FEATURES OF THE ORGANIZATION OF THE ARCHITECTURE OF THE INTERNATIONAL SYSTEM OF IDENTIFICATION OF MOBILE DEVICES BASED ON IMEI CODES

Davronbekov Dilmurod[1], Isroilov Jamshid[1]

[1]Tashkent University of Information Technologies Named after Muhammad al-Khwarizmi, Tashkent,Uzbekistan.
E-mail: jamshid@mail.ru

K E Y W O R D S

IMEI, GSMA, CEIR, EIR, mobile networks, device identification, cloning, mobile operators, blacklist, whitelist

A B S T R A C T

This article examines the architectural features of the international IMEI (International Mobile Equipment Identity)-based mobile device identification system in modern telecommunications networks. It analyzes the interactions between equipment manufacturers, the global GSMA association, centralized CEIR systems, and operator registries (EIRs). The processes of registration, verification, and data exchange between international and national equipment identification levels are examined. Particular attention made to mechanisms for identifying cloned and duplicated IMEIs, ёas well as issues of ensuring the security of data transmission channels. A structural model of a distributed IMEI control system with elements of centralized analytics and international information exchange is proposed. The results of the study demonstrate that the integration of the GSMA, CEIR, and EIR can significantly improve the level of mobile network security and reduce the risks of exploitation of illegal devices.

INTRODUCTION

Modern telecommunications networks are characterized by a high degree of global integration, the rapid development of mobile technologies, and a constant increase in the number of connected devices. The widespread use of smartphones, IoT devices, and smart terminals significantly increases the demands on mobile equipment identification, control, and security mechanisms. Under these conditions, the task of reliable device identification is becoming one of the key challenges of modern mobile communications systems.

IMEI monitoring systems are widely used by telecom operators, international telecommunications organizations, and government regulators to enhance information security and network infrastructure reliability. This technology is particularly relevant given the increasing incidence of IMEI spoofing and cloning, which can lead to disruptions in identification processes and unauthorized access to mobile services. [1]

The IMEI control architecture is a distributed, multi-tiered system that includes equipment manufacturers, international GSMA databases, centralized CEIR (Central Equipment Identity Register) systems, operator EIR (Equipment Identity Register) systems, and mobile operator networks. Interaction between these elements ensures centralized equipment control, the creation of global blacklists, and the rapid identification of suspicious devices.

Additionally, IMEI verification systems integrate with of modern wireless communications networks architecture elements, including HSS, EIR, PCRF, and other EPC/5GC network core components. This enables automated verification of mobile equipment identifiers during device registration on the network and improves the effectiveness of network security mechanisms in modern telecommunications systems. [2]

LITERATURE REVIEW

(cc) BY

Active research is underway in the field of mobile device identification, aimed at evolving telecommunications network security, combating IMEI counterfeiting and optimizing mobile fleet management. This challenge is particularly pressing given the rapid growth in the number of smartphones and IoT devices, as well as the escalating threats posed by illegally modified equipment.

A significant part of scientific work is devoted to the analysis of the international identification system IMEI (International Mobile Equipment Identity). GSMA research examines the mechanisms for distributing TAC codes, centralized registration of mobile devices, and maintaining global equipment databases. It emphasizes the importance of international cooperation between telecom operators and national regulators for effective device control. [3,4]

Research shows that using CEIR can improve the efficiency of detecting illegal equipment through inter-operator synchronization of blacklist databases. The scientific literature also discusses the shortcomings of existing IMEI control systems, including synchronization delays between operator databases, the possibility of cloning identifiers, and insufficient security of information exchange channels between elements of the GSMA, CEIR, and EIR infrastructure.

Current research also focuses on the use of cryptographic methods for IMEI protection, machine learning algorithms, and data mining to detect abnormal device behavior and cloned identifiers. Another promising area is the use of blockchain technologies to create distributed IMEI data storage systems.

Despite significant research, issues of full integration and synchronization between the international GSMA, CEIR, and operator EIR systems remain understudied. This necessitates further research aimed at developing more efficient architectural solutions and intelligent mechanisms for protecting mobile identifiers in modern wireless networks. [5]

RESEARCH METHODOLOGY

The study utilized a systems approach to analyzing the architecture of the international mobile device identification system.

The main research objects are:

- GSMA IMEI Database;
- National CEIR systems;
- Operator EIR registries;
- International data exchange mechanisms.

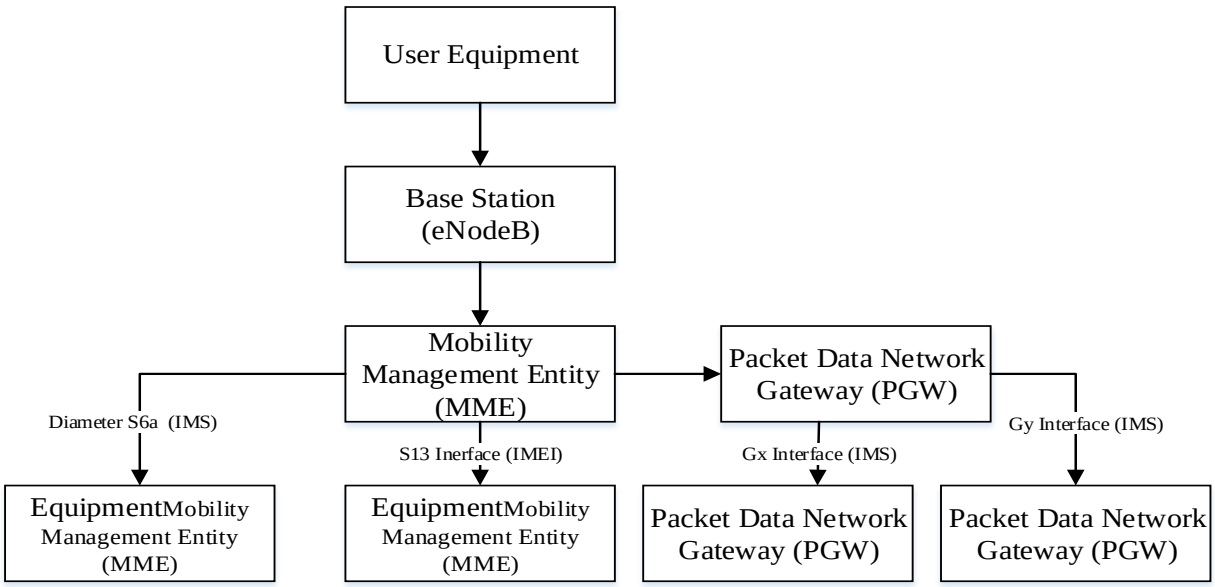


Figure 1 — Architecture of interaction between LTE network elements during subscriber authentication and mobile device IMEI verification [7,10,22].

The figure shows a structural diagram of the interactions between the main elements of the LTE/EPC network during user equipment registration, subscriber authentication, and mobile

(cc) BY *dtai.uz*

device authentication using the IMEI identifier. Initially, the user equipment (UE) establishes a connection via the radio interface with the eNodeB base station, which transmits signaling and user traffic to the LTE network core. The connection request is then sent to the MME (Mobility Management Entity), which centralizes mobility management, security, and session establishment procedures. [10]

During authentication, the MME transmits the IMSI to the HSS (Home Subscriber Server) via the Diameter S6a interface, where the SIM/USIM card is authenticated, the subscriber is identified, and connection security parameters are generated. At the same time, the MME initiates the equipment verification procedure by sending the mobile device's IMEI to the EIR (Equipment Identity Register) via the S13 interface. This step allows for the device's legitimacy to be determined, cloned or blocked IMEIs to be detected, and suspicious equipment to be prevented from connecting to the operator's network.

After successful authentication and device verification, the MME communicates with the Packet Gateway (PGW), which facilitates user traffic transmission and connectivity to external IP networks. To manage quality of service parameters and charging policies, the PGW communicates with the Policy and Charging Rules Function (PCRF) node via the Gx interface and with the Online Charging System (OCS) via the Gy interface. This communication enables centralized control of internet sessions, traffic consumption monitoring, QoS management, and online billing in real time. [11]

Thus, the architecture presented in the figure demonstrates a comprehensive mechanism for interaction between LTE network elements aimed at ensuring secure identification of subscribers, verification of the authenticity of mobile devices, preventing the use of cloned IMEIs and efficient management of mobile communication and data transfer services.

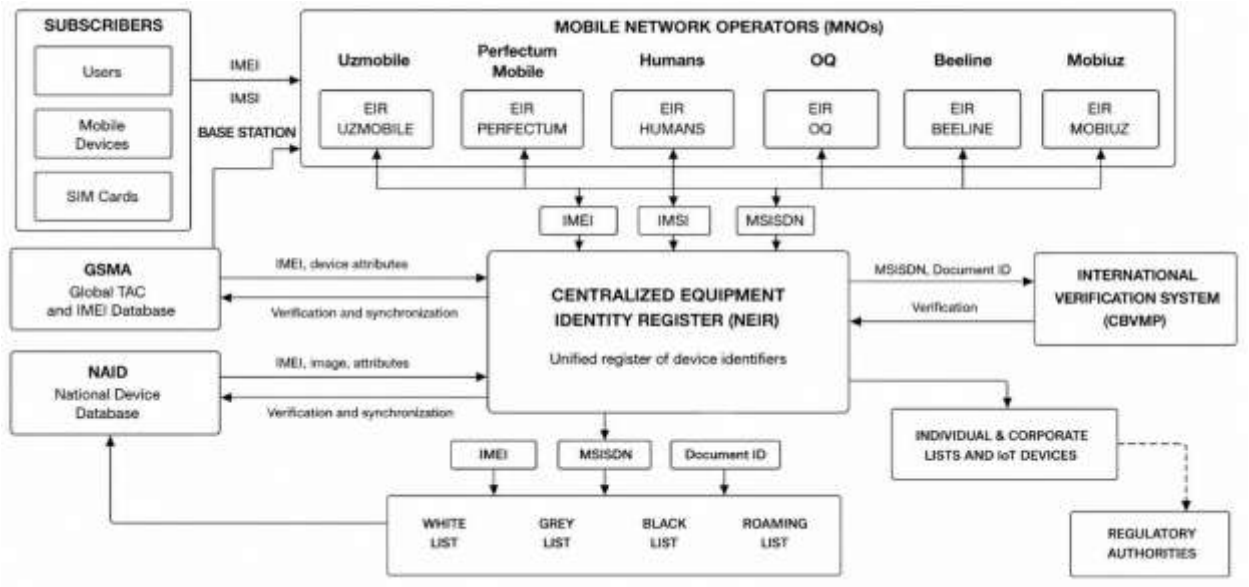


Figure 2. Architecture of a centralized IMEI control and verification system in mobile networks. [12,21]

The figure-2 shows the architecture of a centralized IMEI control system based on the interaction of mobile operators, international GSMA databases, national NAID registries, and the centralized NEIR device registry. The system provides mobile device identification, IMEI verification, blacklist/whitelist database synchronization, and integration with international verification systems and government regulatory bodies. The presented model enables multi-level control of mobile equipment, detection of cloned devices, and enhanced security of telecommunications infrastructure.The presented architecture demonstrates a centralized model for interaction between mobile operators, national regulators, and international databases in a mobile device control and identification system based on the IMEI (International Mobile Equipment

(cc) BY

Identity). The main goal of this infrastructure is to ensure reliable identification of mobile equipment, prevent the use of cloned and illegally modified devices, and centralize the management of mobile identifier databases.

Initially, the subscriber uses a mobile device (handset) with a SIM card to connect to the mobile operator's network via a Base Transceiver Station (BTS). During registration, the device transmits its International Mobile Equipment Identifier (IMEI) and International Mobile Subscriber Identifier (IMSI), which are used to further verify the authenticity of the device and subscriber profile.

The information is then sent to the infrastructure of mobile network operators (MNOs), where local Equipment Identity Registers (EIRs) operate. Each operator uses its own EIR to store and process information about registered devices, their status, and their security categories. At this level, an initial IMEI check is performed, the device's whitelisting, graylisting, or blacklisting is determined, and the equipment's registration on the network is analyzed.

The central element of the architecture is the National Equipment Identity Register (NEIR), a national system that provides centralized data integration between mobile operators, international organizations, and government regulators. NEIR aggregates information on IMEI, IMSI, MSISDN, and user identification documents (DOC ID), creating a unified space for monitoring mobile devices at the national level. [13]

The NEIR system interacts with the international GSMA database, which contains global data on TAC codes, mobile device attributes, and registered hardware identifiers. It also exchanges data with national NAID databases, enabling verification of device images, hardware parameters, and additional identification attributes. Using a centralized verification mechanism improves the reliability of IMEI verification and reduces the likelihood of cloned devices being used.

To confirm the identity of the device owner, the architecture includes interaction with the CBVMP system, which verifies the MSISDN and subscriber identification documents. This approach provides an additional level of security by matching device data, SIM card data, and the user's identity.

Based on the analysis results, NEIR categorizes devices into several security categories: White List, Gray List, Black List, and Roamers List. The White List contains authorized devices officially registered in the system. The Gray List includes suspicious devices requiring additional verification. The Black List is composed of stolen, cloned, or blocked devices whose use is restricted by the telecom operator. The Roamers List contains information about devices operating in international roaming mode.

The final layer of the architecture is the Regulatory Function, which ensures government oversight of mobile equipment, centralized management of blacklist databases, and coordination of interactions between national and international levels of telecommunications infrastructure. The integration of all these components allows for the creation of a multi-layered monitoring system aimed at enhancing the security of mobile networks and preventing the use of illegal equipment.

Table 1

Comparative analysis of architecture levels

System Component	Main Function	Processed Data	Infrastructure Layer
Handset/SIM	Generating a registration request	IMEI, IMSI	Subscriber level
BTS	Transmission of signaling traffic	Radio data	Radio access
MNO/EIR	Local equipment testing	IMEI	Operator level
NEIR	Centralized processing of identifiers	IMEI, IMSI, MSISDN	National level

(cc) BY

GSMA	Global TAC and IMEI registration	TAC, IMEI Attributes	International level
CBVMP	User identity verification	MSISDN, DOC ID	Government level
Regulatory Function	Control and regulation	Blacklist, Policies	Regulatory level

Table 1 presents a comparative analysis of the main architecture layers of a centralized mobile device control and identification system based on IMEI. The table presents the key components of the telecommunications infrastructure, their functional purpose, the types of data processed, and the corresponding interaction layers within the system. The analysis demonstrates the multi-layered organization of the architecture, including the subscriber, operator, national, international, and regulatory levels. The integration of BTS, MNO/EIR, NEIR, GSMA, and regulatory mechanisms ensures centralized IMEI processing, data synchronization, mobile device identification, and enhanced mobile network security. [14]

Table 2

Comparison of IMEI list categories

List Category	Characteristic Network	Access Status Device
White List	Legal and verified device	Full access
Gray List	Suspicious Device	Limited Control
Black List	Stolen or cloned device	Blocking
Roamers List	Device in international roaming	Temporary access

Table 2 shows the classification of IMEI list categories used in modern mobile device identification and control systems. These categories help determine the level of trust in equipment and the extent of a device's permitted access to the mobile network. The white list includes legitimate and verified devices with full access to network services, while the grey list contains suspicious equipment requiring additional monitoring and control. The black list consists of stolen, cloned, or illegally modified devices subject to blocking on the operator's network. A separate category is made up of international roaming devices, which are granted temporary access in accordance with inter-network policies. Using this classification improves the effectiveness of security systems and centralized IMEI control in telecommunications infrastructure. [15]

Table 3

Analysis of the advantages of a centralized architecture

Advantages	Description
Centralized identification	Formation of a unified database IMEI
Interoperator synchronization	Blacklist database exchange
Improving security	Detecting cloned devices
Integration with GSMA	International equipment control
Government regulation	Control of illegal import of devices
scaling	Possibility of integrating LTE/5G infrastructure

Table 3 summarizes the key advantages of a centralized IMEI control system architecture in modern mobile networks. The presented analysis demonstrates that a centralized approach ensures the formation of a unified database of mobile equipment identifiers, improves the efficiency of

(cc) BY

inter-operator synchronization, and facilitates the rapid exchange of blacklist databases between telecommunications infrastructure participants. Additionally, the architecture enhances security by detecting cloned devices and integrating with international GSMA systems. A significant advantage is also the ability to regulate government processes for monitoring illegal imports of mobile equipment and support scalable integration with LTE/5G network infrastructure.

The presented architecture of a centralized IMEI control system demonstrates a comprehensive approach to ensuring the security of mobile telecommunications networks. The integration of operator EIR databases, the national NEIR registry, the international GSMA infrastructure, and regulatory mechanisms significantly improves the detection of cloned, stolen, and illegally modified devices. The use of centralized mechanisms for IMEI verification, MSISDN matching, and identification document matching enhances subscriber identification reliability and minimizes the risks of unauthorized access to mobile networks.

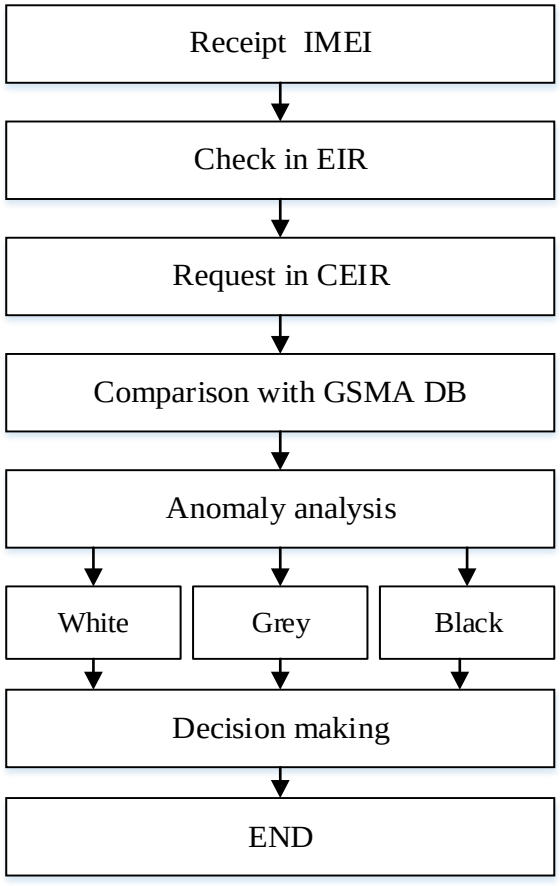


Figure 3. Algorithm for intelligent detection of cloned IMEI in telecommunication networks.[17]

The figure shows a flowchart of the IMEI cloning detection algorithm in a centralized mobile device monitoring system. The proposed algorithm is designed to ensure reliable identification of mobile equipment, detect abnormal network activity, and prevent the use of cloned or illegally modified devices in the mobile communications infrastructure. The algorithm's architecture is based on sequential processing of IMEI identifiers using operator, national, and international telecommunications network databases.[1,7,17]

The initial stage involves obtaining the mobile device's IMEI during the equipment registration process on the telecom operator's network. Once the identifier is received, it is initially checked against the local Equipment Identity Register (EIR), which contains information about authorized, suspicious, and blocked devices. This stage allows for basic equipment filtering and the presence of the IMEI in the operator's local blacklist and whitelist databases. The next step in the algorithm is to generate a request to the CEIR (Central Equipment Identity Register), a centralized system designed for inter-operator information exchange and centralized storage of mobile equipment identifier data. Using the CEIR enables IMEI matching across different mobile networks and improves the efficiency of identifying cloned devices at the national and international levels.

After data processing, CEIR compares the device identifier with the global GSMA DB, which contains information on TAC codes, equipment manufacturers, and mobile device attributes. This stage includes checking the TAC code for the device model, analyzing the correctness of the IMEI structure, and matching the equipment parameters with the global registration data of the GSMA international system.

The key element of the algorithm is the anomaly analysis stage, which is aimed at identifying signs of IMEI cloning. This stage utilizes several analysis criteria, including comparing the device's geographic registration coordinates, identifying simultaneous activity of the same IMEI in different networks and regions, verifying the TAC model of the equipment, and analyzing the device's network activity in various mobile infrastructures. This approach allows for

(cc) BY

the detection of cases of impossible device geolocation and the recording of cases of simultaneous registration of the same IMEI in different network locations within a minimal period of time.

Based on the analysis results, the system classifies the device into White, Gray, and Black categories. White corresponds to legitimate and verified devices, Gray includes suspicious equipment requiring additional monitoring, and Black is used for devices identified as cloned, stolen, or illegally modified. After classification, the system decides whether to allow network access, limit the device's functionality, or completely block its registration in the mobile infrastructure.

The presented flowchart demonstrates a comprehensive IMEI intelligence algorithm that enables multi-level verification of mobile equipment, integration of local and international databases, and improved security performance of modern wireless communications networks. The use of centralized anomaly analysis mechanisms significantly enhances the protection of mobile infrastructure against IMEI cloning and other forms of fraudulent network activity.

RESULTS

The study found that the centralized architecture of the GSMA–CEIR–EIR interaction enables the development of an effective multi-level system for identifying and monitoring mobile devices in modern telecommunications networks. An analysis of existing IMEI processing mechanisms showed that the integration of international, national, and operator infrastructure layers significantly improves the reliability of mobile equipment identification, reduces the likelihood of cloned devices being used, and strengthens mobile network security mechanisms against unauthorized access.

The analysis confirmed that the use of a centralized interaction model ensures international IMEI synchronization between the GSMA global databases, national CEIR registries, and local operator EIR systems. This integration enables the rapid exchange of mobile equipment identifier data between networks, ensuring near-real-time updates of blacklist, whitelist, and greylist databases. This significantly improves the effectiveness of detecting stolen, cloned, and illegally modified devices across various mobile networks and regions.

Additionally, it has been established that the centralized architecture facilitates the accelerated detection of abnormal network activity associated with the use of duplicate IMEIs. By integrating operator databases and international verification mechanisms, it is possible to identify instances of the same IMEI being registered simultaneously in different geographic locations, analyze device activity across multiple networks simultaneously, and verify that TAC codes comply with mobile equipment specifications. The use of such intelligent analysis mechanisms significantly improves the security of telecommunications infrastructure and reduces the risk of network fraud.

The study's results also showed that unifying mobile device identification procedures helps ensure consistent equipment verification processes across various telecom operators and government regulators. The development of a unified IMEI processing system facilitates the standardization of device registration mechanisms, simplifies international data exchange procedures, and improves the compatibility of telecommunications platforms in modern wireless communications networks.

The comparison of system layer functions presented in this paper demonstrates the distribution of key tasks among the main elements of the IMEI control architecture. The manufacturer layer generates IMEIs and TAC codes, which form the basic identifiers of mobile equipment. The international organization GSMA performs the functions of global registration and centralized storage of the IMEI Database, ensuring the international coordination of device identifiers. The national CEIR layer is responsible for centralized device control, synchronization of White/Grey/Black categories, and the exchange of blacklist databases between operators. Local EIRs implement IMEI verification and equipment verification procedures directly within the operator network, while the operator layer ensures device authentication and provision of access to mobile network services.

(cc) BY

Table 4

Comparison of system level functions

Level	Main Function	Data Type
Manufacturer	Generation IMEI	TAC, SNR
GSMA	Global registration	IMEI DB
CEIR	National Control	White/Grey/Black
EIR	Checking the device	IMEI Verification
Operator	Network access	Authentication

The obtained results confirm that the use of the centralized GSMA-CEIR-EIR architecture ensures a high level of scalability, security, and efficiency for mobile device identification systems. The integration of international and national IMEI control mechanisms significantly improves the reliability of modern telecommunications networks and forms the foundation for the further development of intelligent equipment monitoring systems in contemporary wireless communication infrastructures and next-generation network environments.[13,18,19]

DISCUSSION OF RESULTS

The results obtained demonstrate that the integration of international and national IMEI control systems significantly improves the efficiency of mobile device identification and the security of telecommunications infrastructure. Interoperability between the GSMA, CEIR, EIR systems, and operator databases enables centralized information exchange, accelerates the detection of illegally modified devices, and increases the reliability of equipment verification.

The analysis confirmed that centralized IMEI synchronization enables the efficient creation of blacklist and whitelist databases, increases the speed of blocking stolen devices, and facilitates the unification of identification procedures in of modern wireless communications networks. However, it was found that existing architectures have a number of limitations related to their dependence on centralized servers, data update delays, and the risk of information inconsistency between telecom operators.

An additional problem remains the possibility of IMEI cloning and bypassing blacklisting mechanisms by modifying device software. Analysis has shown that most modern systems focus primarily on static verification of identifiers and have limited capabilities for intelligent network activity analysis.

Promising development areas include the implementation of artificial intelligence and machine learning algorithms for automatically detecting abnormal device behavior and locating cloned IMEIs. Another promising solution is the use of blockchain technologies to create distributed IMEI data storage systems that ensure transparent synchronization and protect information from unauthorized modification.

The obtained results confirm the need for further improvement of the IMEI control architecture, the development of intelligent analysis mechanisms, and the integration of modern cryptographic methods for protecting mobile identifiers in contemporary wireless communication networks.

CONCLUSION

This paper analyzes the architecture of the international mobile device identification system based on IMEI codes and examines the interaction mechanisms between the GSMA, CEIR, EIR, and mobile operator networks. It is established that the multi-level IMEI control architecture ensures centralized identification of mobile equipment, support for global blacklisting and whitelisting systems, and efficient inter-operator data exchange.

The study's results demonstrated that the integration of international and national IMEI verification systems contributes to increased security of telecommunications infrastructure, reduced risks of using illegally modified devices, and increased effectiveness in combating IMEI

(cc) BY

cloning. The importance of integrating identification systems with modern mobile network infrastructure elements for automated verification and control of mobile equipment was further confirmed.

At the same time, limitations of existing systems have been identified, including dependence on centralized databases, synchronization delays, and insufficient intelligent analysis of abnormal device activity. This indicates the need for further improvement of IMEI monitoring mechanisms.

Promising areas of development include the implementation of artificial intelligence and machine learning algorithms for anomaly detection, the use of blockchain technologies for distributed storage of IMEI data, and the development of cryptographic methods for protecting mobile device identifiers.

Thus, improving the IMEI control architecture is an important direction in the development of modern telecommunications systems and plays a key role in ensuring the security, reliability, and integrity of contemporary mobile communication infrastructures and next-generation wireless networks.

Acknowledgment

The authors would like to thank the telecommunications industry experts and scientific consultants for supporting the research in the field of international mobile device identification systems and mobile network security.

REFERENCE

1. Jog Y. et al. Analysing Central Equipment Identity Register (CEIR) Model for Mobile Handset Tracking in India //Management. – 2016. – Т. 5. – №. 4..
2. Loureiro A. J. F., Gallegos D., Caldwell G. Substandard cell phones: Impact on network quality and a new method to identify an unlicensed IMEI in the network //IEEE Communications Magazine. – 2014. – Т. 52. – №. 3. – С. 90-96.
3. 3GPP TS 23.003 version 15.4.0 Release 15. ETSI TS 123 003 V15.4.0 (2018-07)
4. Д.А.Давронбеков, К.П.Абдурахманов, М.О.Султонова, Ж.Д.Исроилов, А.С.Кириакиди Идентификация мобильных устройств по IMEI: монография. – Т: Ташкент, ТАТУ, 2019. – 108 с.
5. Мазниченко Н. И. Сравнительный анализ сценариев двухфакторной идентификации //Актуальные научные исследования в современном мире. – 2021. – №. 2-3. – С. 58-65.
6. Д.Давронбеков, А.Кириакиди, Д.Елькин, Ж.Исроилов, М.Нурматова. Состояние и анализ рынка мобильных устройств для создания единой базы идентификации мобильных устройств по IMEI // International Scientific Journal «Science and World». – 2018. – №11(63). Vol.I. – P.41-42, (14) ResearchBib.
7. Давронбеков Д.А., Султонова М.О., Исроилов Ж.Д. Мобил терминалларни ўғрилашдан ҳимоя қилиш учун IMEI тизими//Muhammad al-Xorazmiy avlodlari.-2018.- №3 (5). - Б.94-97
8. Davronbekov D.A., Khakimom Z.T., Isroilov J.D. Implementation of the Algorithm for Checking and Registering Mobile Devices in the Information System Using the IMEI Code // International Journal of Advanced Research in Science, Engineering and Technology. - Vol. 7, Issue 10, October 2020. – P.15054-15059
9. Jamshid Isroilov, Dilmurod Davronbekov, Zafar Khakimov, Murod Abdullaev and Najmiddin Turaxodjaev Assessment of the reliability of the information system for identifying mobile devices by IMEI code, E3S Web of Conf., 402 (2023)
10. Gepko I. General requirements and security architecture for mobile phone anti-cloning measures //IEEE EUROCON 2015-International Conference on Computer as a Tool (EUROCON). – IEEE, 2015. – С. 1-6.
11. Choudhury H. HashXor: A lightweight scheme for identity privacy of IoT devices in 5G mobile network //Computer Networks. – 2021. – Т. 186. – С. 107753.
12. Haque A. et al. Anonymous device authorization for cellular networks //Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks. – 2021. – С. 25-36.

(cc) BY

13. ITU-T Recommendation E.212. *International Identification Plan for Mobile Terminals and Users*. ITU, 2023.
14. Давронбеков Д.А., Исроилов Ж.Д., Роль IMEI в идентификации мобильных устройств и обеспечении безопасности сетей подвижной связи.
15. Saputra, Farhan, and M. Ridho Mahaputra. "Relationship of purchase interest, price and purchase decisions to IMEI policy (Literature review study)." Journal of Law, Politic and Humanities 2.2 (2022): 66-75.
16. Давронбеков, Дилмурод, and Жамшид Исроилов. "Эволюция стандартов IMEI в контексте перехода к многочастотным беспроводным коммуникациям." Raqamli iqtisodiyot (Цифровая экономика) 12. T (2025): 208-220.
17. Jakhar N. A new design approach for mobile devices security against IMEI tampering and cloning //Int. J. Innov. Res. Comput. Commun. Eng. – 2017. – Т. 5.
18. Davronbekov Dilmurod, and Isroilov Jamshid. "ENSURING SECURITY IN IOT SYSTEMS: APPROACHES TO IDENTIFICATION." Raqamli iqtisodiyot (Цифровая экономика) 13. T (2025): 58-68.
19. Никитин Д. А. Проблемные вопросы внедрения национального центрального реестра идентификации мобильного оборудования //Системы управления, связи и безопасности. – 2019. – №. 2. – С. 28-53.
20. Кашкаров А. Искусственный интеллект и современные методы отслеживания с помощью электронных устройств. СОВРЕМЕННАЯ ЭЛЕКТРОНИКА • № 1 / 2026
21. Omar A. S., Basir O. Decentralized identifiers and verifiable credentials for smartphone anticounterfeiting and decentralized IMEI database //Canadian Journal of Electrical and Computer Engineering. – 2020. – Т. 43. – №. 3. – С. 174-180.
22. Jeong Y. S., Park J. S., Park J. H. An efficient authentication system of smart device using multi factors in mobile cloud service architecture //International Journal of Communication Systems. – 2015. – Т. 28. – №. 4. – С. 659-674.

(cc) BY