Computer Science and Information Systems 21(2):507–524 https://doi.org/10.2298/CSIS221115070K

# A Study of Identity Authentication Using Blockchain Technology in a 5G Multi-Type Network Environment

Jui-Hung Kao[1,*], Yu-Yu Yen[2,3], Wei-Chen Wu[4], Horng-Twu Liaw[5], Shiou-Wei Fan [6], and Yi-Chen Kao[7]

[1] Department of Information Management, Shih Hsin University, Taipei, Taiwan
kjhtw@mail.shu.edu.tw
[2] Center of General Education, Shih Hsin University, Taipei, Taiwan
melyen@mail.shu.edu.tw
[3] Department of Biomedical Engineering, National Yang Ming Chiao Tung University, Taipei, Taiwan
sheepkelly19.be11@nycu.edu.tw
[4] Department and Graduate Institute of Finance, National Taipei University of Business, Taipei, Taiwan
weichen@ntub.edu.tw
[5] Department of Information Management, Shih Hsin University, Taipei, Taiwan
htliaw@mail.shu.edu.tw
[6] Department of Information Management, Shih Hsin University, Taipei, Taiwan
fan@mail.shu.edu.tw
[7] Department of Information Management, Shih Hsin University, Taipei, Taiwan
i110925102@mail.shu.edu.tw

**Abstract.** The 5G technology, known for its large bandwidth, high speed, low latency, and multi-connection capabilities, significantly accelerates digital transformation in enterprises, especially in addressing factory automation challenges. It facilitates efficient machine-to-machine (M2M) and device-to-device (D2D) connectivity, ensuring rapid data transfer and seamless process convergence under 5G standards. Although 5G offers substantial communication and low latency benefits, its limited indoor coverage requires the deployment of decentralized antennas or small base stations. In contrast, Wi-Fi 6 seamlessly complements 5G, providing superior indoor mobile connectivity. This integration is crucial for businesses looking to accelerate digital transformation. To optimize 5G, the deployment of devices such as bypass switches, SDN switches, and MEC in the 5G Local Breakout network enables user access control and fast authentication. Real-world validation confirms the effectiveness of these measures, which are expected to lead to the future of 5G mobile networks.

**Keywords:** Fifth-Generation Mobile Communication, Blockchain, Identity Authentication.

* Corresponding Author

## 1. Introduction

Literat In recent years, the era of fifth generation mobile networks (5G) has arrived, and countries around the world are competing to invest in 5G development resources. The International Telecommunication Union (ITU) has compiled trends released by a variety of organizations and proposed the 5G system specification (International Mobile Telecommunications 2020, IMT 2020), which emphasizes that future communications must meet eight indicators of technical requirements (8KPIs) and three application requirements. The overall system capacity of Extreme Mobile Broadband (eMBB), Massive Machine Type Communication (mMTC), and Ultra Reliable Low Latency Communication (uRLLC) is 1000 times that of 4G (4th Generation Mobile Networks) to meet the bandwidth requirements of 5G communication [1].

As a new technology, 5G has some limitations in terms of physical constraints. Wireless 5G signals will be transmitted at a significantly smaller distance than 4G; that is, to serve devices within the same range, 5G will require more base stations than 4G, which is undoubtedly a barrier to 5G adoption, whether due to the impact of deployment time or increased cost. To overcome these limitations, a possible solution is to use the free unlicensed spectrum available in Wi-Fi (Wireless Fidelity) technology. As such, a complementary solution is proposed to have 5G and Wi-Fi 6 coexist, so that the two technologies can complement each other to provide better service quality and higher speed, lower latency, and higher capacity for end users. However, in this multi-type 5G network environment, how to enable IoT devices to have a unique and identifiable identity, with undeniability and privacy, and the ability to authenticate each other and switch connections in different network environments without interruption has become an important issue [2, 3].

The core of the 5G system is secure identity management, where only users who have passed identification and authentication can access network services. 5G inherits the powerful cryptographic components (e.g., key generation functions and interdevice and internetwork authentication) and security features of the original 4G system. It should be mentioned that a new security function in the 5G system is the identity authentication framework, which provides mobile service operators with the flexibility to choose the identity authentication credentials, logo format and authentication method for users and IoT devices, unlike previous mobile networks that required a physical SIM (Subscriber Identity Module) card as the credential. The different authentication methods available are called the 5G Authentication and Key Agreement (5G-AKA) and the Extensible Authentication Protocol (EAP) [4, 5].

The purpose of this study is to investigate the interoperability between the fifth-generation mobile communication network and the new wireless LAN technology of Wi-Fi 6. Both Wi-Fi 6 and 5G have improved transmission efficiency, bandwidth, and quality, which is of great help for manufacturing automation, telemedicine, and other critical IoT devices in many industries. Regarding the issues of how to retain original characteristics and also care for information security in these fields, this study focuses on how to use blockchain technology to identify IoT devices when switching between Wi-Fi 6 and 5G signals for research and discussion.

## 2. Materials and Methods

### 2.1. Introduction to the 5G network environment

There are two environmental modes of 5G network architectures [6]: NSA and SA. The first is the NSA architecture, which is the 5G network formed by LTE (long-term evolution) 4G technology and the 5G radio access architecture; the second is the SA architecture. Before discussing the SA architecture, we should first introduce 5G NR. NR is the name of 5G New Radio, which is a global standard for 5G with OFDM (Orthogonal Frequency Division Multiplexing) and this standard was approved as a 5G connectivity standard by the international standards organization 3GPP (The Third Generation Partnership Project), which is composed of enterprises such as Huawei and Samsung, etc. Therefore, the 5G SA is composed of new radio access technology (RAT), which is different from the 5G process made up of the NSA.

The difference between 5G and 4G technologies (as shown in Fig. 1.) is that 5G NR uses a large number of Parallel Narrowband Subcarriers instead of Single Broadband Carriers to transmit data, so NR can cover low frequencies (450 MHz to 6000 MHz), lower frequencies than 6 GHz and higher frequencies (24250 MHz to 52600 MHz), higher frequencies than 24 GHz and millimeter wave range; that is, it can fully cover the spectrum from 6 GHz to 100 GHz in the millimeter wave (mmWave) band to meet the standard required for 5G. The emergence of NR technology is very helpful for the three main characteristics of 5G, eMBB, mMTC and URLLC, allowing for a new specification and standard for 5G [**7**].

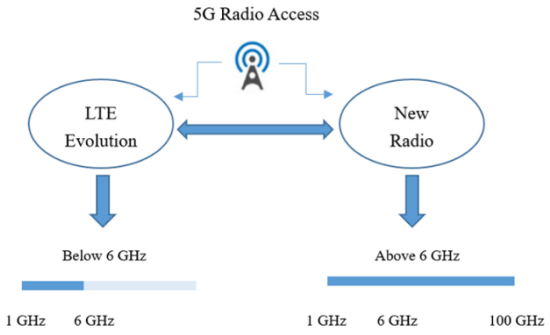


**Fig. 1.** NSA and SA Environments

### 2.2. Introduction to the 5G authentication mechanism

The 5G authentication mechanism is a continuation of the 4G authentication mechanism with improvements including the 3 identity authentication mechanisms of EAP-AKA

(Extensible Authentication Protocol-Authentication and Key Agreement), 5G-AKA and EAP-TLS (Extensible Authentication Protocol-Transport Layer Security), of which EAP-TLS [8] is defined in 5G for limited use conditions (e.g., IOT environments).

The Service Based Architecture (SBA) is proposed for 5G in the definition of the core network (as shown in Fig. 2.) [9]. The physical architecture and service request definition are very different from those of the 4G core network, so we will not discuss the 4G architecture here but focus on the 5G architecture, which has the following five major parts:

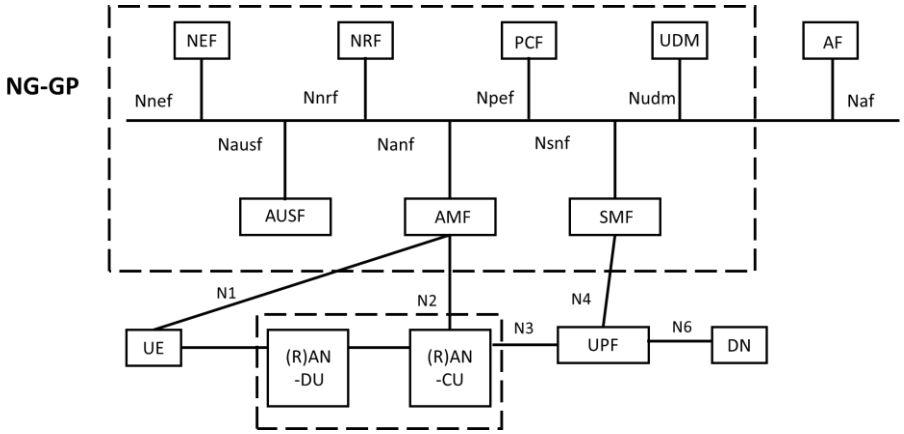


**Fig. 2.** SBA Services for the 5G Core Network Architecture

(1) Security Anchor Function (SEAF)

UE and its local network need to communicate through it during the identity authentication process. It can reject UE identity authentication, but relies on the local network of UE to accept identity authentication.

(2) Authentication server function (AUSF)

It has the function to decide whether or not to allow the connection for UE authentication, and it relies on the back-end service to calculate authentication data and keys if 5G-AKA or EAP-AKA is used.

(3) Unified Data Management (UDM)

It is an entity that carries functions related to data management, such as the Authentication Credential Repository and Processing Function (ARPF), which selects identity authentication methods based on subscriber identity and configured policies and calculates identity authentication data and keys as needed.

(4) Subscription Identifier Deconcealing Function (SIDF)

The subscription concealed identifier (SUCI) is decrypted to obtain its long-term identity; that is, the subscription permanent identifier (SUPI), such as the International Mobile Subscriber Identity (IMSI). In 5G, transmission is always done encrypted over the wireless port. More specifically, public-key-based encryption is used to protect the SUPI (Subscription Permanent Identifier). Therefore, only SIDF (Subscriber Identity Deconcealing Function, SIDF) has access to the private key associated with the public key assigned to UE (User Equipment) to encrypt its SUPI.

## 2.3. 5G-AKA

AUSF (Authentication Server Function) provides the identity authentication service via Nausf_UE authentication, while UDM provides the identity authentication service via Nudm_UE authentication [10]. A brief description of the 5G authentication procedure is shown in Fig. 3. [11]:

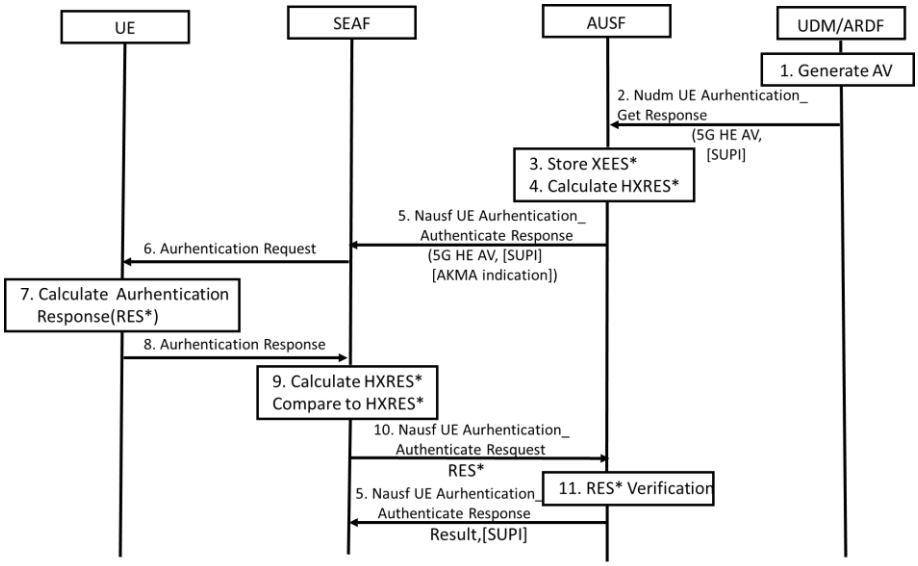


**Fig. 3.** 5G authentication procedure

## 2.4. Wi-Fi 6 identity authentication

Wireless security is an important issue for WLAN systems. Since wireless networks use the so-called open medium, which uses public electromagnetic waves as carriers for transmitting data signals, and there is no physical line connecting the two communicating parties, the risk of data theft is very high if proper encryption or other protection measures are not taken during the transmission process. Therefore, it is particularly important to ensure data security in the wireless network environment of WLAN [12, 13].

(1) Basic Concepts

802.11i is the latest wireless network security standard. IEEE has proposed additional amendments to compensate for the insecure encryption functions of 802.11 with the concept of RSN (Robust Security Network) added to the 802.11i standard to enhance the encryption and authentication functions of wireless network data transmission, and to address the shortcomings of WEP (Wired Equivalent Privacy) encryption mechanism with many corrections [14]. The proposed solution for identity authentication in the

802.11i standard is based primarily on the 802.1X framework and the extensible authentication protocol (EAP), while the encryption algorithm is based on the encryption algorithm of the Advanced Encryption Standard (AES) [15, 13].

(2) Introduction to the Link Authentication Method

The so-called link authentication refers to the 802.11 identity authentication, which is a low-level authentication method. It occurs when an STA is associated with an AP over 802.11, which precedes access authentication. Any STA must be authenticated using the 802.11 identity authentication method before trying to connect to the network, and 802.11 identity authentication can be thought of as the starting point of the handshake process when an STA (station) connects to the network, which is the first step in the so-called network connection process [16]. The IEEE 802.11 standard defines two types of link layer authentication: Open System Authentication and Shared Key Authentication, which are briefly described below:

1) Open System Authentication

This means that any user is allowed to access the wireless network in the sense that no data protection is actually provided, that is, no authentication. In other words, if the authentication type is set to open-system authentication, all STA requests for authentication will pass 802.11 authentication. The open-system authentication consists of two steps: The first step is to request authentication from the STA, and its data contain the STA's ID (Identity) (Media Access Control Address) after the STA sends the authentication request. The second step is for the AP (Access Point) to send back the authentication results, and the content of the authentication reply issued by the AP contains whether or not the authentication result is a success or failure. If the authentication result is "success", then STA and AP have passed the two-way authentication.

2) Shared Key Identity Authentication

The so-called shared key authentication refers to another authentication mechanism in addition to the open system authentication mentioned above. Shared-key authentication requires both STA and AP to be configured with the same key, and the authentication process is as follows. Step 1, STA first sends an authentication request to AP; Step 2, after receiving the authentication request, AP randomly generates a Challenge packet (i.e., a string) and then transmits the string to STA; Step 3, STA copies the string received from AP into a new message and then encrypts it with the key and sends it back to AP; Step 4, after receiving the message from STA, AP will decrypt the message with the key and then compare the decrypted string with the one given to STA at the beginning; if they are the same in accordance with the comparison, it means STA has the same shared key at the wireless device, that is, it has passed the shared key authentication requirement; otherwise, the shared key authentication result is "failure."

### 2.5. Integration of Two Access Technologies

IOTA (Integration of Two Access Technologies) was founded in 2015 by David Sønstebø and others with the goal of enabling the communication of various devices on the IoT, which is faster, used by more people, and can withstand a larger number of transactions than traditional blockchain, and is currently the most popular decentralized ledger technology in Europe. In recent years, more and more cities are moving smart and

providing many citizen-friendly smart city services, among which the number of services that users have to pay for is increasing. IOTA proposes a block-chain technology solution for Internet of Things (IoT) systems that aims to over-come the limitations or problems of existing IoT systems mentioned above. As de-scribed above, the rarely mentioned characteristics of blockchain technology, such as decentralization, invariance, availability, tracking and tracing, and integrity, smart contracts make it a disruptive technology for IoT applications [17, 18].

IOTA is a kind of revolutionary public distributed ledger of the new generation with a new invention called "Tangle" at its core. Tangle is a new data architecture based on the Directed Acyclic Graph (DAG) [19]. Therefore, it has no blocks, no chains, and no miners. Due to this radical new architecture, IOTA works completely differently from other blockchains [20].

The main difference worth mentioning (other than DAG versus blockchain) is how IOTA reaches consensus and how it conducts transactions. As mentioned earlier, there is no miner role exists. This means that every participant in the network who wants to conduct transactions must actively participate in the network consensus by approving 2 past transactions. This proof of the validity of two previous transactions ensures that the entire network reaches consensus on the current status of approved transactions and enables a variety of unique functions that can only be seen in IOTA [21].

IOTA is the missing puzzle for the machine economy to fully emerge and play out its intended potential. We envision IOTA as the public, permission-exempt backbone of IoT, enabling true interoperability between all devices.

Due to its architecture, IOTA has a unique series of functions [22]:

Scalability

IOTA can achieve high transaction throughput thanks to parallel validation of transactions, with no limit to the number of transactions that can be validated at a given interval.

No transaction fees

With the launch of smart contracts in November 2021, IOTA does not charge transaction fees, which is a great advantage and is a good choice for data transaction validation.

Decentralization

IOTA has no miner role, and every participant who performs transactions on the network is actively involved in the consensus. Therefore, IOTA is more decentralized than any blockchain.

Quantum Immunity

IOTA uses a new technique, called Curl's ternary hash function, which can resist quantum attacks and avoid brute-force cracking attacks.

## 3. Results

The number of 5G users is growing and the trend is to have multiple heterogeneous wireless network interfaces on mobile devices. Many smart mobile phones are al-ready equipped with wireless LAN interfaces. However, these mobile devices often lack an effective mobility management mechanism to take full advantage of these heterogeneous

network interfaces at the same time. To solve this problem, we use blockchain technology to design a set of intermediary mechanisms that can integrate and roam efficiently among heterogeneous networks, making the identity authentication of end devices more convenient and secure.

### 3.1. IOTA decentralized ledger technology

IOTA's underlying ledger architecture, Tangle, is not designed in terms of blocks and chains, but rather in terms of a decentralized architecture. When the data are placed on the IOTA's decentralized ledger [23], they are copied and distributed to numerous network nodes to achieve the characteristic that the data cannot be tampered with. In addition, Tangle does not have a mining mechanism [24], but rather validates transactions through IOTA users and, therefore, does not require transaction fees. The nature of Tangle architecture is that the larger the transaction size, the higher the availability, so it is more suitable for the quantitatively large IoT industry than traditional blockchain technology [25].

Tangle

Tangle, as mentioned by IOTA, has a data structure of a directed acyclic graph (DAG) where each message is attached to 2 to 8 previous messages, and anyone can attach messages at different locations in front of Tangle, and the protocol can process these different messages in parallel. There is no cost to send a message on Tangle, because the network has no miners or pledgers. In Tangle, PoW (Proof-of-Work) is not used to protect the network; instead, PoW is only used to block spam, and all IOTA nodes validate messages and use different functions to reach consensus when confirming messages [26].

Directed Acyclic Graph

In general, IOTA operates in such a way that there is no domain-wide blockchain, but a directed acyclic graph (DAG), which is the Tangle described in the previous section. All transactions issued through the nodes constitute the Tangle, the set of ledgers in which all transactions are stored. When a new transaction is created, it must validate two previously completed transactions, and these validation relationships are represented by the directed nodes. If there is no direct-connected directed node from transaction A to transaction H, but there is a directed node path of length at least greater than two, we say that transaction A indirectly validates transactions B and D. Furthermore, there is a Genesis transaction that is validated directly or indirectly by all transactions (as shown in Fig. 4.). Assuming that H is the Genesis Transaction, the following description is given in the IOTA technology: At the beginning there is an address that has all the tokens. Then, through the behavior, the Genesis Transaction will transfer the IOTA coins to other founder’s addresses, stating that all tokens are generated by the Genesis Transaction, which means that no new token will be generated, and this is also the reason why the DAG will not loop. In fact, simply put, it is the concept of receiving IOTA coins without the need for mining behavior [27].

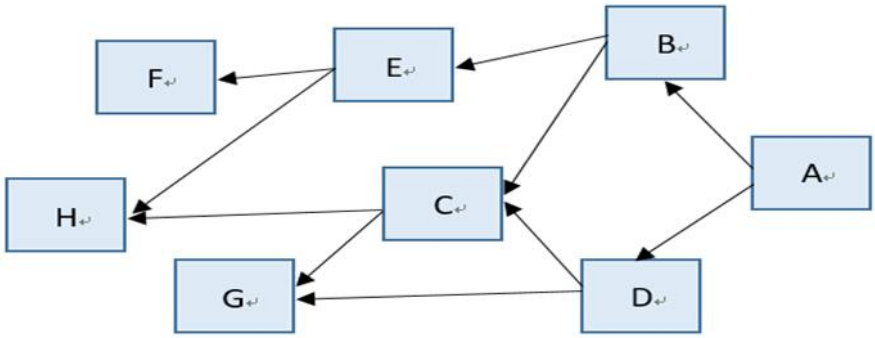


**Fig. 4.** 5G authentication procedure

### 3.2. The Cross-network Authentication Information Security Framework for 5G and Wi-Fi 6

With the proliferation of fifth-generation mobile communication technology (5G) and Wi-Fi 6, there has been an increasing demand for faster communication speeds, greater capacity, and enhanced data security. Against this backdrop, ensuring efficient and secure data exchange between these two major communication technologies has become a paramount concern. This article elucidates how IOTA's Keccak-384 and the sponge function facilitate secure data exchanges in cross-network authentication communication between 5G and Wi-Fi 6.

First, let us explore the background of IOTA and the rationale behind its adoption of Keccak-384 [28]. As mentioned previously, IOTA initially employed the SHA-3-384 algorithm, but due to potential security vulnerabilities, shifted its preference to Keccak-384[1]. The foundation of this algorithm is the sponge function. Thus, by using the Keccak-384 sponge function, IOTA ensures the security of its blockchain transactions, making it resistant to various collision attacks [29].

Introduced by Guido Bertoni's team in 2007, the sponge function is based on the properties of sponges, with the ability to absorb and squeeze out large amounts of data. This trait allows the sponge function to accept input of any length, undergo specific algorithmic processing, and produce output of the desired length [30].

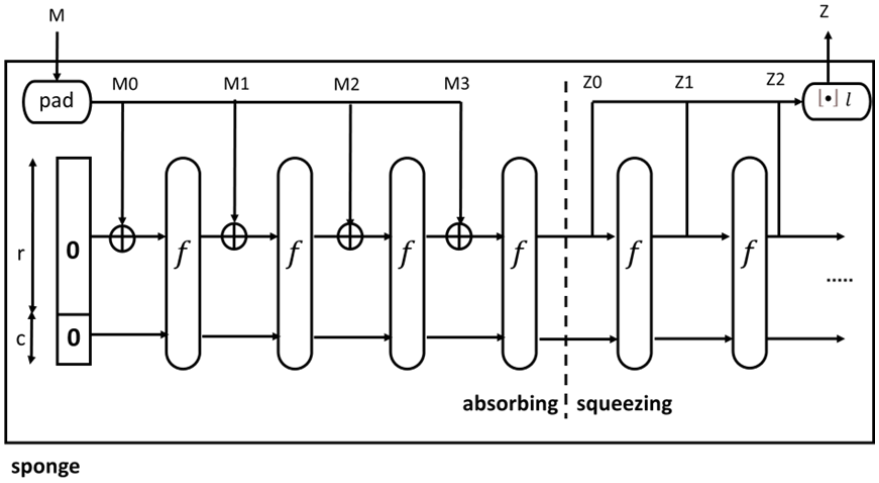


**Fig. 5.** Schematic diagram of the operation of the sponge function

As described by the IOTA Foundation, this function is made up of three main components:

Memory State (S): This particular state encompasses 'b' bits and is segmented into two sections: R (comprising 'r' bits) and C (amounting to b-r bits or 'c' bits). Here, 'r' denotes the Bitrate, while 'c' signifies the Capacity.

Transformation function (f): This function transforms S to a fixed size. IOTA has chosen Keccak-384 as its transformation function, which is a variant of the sponge function from the Keccak family.

Padding function (P): This function ensures that the input M is a multiple of the bitrate 'r'. It continually adds data until this condition is met, after which the padded data are segmented into multiple chunks of size 'r'.

In the high-speed communication environment of 5G and Wi-Fi 6, ensuring data integrity and security becomes paramount. Utilizing the sponge function allows efficient encryption of communication data. During the absorption phase, the original data are XORed with data that is a multiple of the bitrate 'r', and through the function 'f', are transformed multiple times, resulting in a complex data set. In the squeezing phase, the desired length data is extracted from the transformed data.

However, depending solely on the sponge function fails to meet all the security requirements of cross-network authentication communication between 5G and Wi-Fi 6. An effective mechanism to ensure the authenticity and integrity of communication between the two parties is essential. This is where IOTA's Keccak-384 comes into play. Through Keccak-384, IOTA can generate a unique address and signature, ensuring the authenticity and integrity of the data during transmission.

**5G local breakout private network**

Local breakout private networks focus on data offload processing and are typically deployed between the base station and the core network. Mobile communication operators can choose to deploy MECs at the appropriate location based on requirements such as business type, processing capacity, network planning, etc. to achieve transparent deployment of terminals and networks. According to ETSI White Paper No. 28 [10], if an MEC server is deployed in the core network, MEC can be integrated with S/P-GW, and when MEC is deployed near the RAN side of the wireless network, the MEC server can be a standalone network element, or MEC functions can be integrated into the hub node or eNodeB. If the MEC server is a standalone element, it can be a device of a different vendor from that of HubNode and eNodeB.

The MEC mobile edge computing network provides application developers and content service providers with cloud computing capabilities and the IT service environment for the mobile edge network to achieve ultralow latency, large bandwidth, and real-time access to network information with the following key technologies [11]:

(1) Temporary storage of content on the wireless side: the MEC server can obtain the hotspot content in the service, including video, pictures, documents, etc., through interconnection with the service system and carry out local temporary storage. During the service process, the MEC server performs real-time deep packet parsing of the data on the base station and can directly push the content in the temporary storage to the terminal if the service content applied by the terminal is already in the local temporary storage.
(2) Local diversion: users can access the local network directly through the MEC platform, and the local service data stream does not need to go through the core network, but is directly diverted to the local network by the MEC platform, which can reduce the return bandwidth attrition and service latency and improve the user service experience.
(3) Business optimization: through the MEC server near the wireless side, information from the wireless network can be collected and analyzed in real time, and the network conditions can be obtained to perform dynamic and quick optimization of services, select the appropriate service rate, content diversion mechanism, congestion control strategy, etc.
(4) Through the MEC platform, mobile networks can provide network resources and capabilities to third parties (MVNOs), open up capabilities such as network monitoring, network infrastructure services, QoS control, positioning, big data analysis, and others to the outside world, identify the development potential of network services, and achieve a win-win situation with partners.

## 4. Discussion

This study builds a 5G Local Breakout Private Network System environment and combines with Wi-Fi 6 to extract the MAC of the terminal carrier to build a security validation loop to validate that the IOTA transaction achieves a fast identity authentication mechanism to provide high-speed computing and reduce the transmission

latency, focusing on the local offload of information services to reach the near-side service access, and how to manage specific users accessing the field and provide a flexible and customized field management mechanism since the provision of application services in the field and the management of users accessing the field have high information security requirements.

### 4.1. 5G local breakout standalone private network

If an enterprise requires high network autonomy and privacy, it is provided with a standalone private network, from the base station, the MEC to the core network, with a complete set of mobile network deployment placed on the enterprise client side, and a standalone private network is set up to provide the dedicated base station for the enterprise, and the signal coverage is based on the area of the private network of the enterprise (as shown in Fig. 6.).

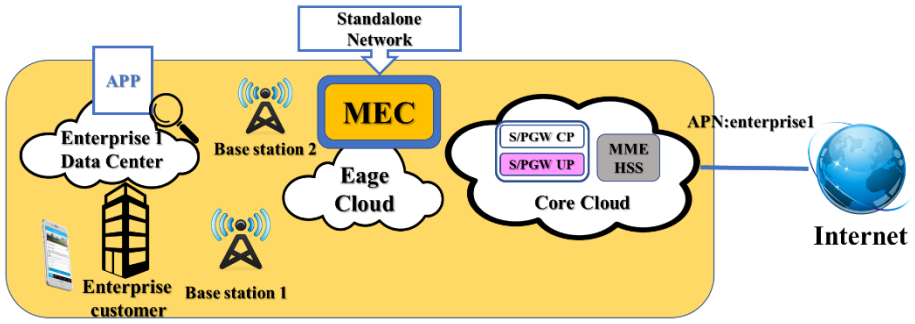


**Fig. 6.** MEC Standalone Private Network Architecture

In order to provide high-speed computing and reduce transmission latency, MEC mobile edge computing focuses on the local offload of information services to reach the near-side service access, and enterprises often deploy MEC directly in the fields of the enterprises. Since enterprise customers have high information security requirements for the provision of application services in the field and the management of users accessing the field, how to manage specific users accessing the field and provide a flexible and customized field management mechanism is the core of the problem to be discussed in this paper.

Through the implementation of MEC type private access, this architecture can access the signals and services flowing through the network by connecting in series base stations and core networks in series in a transparent and pass-through manner, and it can conduct in-depth tests of the MEC mobile edge computing network, develop dynamic service content, application host management, and content diversion mechanism, provide control of the users accessing the fields, and site equipment network management such as real-time alarm notification, remote monitoring, etc. It is the most flexible MEC mobile edge computing architecture.

### 4.2. Process Design for Identity Authentication of 5G and Wi-Fi Combined with IOTA

In this study, we simulate how to authenticate the terminal identity through the integration of two access technologies in a hybrid multi-type network environment of a standalone 5G Local Breakout private network combined with Wi-Fi 6. The architecture and flow of the system are shown in the system authentication flow chart. The main authentication mechanism is divided into three parts. The first part is the terminal device, the second part is the identity authentication web page, and the third part is the IOTA node (as shown in Fig. 7.).

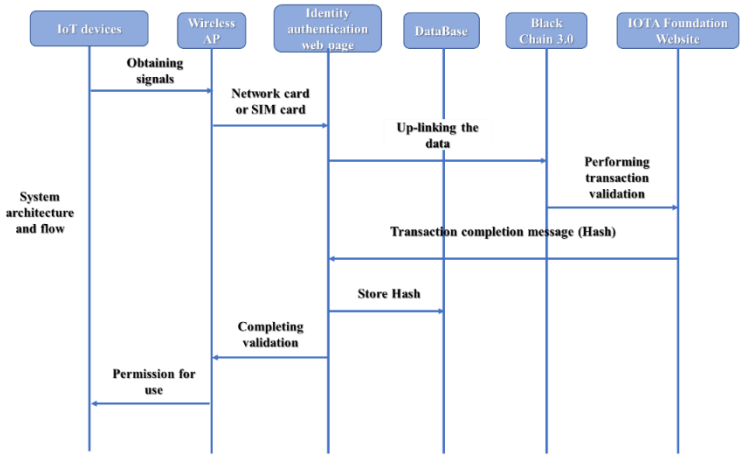


**Fig. 7.** System Authentication Flow Chart

### 4.3. IOTA node transaction validation

The 5G and Wi-Fi identity authentication process combined with IOTA includes a Hash that is obtained after the transaction is completed. To validate whether or not the data in this hash is the data of the original network card, this hash can be entered into the IOTA node website to query it (as shown in Fig. 8.).

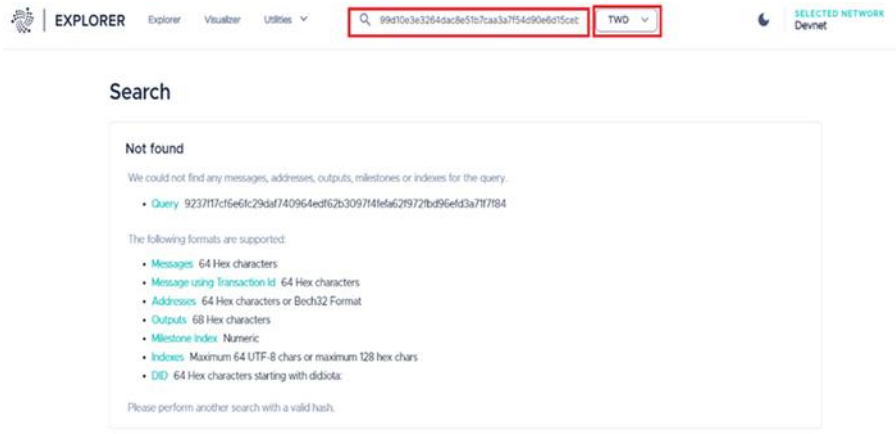


**Fig. 8.** IOTA Foundation Validation Screen

The data validation screen clearly shows that the Hash of this transaction can be used to find the data of the original transaction on the network card, which confirms that the result of this study is correct (as shown in Fig. 9.).

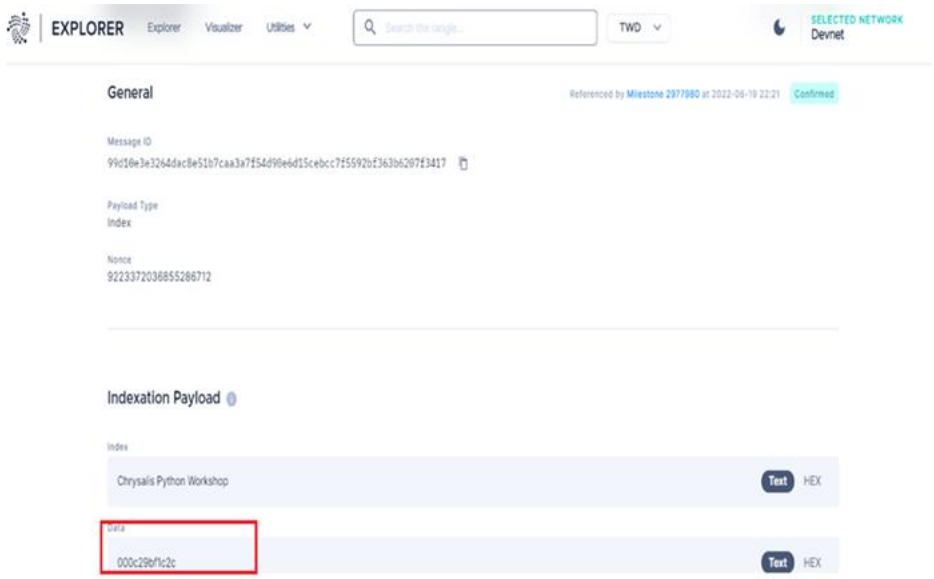


**Fig. 9.** Data Query Screen of the Node Transaction

From this validation website, we can see the transaction validation record screen (as shown in Fig. 10.). Before completing the validation of this transaction, we have validated the two-transaction data on the right side and know the transaction data we have completed and the transactions that are provided for validation.

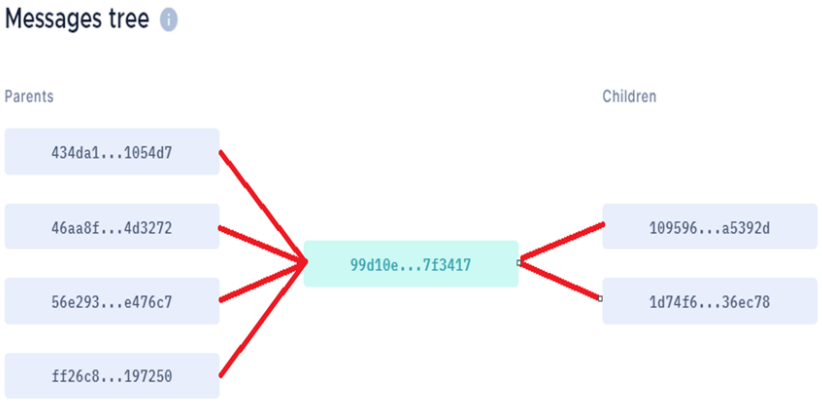


**Fig. 10.** Validation record screen of the node transaction

## 5. Conclusions

The lack of penetration of 5G signals requires the use of free unlicensed spectrum available in Wi-Fi technology to compensate for this problem. Therefore, the coexistence of 5G and Wi-Fi 6 in the future environment makes the two technologies complement each other, which has become the new trend in wireless communication in the future. The development of blockchain technology is no longer based primarily on mining; instead, it is replaced by the application of IoT and the validation through smart contracts. After blockchain 3.0 technology has overcome the problem that the more people use the blockchain, the slower it becomes and no longer has the role of miners. The IOTA Foundation created a new decentralized ledger technology called Tangle, which solves the current problem of blockchains 1.0 and 2.0 that the more people use it, the less efficient it is, and creates a new consensus method in a decentralized peer-to-peer solution. In other words, as long as two transactions are validated, it is no longer the mining ability that determines the trading partner.

The IOTA technology uses bundles to organize several transactions, including the output to the receiving address and the input from the sending address; in the IOTA technology transaction validation behavior, the transaction signature can be simply converted to the terminal MAC, so that the IOTA transaction mode is used for validation, and private nodes are set up in the 5G multi-type network. Then the relevant functions provided by IOTA are used to solve the identity authentication (network card) problem of IoT devices in WI-Fi -6 and 5G network environment through IO-TA technology.

Simply put, the characteristic that the IOTA signature can be converted to the terminal MAC is used to package the IOT network cards into a transaction using the Python function developed by IOTA, and the transaction is sent to the IOTA node for validation using the IOTA validation function. After validation, the HASH value of a transaction is sent back, completing a transaction. The next step is to prove the validity

of the obtained HASH value. In the IOTA node validation function, the above HASH value can be entered to decode the network data from the initial validation to achieve fast identity authentication.

This study enables the establishment of terminal devices that can allow WI-Fi-6 and 5G network environments to have unique and identifiable identities, with non-repudiation and privacy, and with the function of mutual authentication, for authentication in heterogeneous network environments. This study has already addressed this problem using IOTA technology, which can also be combined with blockchain technology in the new heterogeneous wireless network environment and is very convenient. Their applications can be very diversified, and we believe that more and more studies related to blockchain and 5G environment will be conducted to maximize the potentials of relevant technologies.

## References

1. S. Henry, A. Alsohaily and E. S. Sousa.: 5g is real: Evaluating the compliance of the 3gpp 5g new radio system with the itu imt-2020 requirements, IEEE Access, 8, 42828-42840. (2020)
2. C.-C. LIU.: A lightweight security scheme with mutual authentication in mobile edge computing. Master's Thesis, Department of Information and Communication Engineering,Chaoyang University of Technology. (2020)
3. W. Serrano, The blockchain random neural network for cybersecure iot and 5g infrastructure in smart cities, Journal of Network and Computer Applications, 175, 102909. (2021)
4. K.-H. LIN.: An efficient group-based service authentication and session key negotiation scheme for mmtc devices in 5g. Master's Thesis, Computer Science and Information Engineering,National Chung Cheng University. (2019)
5. K. Yue, Y. Zhang, Y. Chen, Y. Li, L. Zhao, C. Rong and L. Chen.: A survey of decentralizing applications via blockchain: The 5g and beyond perspective, IEEE Communications Surveys & Tutorials , 23 , no. 4, 2191-2217. (2021)
6. M. Hirzallah, M. Krunz, B. Kecicioglu and B. Hamzeh.: 5g new radio unlicensed: Challenges and evaluation, IEEE Transactions on Cognitive Communications and Networking ,7, no. 3, 689-701. (2020)
7. E. Al Abbas, M. Ikram, A. T. Mobashsher and A. Abbosh.: Mimo antenna system for multi-band millimeter-wave 5g and wideband 4g mobile communications, IEEE Access ,7, 181916-181923. (2019)
8. Q. Hao, L. Sun, S. Guo, H. Liu, D. Qian and X. Zhu.: Improvement of eap-tls protocol based on pseudonym mechanism, 2021 International Conference on Wireless Communications and Smart Grid (ICWCSG), IEEE, 23-28. (2021)
9. Y. Siriwardhana, P. Porambage, M. Liyanage and M. Ylianttila.: A survey on mobile augmented reality with 5g mobile edge computing: Architectures, applications, and technical aspects, IEEE Communications Surveys & Tutorials ,23, no. 2, 1160-1192. (2021)
10. A. Ghosh, A. Maeder, M. Baker and D. Chandramouli.: 5g evolution: A view on 5g cellular technology beyond 3gpp release 15, IEEE access ,7, 127639-127651. (2019)
11. A. Yazdinejad, R. M. Parizi, A. Dehghantanha and K.-K. R. Choo.: Blockchain-enabled authentication handover with efficient privacy protection in sdn-based 5g networks, IEEE Transactions on Network Science and Engineering ,8 ,2019, no. 2, 1120-1132.
12. E. Mozaffariahrar, F. Theoleyre and M. Menth.: A survey of wi-fi 6: Technologies, advances, and challenges, Future Internet ,14, no. 10, 293. (2022)

13. K. Ramezanpour, J. Jagannath and A. Jagannath.: Security and privacy vulnerabilities of 5g/6g and wifi 6: Survey and research directions from a coexistence perspective, arXiv preprint arXiv:2206.14997. (2022)
14. J.-D. Li and C.-P. Fan.: Design and vlsi implementation of low latency ieee 802.11 i cryptography processing unit, Journal of Advances in Computer Networks ,8, no. 1. (2020)
15. B. Dey, S. Vishnu and O. S. Swarnkar.: An efficient dynamic key based eap authentication framework for future ieee 802.1 x wireless lans, Proceedings of the 2nd International Conference on Digital Signal Processing,125-131. (2018)
16. M. Rudenkova.: A methodology of modeling the ieee 802.11 wireless lan using ns-3, 2020 V International Conference on Information Technologies in Engineering Education (Inforino), IEEE, 1-4. (2020)
17. L. Tennant.: Improving the anonymity of the iota cryptocurrency, Univ. Cambridge, Cambridge, UK, Tech, 1-20. (2017)
18. B. Goswami and H. Choudhury.: A blockchain-based authentication scheme for 5g-enabled iot, Journal of Network and Systems Management ,30, no. 4, 1-33. (2022)
19. S. Popov.: The tangle, White paper ,1, no. 3. (2018)
20. M. Bhandary, M. Parmar and D. Ambawade.: A blockchain solution based on directed acyclic graph for iot data security using iota tangle, 2020 5th International Conference on Communication and Electronics Systems (ICCES), IEEE, 827-832. (2020)
21. S. Sicari, A. Rizzardi and A. Coen-Porisini.: 5g in the internet of things era: An overview on security and privacy challenges, Computer Networks,179, 107345. (2020)
22. I. Guidebook.: What is iota? (2022)
23. X. Xiao, F. Guo and A. Hecker.: A lightweight cross-domain proximity-based authentication method for iot based on iota, 2020 IEEE Globecom Workshops GC Wkshps, IEEE, 1-6. (2020)
24. C. Igiri, D. Bhargava, C. Udanor and A. Sowah.: Blockchain versus iota tangle for internet of things: The best architecture, Blockchain Technology, 259-278. ,(2022)
25. Y.-C. Wang.: Implementation of iot service management by applying blockchain and the study of peering management scheme in the chain. Master's Thesis, Department Communication Engineering,National Central University. (2019)
26. W. F. Silvano and R. Marcelino.: Iota tangle: A cryptocurrency to communicate internet-of-things data, Future Generation Computer Systems ,112, 307-319. (2020)
27. P. Gangwani, A. Perez-Pons, T. Bhardwaj, H. Upadhyay, S. Joshi and L. Lagos.: Securing environmental iot data using masked authentication messaging protocol in a dag-based blockchain: Iota tangle, Future Internet ,13, no. 12, 312. (2021)
28. I. Dinur, O. Dunkelman and A. Shamir.: Collision attacks on up to 5 rounds of sha-3 using generalized internal differentials, International Workshop on Fast Software Encryption, Springer, 219-240. (2013)
29. F. Liu, T. Isobe, W. Meier and Z. Yang.: Algebraic attacks on round-reduced keccak, Information Security and Privacy: 26th Australasian Conference, ACISP 2021, Virtual Event, December 1–3, 2021, Proceedings 26, Springer, 91-110. (2021)
30. M. Colavita and G. Tanzer.: A cryptanalysis of iota's curl hash function, White paper, 1-13. (2018)

**Jui-Hung Kao** is an assistant professor at Shih Hsin University since 2020. During his tenure as project manager at the Research Center for Humanities and Social Sciences in 2014, he was responsible for the administrative business of research and program execution, which combined statistical methods with spatial information visualization, and is good at writing programs and data analysis. The topics of empirical research focus on three parts: spatial data analysis, medical management research, and long-term medical policy.

**Yu-Yu Yen** has been working as adjunct assistant professor in the Center for General Education at Shih Hsin University since 2022, and has also been assisting in the 5G Education Network Industry-Academia Collaboration Project at the Center for Cloud & IOT research in the College of Management, Shih Hsin University. She also currently enrolled in a PhD program in the Department of Biomedical Engineering, National Yang Ming Chiao Tung University.

**Wei-Chen Wu** was born in Taipei, Taiwan R.O.C. He is Assistant Professor in the Department of Finance at the National Taipei University of Business. He received his Ph.D. degree in Information Management from National Central University in 2016. From 2020-2021, He was Assistant Professor in the Department of Finance at the Feng Chia University. From 2008-2016, he was also an Assistant Professor and Director of the Computer Center at the Hsin Sheng College of Medical Care and Management. His teaching interests lie in the area of programming languages, ranging from theory to design to implementation, and his current research interests include blockchain technology, fintech cybersecurity, network security, and deep learning. Wei-Chen Wu has collaborated actively with researchers in several other disciplines of computer science. He has served on many conference and workshop program committees and served as the workshop chair for Frontier Computing Conference (FC2017~FC2021) and Machine Learning on FinTech, Security and Privacy Conference (MLFSP2019~MLFSP2022).

**Horng-Twu Liaw** is a professor of Information Management at Shih Hsin University since 2004, and he is the Vice President of Shih Hsin University since 2018. He has studied e-Commerce and networking communities, service-oriented information technology and management, information system development and project management, network management and information security, and information security management. The focus of empirical research in recent years has focused on spatial data analytics, information security, big data analytics, and artificial intelligence.

**Shiou-Wei Fan** is a full-time lecturer at Shih Hsin University, has served as the Chief of network management division in the Office of Library and Information Services for 27 years. His main expertise is network management, network security, and cloud services.

*Received: November 15, 2022; Accepted: September 19, 2023.*