issue addressed by trusted computing is the need to store the secrets like cryptographic keys in a trusted and secure environment. In mobile devices, this is where TEE comes into play. Trusted computing for mobile communication also deals with privacy, not just of users, devices, and traffic, but also of the network itself.

In our current telecommunication system (4G), much improvement to the security architecture has been made, to a highly successful degree. However, one trust issue relates to the verification of actual subscribers. An example highlighted by Wong explains the case in which “the network devices or elements could be stolen by a social engineer, but in the system, the record still indicated the identity of the subscriber which is incorrect information” [1].

When the newer 5G communication is combined with advanced network technologies like NVF (Network Functions Virtualization) and cloud computing, it provides unmatchable capabilities like high speed and connecting to a maximum number of edge computers. To reiterate, high capabilities come with threats and security risks. Wong describes the attack surface by pointing out, “As a result [of the combination], one might face various levels of trust issues in between mobile network operators (MNO), tenants, end-users, subscribers and different types of service and infrastructure providers” [1]. One of the major attacks which come with NVF is because of corrupted hypervisors that can lead to problems like escalation of privileges. Other associated problems include authentication and data privacy which can lead to the leakage of private data of citizens like health, media, et cetera during communication.

In this project, we aim to contribute a detailed survey about how trusted computing has evolved over the years and provide ways to implement trust and security in mobile communication networks starting from 3G, to 5G. Our work will identify trends in trusted computing research for mobile communication and highlight the various techniques explored in the field. The technologies which we are majorly considering for the comparisons are – Blockchain, Network Functions Virtualization, Subjective Logic, Cross Chain Computing, Mathematical models like Big Data and Bayesian Networks, and PKI. We will also compare the papers according to the root of trust they have used, for example, whether they have used TEE or TPMs as the RoT or they have defined some new Root of Trust. Also, we have considered the main security issue which the papers are addressing by implementing the technologies and RoT.

2. Related Literature

Mobile network technologies like 3G and 4G, despite being an old form of communication now as the world moves to 5G, are still widely used in many parts of the world where 5G infrastructure is not set up yet. In this section, we produce summaries of papers chosen for our survey. In this section, we first discuss the security requirements and architecture required or used in 4G systems. We then focus on the same aspects for newer 5G network architectures, which pose different challenges to previous mobile communication designs.

The work by Zheng et al. [2] discusses the security requirements for 4G networks across domains like security requirements on Mobile Equipment & Universal Subscriber Identity Module, security requirements on radio interface and network operator, security visibility, security configuration, and security scalability. The authors provide an analysis of trusted computing in a mobile platform. The authors describe how more efforts are included in developing security schemes for 2G/3G networks while mobile equipment remains open to many backdoor attacks, viruses, and breaches of sensitive data. The paper also discusses 4G security architecture and framework based on TPM and Public Key Infrastructure. The authors propose TMP-Based Hybrid AKA (Authentication and Key Agreement) Scheme which is more secure, scalable, and convenient to handle security issues that come with 4G networks [2]. Another work from the same authors further describes a hybrid AKA and authorization scheme [3]. In this scheme fingerprint is used in parallel to public key infrastructure to provide authentication between user, Mobile equipment, home environment and universal subscriber identity module (USIM) [3].

Describing the work by Ming-fu et al. [4] stresses the security requirements related to an all-IP network and provides an analysis of the related threats to the existing security measures in a 4G network. The authors argue that only improving security mechanisms and protocols to provide security to air interfaces is not enough and the security of a mobile network should depend on a secure terminal environment. Hence, they propose a trusted computing framework scheme by creating a trusted computing environment for the mobile terminal which helps by providing integrity of software and validity to software using access control.

The work by Yingyou et al. [5] concentrates on trusted computing technology and threats faced by 3G networks and proposes an architecture of a trusted mobile platform that is based on the mobile trusted module. The authors also propose a formal analysis method which deals with the defects in secure booting and how it can be improved.

Moving on to 5G, we look at some key points regarding trusted computing as mentioned in [6], "In 5G, the trust assumptions are different than in previous standards, like 3G or 4G. Most notably, the level of trust the system needs to put into the SNs has been reduced. One important property provided by 5G is that an SN can no longer fake authentication requests with the HNs for subscribers not attached to one of its base stations" [7]. As mentioned in our previous section, the corrupted hypervisor attacks lead to the compromise of confidentiality, integrity and availability of data. For this the authors suggested the TPM - for the root of trust for the securing the integrity of booting time and making the TPM as the requirement for the further steps like remote attestation. They suggested the use of TEE for the software trust of NFV. In this work, the authors highlighted the importance of the TPM and TEE. They described for securing the integrity of NFV and VNF, TPM would be accurate during the boot time. However, for runtime, securing the confidentiality with the integrity, TEE would be best for the introspection risks. Also in the communication phase of 5G and beyond, encrypted transmission services like TLS - TPM would be good to secure the encrypted keys [7].

The work by Yang et al. [8] aims to address the security risks posed by heterogenous MEC (mobile edge computing) systems by proposing their own distributed blockchain-based trusted architecture. Their proposed BlockTC deals with privacy protection of the topology, which they claim is an often-ignored aspect of multidomain collaboration. They propose verification schemes that do not require the disclosure of private domain information during the collaboration. Their work focuses on multi-server trusted routing and privacy protection using certain designs – backup dual links, distributed ledgers and collaboration routing consensus. These features allow for the maintenance and verification of MEC collaboration without exposing privacy across the network and data consistency with the blockchain ledger [8].

Similarly, Kholidy et al. [9] proposed a blockchain based decentralized trusted computing platform for secure data sharing between the edge devices. In this work, BTCP addresses the problems and threats during the sharing of spectrum. They used the ZKP (Zero Knowledge Proof) technology in which the blockchain platform will use the edge devices resources and track the reputation of the particular device on which the BTCP will make decisions whether the communication can happen or not. They created two parts - first one - Lightweight blockchain platform - in which they presented detailed tentative protocol which is followed by the edge devices and MEC for getting subscription from Omnipurpose Edge Chain - OEC (which is basically the blockchain platform which was using the edge devices resources). The second part - An incentive based reputation management - this part of the blockchain platform deals with the tracking of the changes happening to the reputation of the devices, computation needs and the changes in peers or participants [9]. He et al. also use blockchain; their work focuses on how to maintain trusted computing during the cross-chain process in their proposal of a cross-chain trusted scheme for multi-chain 5G networks [10].

Zhiming et al. developed a subjective logic model based - 5G Intelligence Network Trust Model, for detecting the data credibility in 5G communication [11]. The authors combined the 5G Intelligence Network Trust Model and the Josang Subjective logic and created a trust model to solve the issue of data credibility, that is the trust of data (uncertainty) in 5G communication in a dynamic environment. They extended the features of the Subjective Logic model, since the model itself is not able to address the 5G communication credibility in a dynamic environment. In the end they simulated the model and the output proved to be highly efficient.

[12] The authors addressed the security issues in the 5G neural host where the NFV is used to reduce the cost of operation and when sent to the edge computers in MEC. For addressing these issues, the authors proposed the enhancement in edge computing in which they used the ARM based edge computers to secure the privacy and data that the citizens share on the network, for example the photos, files, health data et cetera. The 5G City VIM and NFVs are based on the virtualization security in which the edge devices are based on ARM technology, hence providing the authentication and security. At the base of these technologies lies the VOSYSmonitor, which divides the system into ARM TrustZone in the edge computers for enabling the TEE to implement TCB (virtualized). This virtualized TCB is used to store the cryptographic keys and the secrets, and provides to Edge computers through predefined API calls. Additionally, we look at remote attestation implementations as discussed by Oliver [13].

As 5G is a new technology, many researchers have concerns about security issues which could be a huddle in the fastest mobile network. Authors in [14], have intensely analyzed the issues and also suggested the research directions for security professionals to take security issues into consideration. In [15], the author proposed a TEE as a Service framework TEEaaS the combination of cloud and TEE, a cloud service for making it easier for customers to use the 5G technology. Some authors combined the 3GPP and O-RAN technologies with 5G to address the issues of privacy and security issues [16]. IoT-based 5G networks can be made more robust by using a modified version of the AES algorithm, as proposed by authors in [17], where the encryption of the data in transit in the 5G network could be made faster and more secure. In [18], the authors addressed the ” user-controlled privacy” attribute that could be included in 5G mobile networks by using the concept of distributed systems, establish with the help of trusted third parties.

3. Threat Landscape in 4G and 5G Mobile Networks

The threat landscape for 4G and 5G communication is vast and the vectors are many as can be seen in Figure 1 [28].

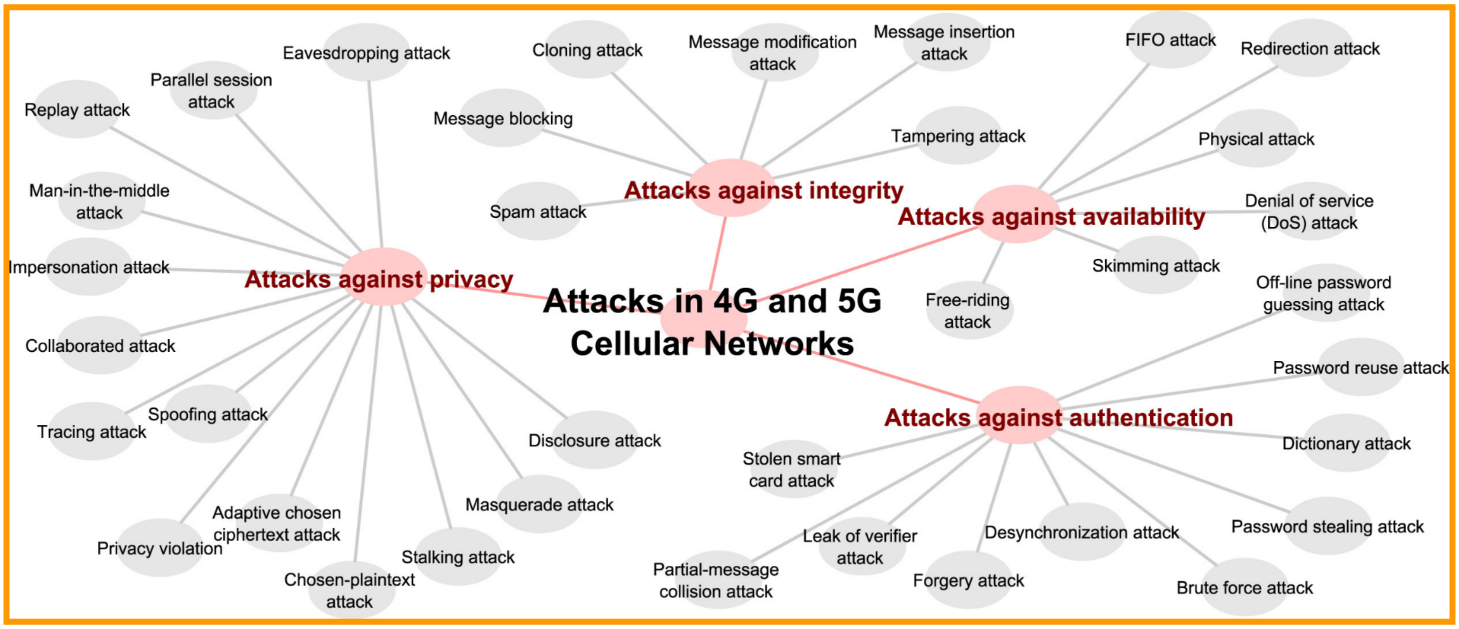


Figure 1: Threat Landscape in 4G and 5G Mobile Networks [28]

Ferrag et al. give a description of four categories of attacks in 4G and 5G communication networks:

Attacks against privacy

The goal of this category is to classify 14 different attack types which consist of eavesdropping attack, parallel session attack, replay attack, Man-In-The-Middle (MITM) attack, impersonation attack, collaborated attack, tracing attack, spoofing attack, privacy violation, adaptive chosen ciphertext attack, chosen-plaintext attack, stalking attack, masquerade attack, and disclosure attack. The most dangerous among these attacks is the MITM attacks due to it being on the False Base Station attack. This attack has a malicious third-party masquerading as a real network's Base Transceiver Station. MITM attacks are a particular form of replay attacks and replay attacks can be easily detected by checking timestamps in a card-based password authentication and key agreement scheme. So, research was conducted to confirm if MITM attacks could also be detected using timestamps. The privacy-preserving authentication scheme found that though checking timestamps was insufficient to detect MITM attacks, it was necessary to use private keys that are unknown to the attackers.

Attacks against integrity

This category focuses on the classification of six attack types which are, spam attack, message blocking, cloning attack, message modification attack, message insertion attack, and tampering attack. Manipulation of exchanged data between 5G access points and mobile users is the foundation of integrity-based attacks. Cloning attacks are based on a man-in-the-middle rouge BTS which has access to the cross-layer information. It performs the cross-layer attack on the 5G network by initially conducting passive sniffing of uplink and downlink channels. This is followed by parsing 5G control messages and extraction of cross-layer information. Finally, attack vectors such as a BTS cloning attack or physical layer jamming attack is created.

Attacks against availability

Six attacks are classified within this category, and they are, First In First Out (FIFO) attack, redirection attack, physical attack, skimming attack, and free-riding attack. The main goal of an availability-based attack is to render a service as unavailable. The FIFO attack can be initiated by an adversary after gathering the enter and exit time intervals. The redirection attack can be launched by the adversary when they are able to collect the relevant user entity information by increasing the signal strength or through the impersonation of a base station in the 4G and 5G networks. Free-riding attacks are considered a serious threat to 4G and 5G networks as they can limit the availability of device-to-device communication.

Attacks against authentication

This category deals with the classification of ten attack types, namely, password reuse attack, password stealing attack, dictionary attack, brute force attack, desynchronization attack, forgery attack, leak of verifier attack, partial-message collision attack, and stolen smart card attack. Authentication-based attacks are focused on disrupting the client-to-server authentication and vice versa. Password stealing and reuse attacks aim to disrupt the password-based authentication by having the attacker impersonate a legitimate user and attempt to login on the server. The attacker uses a dictionary of different words to guess the correct password. An attacker that can steal a user’s smart card, is then able to extract all the personal stored user information without any passwords. This is a form of off-line guessing attack and stolen smart card attack.

4. Classification of Technologies and Addressable Issues

Technologies used in Trusted Computing for Mobile Networks

From our literature review, we have identified the main technologies used to address the key security issues relating to 4G and 5G technologies, as shown in Figure 2:

Blockchain: Blockchain is way to securing cryptocurrencies. Blockchain is a secure type of ledger. Blockchain help in organizing and distributing the ledger into blocks. Here each block contains transaction data like the receiver, sender, amount, block hash and hash of previous block in the sequence (can also be considered previous transaction block). Hence if anything in a block is modified, the block hash gets modified, and the next block will no longer have a matching previous block hash which protects ledger from fraud and theft.

Network functions virtualization (NFV): As we are moving more towards virtualization, Network functions virtualization (NFV) provides a way in which we can replace the network appliance hardware with virtual machines. This helps in separating the communications services and the hardware devices like firewalls. Now one can provide new services without updating or installing the hardware. Virtual services are also less expensive and don't require specialized hardware to run.

Subjective logic is a calculus for probabilities which considers epistemic uncertainty with source trust into account. Subjective logic is used when you have systems or situations having uncertainty and unreliability. **Network Trust model** using subjective logic helps us determining that the data used in a transaction is credible or not.

Cross chain computing helps in sending messages, transferring tokens, initiating actions across any network. Cross chain computing helps different independent blockchains to communicate with each other and share data.

Public Key Infrastructure can be defined as collection of all the hardware, policies, software, procedures, etc which are used to manage, create, modify, distribute, and store public keys and certificates. It uses asymmetric encryption to provide confidentiality and authenticity of the user or device.

Network Slicing helps network operators manage a network by distributing network into a set of logical networks where each network is supposed to have a well-defined purpose. Network slicing helps achieve isolation, provide better security and service flexibility.

Trusted Execution Environment is an isolated part of the CPU or any processor which runs independent of operating systems or any application. Trusted Execution Environments help process secure data, provide cryptographic functions execution, and help deal with secrets by providing a secure environment.

AAA in networking stands for Authentication, Authorization, and Accounting which helps in access control of resources of a system. Authentication stands for identifying the user, Authorization is the level of access the user has to access the resources and Accounting helps in keeping track of all resources shared for a given time.

Zero Trust Model is basically trusting no one and everyone whether identified within a system or not has to be authenticated and authorized every time while giving access to the data or applications of a system. Every device, user, application, third party, etc is always treated as an untrusted source.

Physical layer Encryption is a way of encrypting the physical layer which is responsible for transmission of data over a wireless or wired medium. Using encryption all the data transmitted including but not limited to IP addresses, personal data, port, etc is encrypted and protected from the outer world.

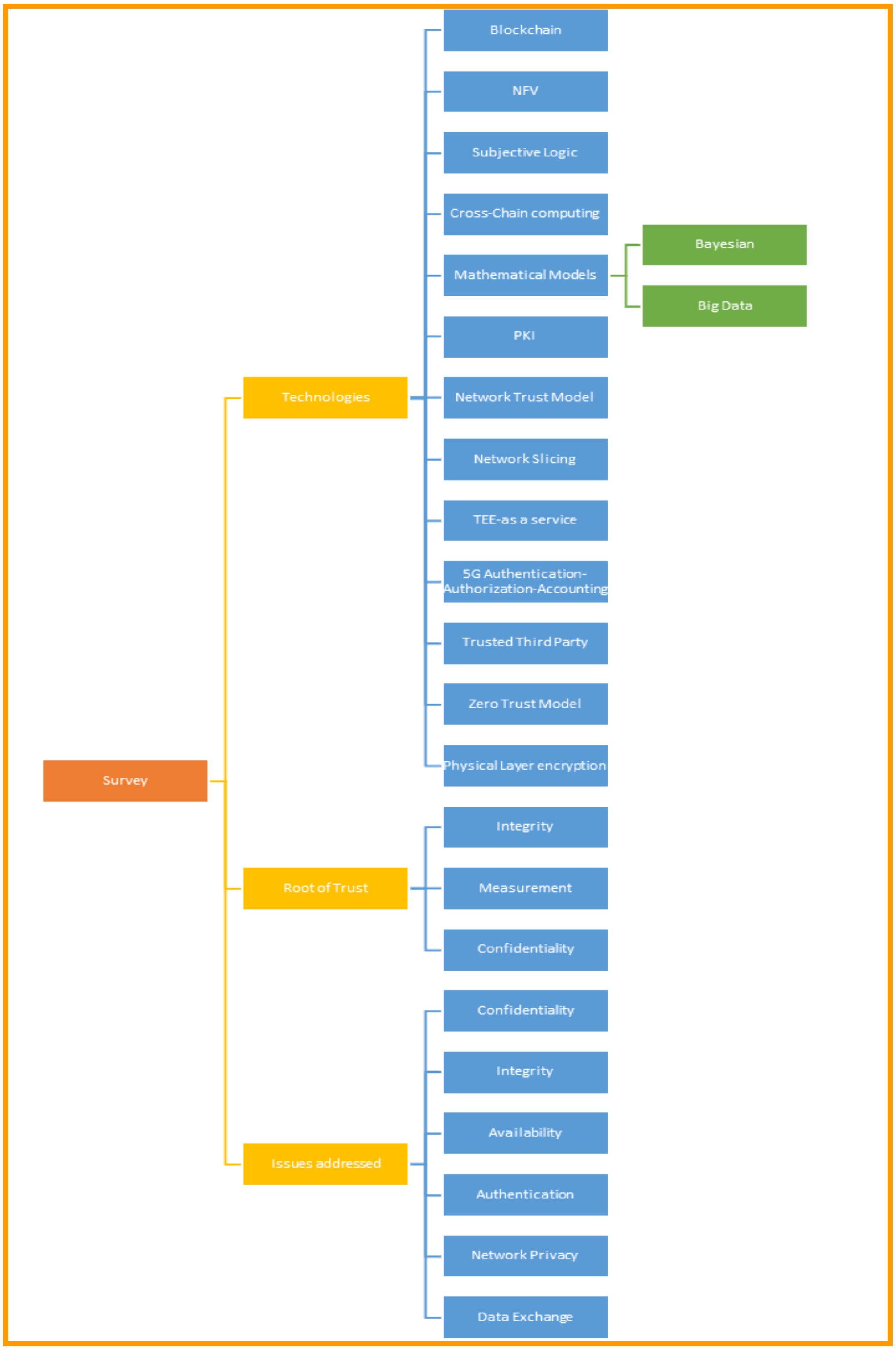


Figure 2: Classification of Technologies and Addressable Issues

Categories of Addressable Issues

Based on our literature review, we have additionally identified the most significant issues that plague 4G and 5G technologies, broadly categorizing them into the following:

- Confidentiality of Data
- Integrity of Data
- Availability of the Network
- Authentication
- Privacy of the Network
- Data Exchange between Components in the Network

Figure 2 depicts these addressable issues, of which many are standard when discussing security solutions. However, with 5G network architectures, a novel area to be addressed comes into play - 'privacy of the network'. Trusted computing for mobile communication must also deal with privacy of the network structure, in addition to that of users, devices, and traffic. This may include ensuring that information about the components in a network are not leaked. In MEC, topology information must be confidential between domains. For example, Yang et al. [8] gives examples such as node connection relationships, traffic information on links, resource utilization in the current network, etc. The authors explain the importance of this, "Once the privacy leakage occurs, criminals can obtain the complete topology data to analyze the traffic status to track user behavior and steal data by disguising as computing nodes, etc., which will do great harm to the MEC system." Moreover, we add another important category of issues, which relates to the process of data exchange between components in the network.

5. Discussion of Current Trends and Analysis of Trusted Computing Principles

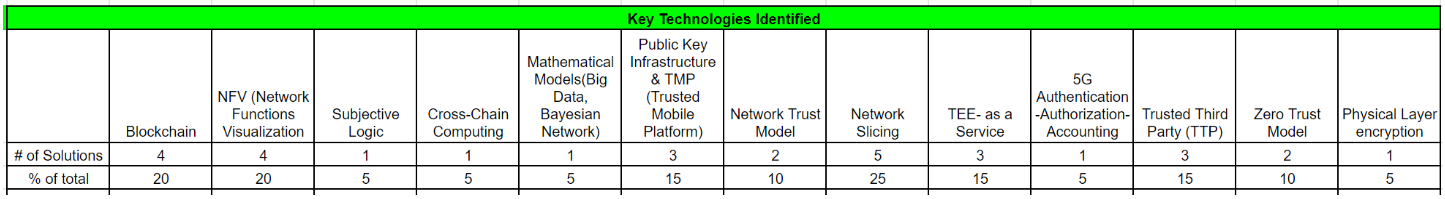
In this section, we analyze 20 proposed solutions in the literature for 4G, 5G and beyond. The below table shows a list of these research solutions:

Research Paper Title	Reference Number
Distributed Blockchain-Based Trusted Multidomain Collaboration for Mobile Edge Computing in 5G and Beyond	[8]
Cross-chain Trusted Service Quality Computing Scheme For Multi-chain Model-based 5G Network Slicing SLA	[10]
Trust, security and privacy through remote attestation in 5G and 6G systems	[13]
An Overview of Proactive Forensic Solutions and its Applicability to 5G	[19]
Trusted Execution Environment-Enabled Platform for 5G Security and Privacy Enhancement	[15]
Towards 5G Zero Trusted Air Interface Architecture	[16]
Secure Spectrum and Resource Sharing for 5G Networks using a Blockchain-based Decentralized Trusted Computing Platform	[9]
5G Intelligent Network Trust Model Based on Subjective Logic	[11]
Trust in 5G and Beyond	[7]
Edge Computing Enhancements in an NFV-based Ecosystem for 5G Neutral Hosts	[12]
The Fifth Generation (5G) Trust Model	[1]

Trusted Computing-Based Security Architecture For 4G Mobile Networks	[2]
AKA and Authorization Scheme for 4G Mobile Networks Based on Trusted Mobile Platform	[3]
A Scheme of Mobile Platform Based on Trusted Computing	[5]
Design and implementation of mobile trusted module for trusted mobile computing	[20]
A Security Architecture for 5G Networks	[21]
Security Trust Zone in 5G networks	[31]
5G Visions of User Privacy	[18]
Security Measures in IOT based 5G Networks	[17]
A Trusted Mobile Phone Reference Architecture via Secure Kernel	[22]

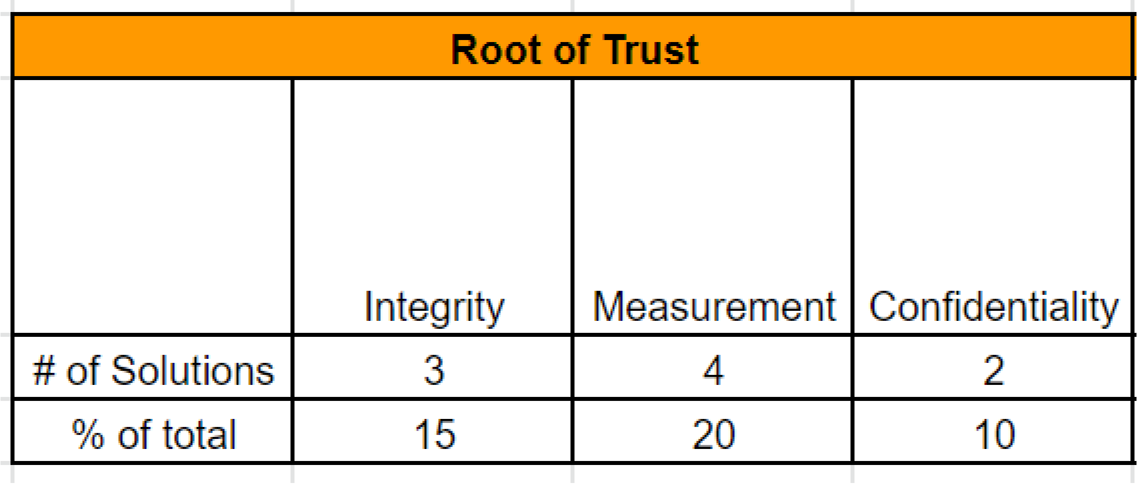
Table 1: List of Papers Analyzed

After analyzing 20 solutions proposed for 4g, 5g and beyond, we inferred some trends in technologies used, issues addressed, as well as the occurrence or mention of the root of trusts, as shown by Figure 2.



	Key Technologies Identified												
	Blockchain	NFV (Network Functions Visualization	Subjective Logic	Cross-Chain Computing	Mathematical Models(Big Data, Bayesian Network)	Public Key Infrastructure & TMP (Trusted Mobile Platform)	Network Trust Model	Network Slicing	TEE- as a Service	5G Authentication -Authorization-Accounting	Trusted Third Party (TTP)	Zero Trust Model	Physical Layer encryption
# of Solutions	4	4	1	1	1	3	2	5	3	1	3	2	1
% of total	20	20	5	5	5	15	10	25	15	5	15	10	5

Table 2: Analysis on Key Technologies

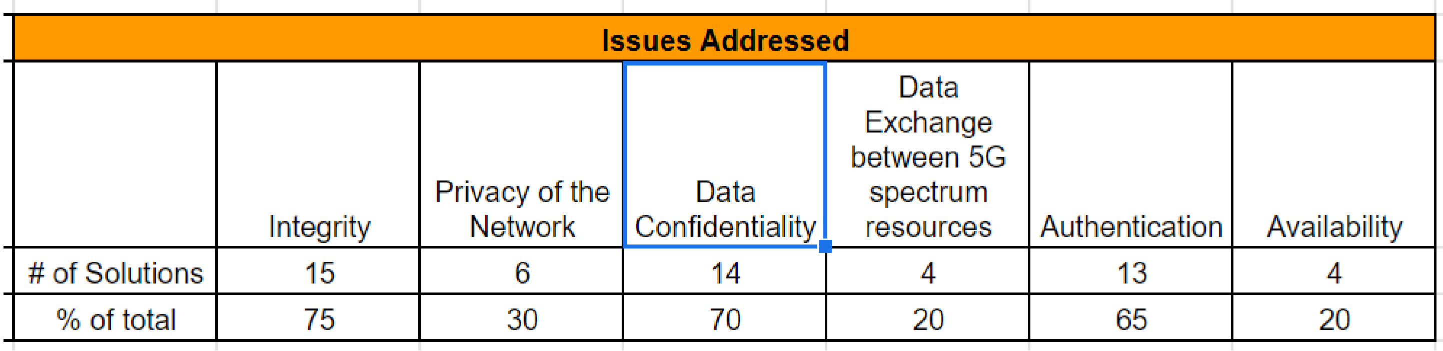


	Root of Trust		
	Integrity	Measurement	Confidentiality
# of Solutions	3	4	2
% of total	15	20	10

Table 3: Analysis on Root of Trust

PKI and TMP were explored for 4G but we see the research moving in a different direction since focus has shifted to 5G. NFV, Blockchain and network slicing are very prevalent trusted technologies, mostly for 5G solutions. In the statistics, we see the use of multiple of these solutions in one proposed work. We also see new techniques like Cross-Chain Computing, Network Trust Model with Subjective Logic, enhancing 5G (Authorization, Authentication and Accounting) AAA model, Physical layer encryption are some ways in which 5G network, security and privacy issues solutions are implemented. The most widely used technique for 5G networks is Network Slicing. This technique allows multiple virtualized and independent 5G networks creation on a common physical system or infrastructure which is widely useful for 5G networks as we move towards software defined networking.

Another focus of our analysis is the emphasis that many of the works reviewed do not delve too much into trusted computing keyphrases - Root of trusts, minimizing the TCB, etc. As you can see from table 3, there is very little mention or focus on the root of trusts although some of the solutions counted here are due to their use of TEEs and TPMs in their proposed architecture.



	Issues Addressed					
	Integrity	Privacy of the Network	Data Confidentiality	Data Exchange between 5G spectrum resources	Authentication	Availability
# of Solutions	15	6	14	4	13	4
% of total	75	30	70	20	65	20

Table 4: Analysis on Root of Trust

Based on Table 4, we can see that the most addressed issues are integrity of data and confidentiality and authentication. However, certain issues such as availability, network privacy (a newly popularized issue with 5G) and effective data exchange between various 5G components in the proposed work are not addressed very poorly.

This leads us to our major conclusion; the specific field of "Trusted computing for Mobile Networking" needs to have design principles, definitions of components and formal structures/standards laid down. With a formal model and structure such as this, research in the field will be more consistent and could be useful as guidelines. This solves the problem of solutions only addressing certain areas, instead of solving the problem as a whole, adding a higher value to the research community.

6. Challenges and Future Work

In our literature review, we discovered that research in trusted computing in mobile networks is not as comprehensive as it should be, especially with further deployment of 5G on the horizon. The threat landscape is very different from 3G and 4G technologies since software-defined networking (SDN) is being implemented primarily in 5G. Considering our survey on trusted computing technologies used in mobile networks, the majority of the concentration of papers surveyed has been on 5G. 2G/3G/4G has papers ranging from early 2000s, with technologies already evolved and after introduction of Trusted Mobile Computing with TEEs a variety of security issues were resolved.

Considering 5G despite being widely used there are still a wide variety of security and privacy issues that needs to be addressed. Although in the papers surveyed we can see 5G networks being used with blockchains, in cross chain computing, network slicing which increases the threat model exponentially. One of the major use cases has been with blockchain. In relation to blockchain itself is vulnerable to a variety of attacks. 51% attacks, phishing attacks, routing attacks, blockchain endpoint vulnerability, Sybil attacks, etc. Blockchain also faces a big scalability issue. Other areas where 5G is under threat is decentralized security, reduced isolation in 5G networks, network vulnerabilities since 5G uses HTTP and TLS, vulnerabilities carried on from 4G/3G networks and requirement of new hardware for 5G functionality, since 5G is not backwards compatible.

There are a lot of privacy issues that the solutions we've reviewed are trying to address. It's not just user privacy and data security that's the concern; now privacy of the network itself is important, i.e. ensuring that knowledge about the network topology is not leaked. Mobile networking is closely related to IoT & MEC and we see a lot of overlap in our review. Future research will be following IoT & MEC (mobile edge computing) as their use of machine learning and AI is increasing.

7. References

[1] S. Wong, “The Fifth Generation (5G) trust model,” 2019 IEEE Wireless Communications and Networking Conference (WCNC), 2019.

[2] Zheng, Dake, Weichi, Tang “Trusted Computing-Based Security Architecture For 4G Mobile Networks”, Sixth International Conference on Parallel and Distributed Computing Applications and Technologies (PDCAT'05).

[3] Zheng, Dake, Weichi, Tang “AKA and Authorization Scheme for 4G Mobile Networks Based on Trusted Mobile Platform”, 2005 5th International Conference on Information Communications & Signal Processing.

[4] Ming-fu, Ai-qun “A Security Framework for Mobile Network Based on Security Services and Trusted Terminals”, 2011 7th International Conference on Wireless Communications, Networking and Mobile Computing.

[5] Yingyou, Xuena, Shuyi, Hong “A Scheme of Mobile Platform Based on Trusted Computing”, 2010 International Conference on Computational Intelligence and Security.

[6] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, “A formal analysis of 5G authentication,” Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 2018.

[7] Benzaïd, Chafika, Tarik Taleb, and Muhammad Zubair Farooqi. "Trust in 5G and beyond networks." IEEE Network 35.3 (2021): 212-222.

[8] H. Yang, Y. Liang, J. Yuan, Q. Yao, A. Yu, and J. Zhang, “Distributed blockchain-based trusted multidomain collaboration for Mobile Edge Computing in 5G and beyond,” IEEE Transactions on Industrial Informatics, vol. 16, no. 11, pp. 7094–7104, 2020.

[9] Kholidy, Hisham A., et al. "Secure Spectrum and Resource Sharing for 5G Networks using a Blockchain-based Decentralized Trusted Computing Platform." arXiv preprint arXiv:2201.00484 (2022).

[10] Y. He, C. Zhang, B. Wu, Y. Yang, K. Xiao, and H. Li, “Cross-chain trusted service quality computing scheme for multi-chain model-based 5G network slicing SLA,” IEEE Internet of Things Journal, pp. 1–1, 2021.

[11] Zhiming, Diao, et al. "5G Intelligent Network Trust Model Based on Subjective Logic." 2021 IEEE International Conference on Power Electronics, Computer Applications (ICPECA). IEEE, 2021.

[12] Baldoni, Gabriele, et al. "Edge computing enhancements in an NFV-based ecosystem for 5G neutral hosts." 2018 IEEE conference on network function virtualization and software defined networks (NFV-SDN). IEEE, 2018.

[13] I. Oliver, “Trust, security and privacy through remote attestation in 5G and 6G systems,” 2021 IEEE 4th 5G World Forum (5GWF), 2021.

[14] Sicari, Sabrina, Alessandra Rizzardi, and Alberto Coen-Porisini. "5G in the internet of things era: an overview on security and privacy challenges." Computer Networks 179 (2020): 107345.

[15] Valero, José María Jorquera, et al. "Trusted Execution Environment-enabled platform for 5G security and privacy enhancement." Security and Privacy Preserving for IoT and 5G Networks. Springer, Cham, 2022. 203-223.

[16] Sun, Sheng, et al. "Towards 5G Zero Trusted Air Interface Architecture." arXiv preprint arXiv:2211.03776 (2022).

[17] Dey, A., S. Nandi, and M. Sarkar. "Security measures in IOT based 5G networks." 2018 3rd International Conference on Inventive Computation Technologies (ICICT). IEEE, 2018.

[18] Sorensen, Lene Tolstrup, Samant Khajuria, and Knud Erik Skouby. "5G visions of user privacy." 2015 IEEE 81st vehicular technology conference (VTC Spring). IEEE, 2015.

[19] A. Nieto, “An overview of proactive forensic solutions and its applicability to 5G,” 2018 IEEE 5G World Forum (5GWF), 2018.

[20] Mooseop Kim, Youngsae Kim, Hongil Ju, and Youngsoo Park, “Design and implementation of mobile trusted module for trusted mobile computing,” 2010 Digest of Technical Papers International Conference on Consumer Electronics (ICCE), 2010.

[21] G. Arfaoui, P. Bisson, R. Blom, R. Borgaonkar, H. Englund, E. Felix, F. Klaedtke, P. K. Nakarmi, M. Naslund, P. O'Hanlon, J. Papay, J. Suomalainen, M. Surridge, J.-P. Wary, and A. Zahariev, “A security architecture for 5G networks,” IEEE Access, vol. 6, pp. 22466–22479, 2018.

[22] X. Zhang, O. Acıiçmez, and J.-P. Seifert, “A trusted mobile phone reference Architecture via Secure Kernel,” Proceedings of the 2007 ACM workshop on Scalable trusted computing - STC '07, 2007.

[23] M. A. Bouazzouni, E. Conchon, and F. Peyrard, “Trusted mobile computing: An overview of existing solutions,” Future Generation Computer Systems, vol. 80, pp. 596–612, 2018.

[24] N. Asokan, J.-E. Ekberg, K. Kostiainen, A. Rajan, C. Rozas, A.-R. Sadeghi, S. Schulz, and C. Wachsmann, “Mobile trusted computing,” Proceedings of the IEEE, vol. 102, no. 8, pp. 1189–1206, 2014.

[25] D. Ganesan, M. Y. Sharum, N. F. Mohd Sani, and N. A. Mohd Ariffin, “A survey on advanced schemes applied within Trusted Platform Modules (TPM) and iaas in cloud computing,” 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), 2021.

[26] M. Eckel, A. Fuchs, J. Repp, and M. Springer, “Secure attestation of virtualized environments,” ICT Systems Security and Privacy Protection, pp. 203–216, 2020.

[27] R. Khan, P. Kumar, D. N. Jayakody, and M. Liyanage, “A survey on security and privacy of 5G technologies: Potential Solutions, recent advancements, and future directions,” IEEE Communications Surveys &amp; Tutorials, vol. 22, no. 1, pp. 196–248, 2020.

[28] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, “Security for 4G and 5G Cellular Networks: A survey of existing authentication and Privacy-Preserving Schemes,” Journal of Network and Computer Applications, vol. 101, pp. 55–82, 2018.

[29] A. Dutta and E. Hammad, “5G security challenges and opportunities: A system approach,” 2020 IEEE 3rd 5G World Forum (5GWF), 2020.

[30] C. X. Shen, H. G. Zhang, H. M. Wang, J. Wang, B. Zhao, F. Yan, F. J. Yu, L. Q. Zhang, and M. D. Xu, “Research on trusted computing and its development,” Science China Information Sciences, vol. 53, no. 3, pp. 405–433, 2010.

[31] Bin Han, Stan Wong, C. Mannweiler, M. Dohler, and H. D. Schotten, “Security Trust Zone in 5G networks,” 2017 24th International Conference on Telecommunications (ICT), 2017.