IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, May 2023

Improved User Authenticated Key Management Scheme for 6G based Industrial Applications

Dr. G. Nanthakumar[1], E. Nithish[2], R. Ramkumar[3], P. Santhakumar[4], R. Senthilraj[5]
Professor, Department of Computer Science and Engineering[1]
Students, Department of Computer Science and Engineering[2,3,4,5,6]
Anjalai Ammal Mahalingam Engineering College, Kovilvenni, Tiruvarur, Tamil Nadu, India

Abstract: *The Network In a Box is only one of the cutting-edge features that the Sixth Generation (6G) mobile technology is anticipated to provide (NIB). The NIB is a multi-generational, readily installable technology that offers connection services to applications utilised in uncommon circumstances, like on the battlefield or during natural catastrophes. Security is becoming even more crucial in the 6G communication system, and the NIB is no exception. Many active and passive attacks on the applications used in the 6G-enabled NIB are possible as a result of the unsecured channel. Having a secure user authentication and key management system in place is therefore essential. In order to protect the 6G-enabled NIB (iUAKMS-NIB) that can be used in industrial applications, this article suggests an enhanced user authentication and management scheme. The suggested method offers the best security against potential assaults on the 6G communication system because it is a modified and upgraded version of UAKMS-NIB. The key benefit of the suggested plan is that it outperforms other schemes in terms of performance. The analytical outcomes demonstrate that the suggested system offers improved security and is capable of withstanding a variety of attacks. In conclusion, the enhanced User Authentication and Management System that has been proposed is a crucial security measure for the 6G-enabled NIB. It performs better than conventional techniques and guarantees safe user authentication and key management.*

Keywords: 6G.

I. INTRODUCTION

1.1 6G Technology

The sixth generation of wireless technology, or 6G, is still in its early phases of development. The present 5G technology is predicted to be replaced by this one, which will offer even higher data speeds, lower latency, and more capacity [11]. Furthermore, new use cases and applications are anticipated, including holographic communications, cutting-edge virtual and augmented reality, and more accurate location services [12]. Terahertz (THz) frequency communication, which has the ability to greatly enhance data transfer rates, is likely to be one of the core components of 6G. But there are still a lot of technical issues with this technology, and it is still in the research stage [2], [12].Several groups, including tech firms, academic institutions, and governmental bodies, are pushing the development of 6G. 6G is not projected to be widely adopted for some more years, with commercial deployments perhaps beginning in the late 2020s or early 2030s. In general, 6G is anticipated to bring forth a new era of wireless communication with higher speeds and more sophisticated capabilities that will revolutionise the way people interact with technology and communicate [13].

1.2 Network in a Box

In instances where traditional network infrastructure is unavailable, harmed, or destroyed, NIB (Network in a Box) technology offers a self-contained wireless communication network that may be quickly constructed. The system's independence makes it perfect for usage by military and emergency response teams as well as in remote or disaster-stricken locations. NIBs often include portable radios, antennae, and networking hardware together with software components that are convenient to move. Since they can be powered by batteries, solar panels, or other electricity-generating devices, they are very adaptable. Future mobile communication networks, including 6G, are likely to be

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, May 2023

heavily reliant on NIB technology, which is predicted to grow quickly. NIBs may have cutting-edge privacy and security measures in addition to connectivity services to defend against dangers like as cyberattacks.In general, NIBs are a significant development that allow connectivity in places where conventional infrastructure is unavailable or degraded. NIBs are expected to become more more adaptable, secure, and simple to deploy as technology advances, making them a crucial tool for the military, emergency response, and other organisations that require dependable wireless communication in difficult circumstances.

A. 6G-enabled Network in a Box

New technology known as the 6G-enabled Network in a Box (NIB) is being created as part of the upcoming introduction of the next generation of mobile networks. It is a compact, easily deployable gadget that can be used to swiftly set up a secure mobile network in difficult, off-the-grid situations, including war zones. The 6G-enabled NIB will offer its users low-latency, high-bandwidth communication services by combining hardware and software technologies. Also, it will be able to support a variety of applications, such as the Internet of Things, augmented and virtual reality, and high-definition video streaming (IoT).The 6G-enabled NIB's versatility, which enables speedy deployment in a variety of contexts, is one of its key advantages. It is also intended to be extremely secure, using cutting-edge authentication and encryption technologies to guard against online threats and other security hazards. Therefore, it is anticipated that the 6G-enabled NIB would be crucial in meeting the rising demand for mobile access, especially in difficult and isolated locations where standard mobile networks are unavailable or unstable.

1.3 UAKMS

The security protocol known as UAKMS, or User Authentication and Key Management Scheme, is employed in wireless sensor networks (WSNs) to provide safe communication between the sensor nodes. For the sensor nodes, which frequently have limited processing, memory, and energy resources, UAKMS offers secure and effective key management. The system employs a hierarchical structure, with the base station serving as the hierarchy's root node and the sensor nodes serving as its leaves. Keys are distributed by the base station to the higher level nodes in the hierarchy, who then pass the keys down to the lower level nodes. This makes key management and distribution more effective because each node does not need to get a key separately. The base station authenticates the sensor nodes in UAKMS before distributing keys, which also contains a user authentication method. As a result, only approved nodes are permitted to connect to the network and view the data. Overall, UAKMS is a simple and effective method for protecting wireless sensor networks, especially in situations with limited resources. It has been applied to many different things, like healthcare, industrial control, and environmental monitoring.

II. RELATED WORKS

2.1 Privacy-Aware Task Allocation

The widespread use of mobile devices, particularly smartphones, has fundamentally altered the conventional static sensor-based data sensing method, creating a new paradigm for data gathering and analysis known as mobile crowdsensing. (or crowdsensing for short). the use of cellular technology With the aid of modern technologies (such as WiFi, 4G, and Bluetooth) and the extensive embedded sensors (such as the camera, GPS, and accelerometer) on mobile devices, mobile users and participants can easily complete the various tasks that task owners (TOs) have posted on a crowdsourcing platform. The sensing data are produced by the participant's personal expertise in addition to the embedded sensors, providing more thorough and varied information for TOs.

2.2 6G-Enabled Network in Box

NIB and 6G integration leads to decentralised geographical crowdsourcing in industrial automation, but it also compromises task and answer security and exposes the positions of sensor nodes. We provide a safe, decentralised geographical crowdsourcing system for 6G-enabled networks in Box to solve these issues (DSC-NIB). Without relying on a third party, the control station and sensing nodes can gather and transmit data on the blockchain utilising NIB using DSC-NIB. In order to protect the privacy of sensing nodes' positions, the control station negotiates session keys

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, May 2023

and a group key with sensing nodes whose locations fulfil the location strategy. We use the Counter with CBC-MAC (CCM) authenticated encryption for task and answer security.

A. Long-Term Evolution

Enhancing the Long-Term Evolution (LTE) networks' resilience in support of military and public safety activities. These strategies may be made feasible by the 3GPP LTE standards and may also be implemented as software upgrades for current systems. Multiple Servicing/Packet Gateways (S/P GWs), for instance, were able to function dynamically through multiple Sm-GWs in a large number of tiny cells thanks to a management strategy established in [28]. Smart gateways (Sm-GWs), which are SDN-based, were in charge of organising the adaptive distribution of uplink transmission bit rates to evolved NodeBS (eNB) according to requirements.

B. Technological Advancements for 6G Cell Network

The significant technological advancements that may power the 6G cell network. For instance, "cognitive spectrum sharing techniques for new spectrum bands," "integration of localization and sensing capabilities," "achievement of extreme performance requirements in terms of latency and reliability," and "achievement of localization and sensing capabilities." Advanced security and privacy techniques, as well as novel network architecture paradigms like "sub-networks" and "RAN-Core convergence," are all explained.

C. Information exchange in the 6G Era

The emphasis of wireless research is gradually shifting towards 6G as 5G deployments get underway. It is now essential to establish a vision for future communications in order to give that research direction. We strive to provide a complete picture of the communication needs and technology in the 6G era in this piece. The development of digital twin worlds, which faithfully represent our experiences in every instant of space and time, holds the key to the connectedness of the future. These worlds will connect our experiences in the physical, biological, and digital realms. New themes, such as: I novel man-machine interfaces produced by a collection of numerous local devices working cooperatively, are anticipated to shape the requirements and technologies of the 6G system.

D. Lightweight Authentication Scheme

When referring to authentication,[2] the term "lightweight" refers to the usage of procedures with little processing and communication overhead that are appropriate for devices with limited resources, like embedded systems and sensors. These techniques are often made to be effective and use the least amount of memory and processing resources while yet offering a sufficient level of security.

Typical light-weight authentication methods are as follows:

1. Pre-shared keys (PSK): This type of communication uses a secret key that is exchanged between the two parties. PSKs are simple to set up and use few resources, but if the key is stolen, they can be attacked.
2. A challenge message is sent from the server to the client in challenge-response authentication, and the client must react with the right answer.This approach is frequently used in smart card authentication and is effectively implemented on devices with little resources.
3. Using a password that is only good for one authentication session is known as a one-time password (OTP). OTPs are frequently used in two-factor authentication and can be generated using a variety of methods, including time-based or event-based algorithms.

In conclusion, efficient communication security in resource-constrained contexts can be achieved without placing an undue burden on processing or communication resources by using lightweight authentication systems.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, May 2023

III. LITERATURE REVIEW

TITLE	AUTHOR NAME	YEAR	TECHNIQUE	MERITS	DEMERITS
Designing an Enhanced User Authenticated Key Management Scheme for 6G-Based Industrial Applications	Ijaz Darman, Musaria Karim Mahmood, Shehzad Ashraf Chaudhry	16 August 2022	6G enabled NIB technologies	Disaster management lacked networking plans and failed to provide better communication.	Security issue
Network-In-a-Box: A Survey about On-Demand Flexible Networks	M. Pozza, A. Rao, H. Flinck, and S. Tarkoma	Feb. 2018.	On-Demand Flexible Networks	The architecture of a 5G network has evolved into a welldefined design with a precise list of features.	We believe that the Network-Ina-Box can become the building block for generating flexible and adaptable networks.
Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems	W. Saad, M. Bennis, and M. Chen,	May/Jun. 2020	Applications, trends, technologies, and open research problems	New applications: • MBRLLC • MURLLC • HCS • MPS	eMBB URLLC mMTC
Designing Authenticated Key Management Scheme in 6G-Enabled Network in a Box Deployed for Industrial Applications	M. Wazid, A. K. Das, N. Kumar, and M. Alazab	Oct. 2021.	6G-enabled network in a box (NIB) is a multigenerational , rapidly deployable hardware, and software technology for communication.	a new remote user authentication and key management scheme is proposed for securing 6G-enabled NIB deployed for industrial applications,	various passive and active attacks are possible
A Logic of Authentication	M. Burrows, M. Abadi, and R. M. Needham,	1989.	Authentication protocols are the basis of security in many distributed systems,	The goal of authentication can be stated rather simply, though informally and imprecisely.	Their design has been extremely error prone.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, May 2023

IV. SYSTEM ARCHITECTURE

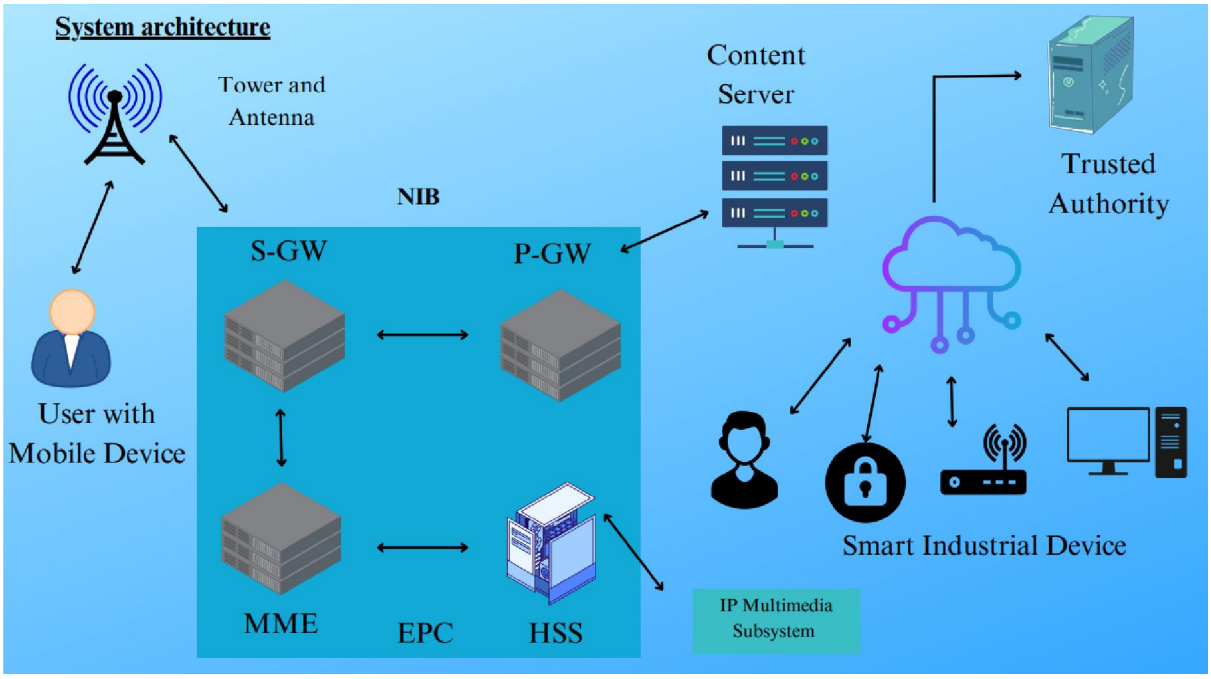

Fig1 (System Architecture)

4.1 Network Model

The network concept shown in the diagram is intended for smart industrial devices that can connect to a 6G network. The architecture is made up of various parts that cooperate to ensure that the device can gather, transmit, and process sensor data in real-time while also offering users value-added services.

The 6G equipped network infrastructure receives sensor data that was collected by the smart industrial equipment. A Network Interface Box (NIB), an Evolved Packet Core (EPC), and different gateway components (P-GW, S-GW, and MME) make up the architecture. These components are in charge of routing the traffic.

The smart industrial device and the rest of the network infrastructure are interfaced by the NIB. It handles packet filtering, traffic shaping, and communication protocol conversion. Making sure that only authorised traffic is permitted to pass through to the EPC is the responsibility of the NIB.All network traffic's authentication, authorisation, and accounting are handled by the EPC. It is made up of different gateway components, including the P-GW, S-GW, and MME. The P-GW is in charge of overseeing IP address distribution and directing traffic to the proper area. The S-GW is in charge of controlling the device's mobility, while the MME is in charge of controlling the network's signalling and control mechanisms.

User authentication and permission are handled by the Home Subscriber Server (HSS). It oversees the authentication and authorisation procedure for each user and keeps user profile information such as authentication credentials like usernames and passwords. The application data is hosted by the content server, which also offers services to users. Users communicate with the gadget by sending requests and commands through the network infrastructure. These requests and directives are received by the content server, which then processes them and replies with the relevant information.

In conclusion, the network model architecture is built to make sure that the smart industrial device can record, transmit, and process sensor data in real-time while also offering users value-added services. It accomplishes this by utilising a number of elements, including the NIB, EPC, HSS, and content server, which collaborate to guarantee that traffic is allowed, authenticated, and processed quickly.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, May 2023

4.2 Threat Model

The well-known "Dolev-Yao threat model" serves as the foundation for the threat model for iUAKMS-NIB (DY model). According to the DY model, parties that engage with end-point entities (such as users and intelligent industrial equipment) are frequently not viewed as trustworthy and communicate with one another across an open channel. In this scenario, the attacker (designated as "A") seeks to undermine the network's security by tampering with messages or by exploiting session keys, private keys, and other session states.The Trusted Authority (TA), which is in charge of registering network entities, is regarded as a completely trusted node in the iUAKMS-NIB threat model. The security of the entire network may be jeopardised if the TA is breached or hacked. As a result, safeguarding the TA is essential to the system's overall security.The Content Server is regarded as a semi-trusted entity, which denotes that it is partially trusted but not entirely so, unlike the TA. As a result, it is feasible for an attacker to take over the Content Server and read confidential data or stop the server from offering its services.

Users and industrial devices are not seen to be reliable and are open to assaults like power analysis attacks, which might let an attacker take control of a user's mobile device and extract any sensitive data that has been saved on it from the device's memory.

In general, the iUAKMS-NIB threat model takes into account a variety of potential attacks and vulnerabilities with the goal of creating a security architecture that may reduce these threats and offer a safe and dependable network infrastructure for industrial applications.

4.3 The UAKMS-NIB Scheme of Wazid et Al.

In this work, we provide a thorough examination of the iUAKMS-NIB system's registration phase, user login phase, and user authentication and key agreement phase. A network architecture called the iUAKMS-NIB was created for industrial applications that need dependable and secure connectivity between smart devices and content servers. To guarantee the security and privacy of users' data, the system combines user authentication, key agreement, and identity de-synchronization procedures. In this article, we go into great detail about each stage and talk about the security measures put in place to defend against various assaults.

A. Registration Phase

The registration phase is the first step in the iUAKMS-NIB system, where a new user provides their details and registers on the system.

- User Registration - To register on the system, the user enters their information, including name, email address, and a secure password. The database of the system contains the user's information.
- Smart Device Registration - Once the user is registered, they can proceed to register their smart device on the system. The user provides the device's details, including the device name and device ID, which are stored in the system's database.
- Content Server Registration - The content server is registered on the system, allowing the smart device to communicate with the server and retrieve data. The content server's details, including the server name and server ID, are stored in the system's database.

B. User Login Phase

The user login phase is the second step in the iUAKMS-NIB system, where the user logs in to the system and authenticates themselves.

- User Authentication -To access the system, the user enters their login and password. The system checks the user's credentials and, if they are legitimate, allows access to the system.
- Session Key Generation-Once the user is authenticated, the system generates a session key that is used to encrypt and decrypt data exchanged between the user's device and the content server
- Secure Communicatio*n*-With the session key, a secure communication channel is established between the user's device and the content server. The session key is used to encrypt all data sent between the user's device and the content server.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, May 2023

In order to keep the system secure, only authorised users must log in, which is why this step is crucial. To defend against attacks that target the user login process, the system employs a number of security measures, including two-factor authentication and password hashing.

C. User Authentication and Key Agreement Phase

With the iUAKMS-NIB system, the user's device and the content server agree on a shared session key during the user authentication and key agreement phase.

- User Identity Verification- The system verifies the user's identity using various techniques, such as biometric authentication or one-time passwords.
- Key Agreement -Using a key agreement technique, such as the Diffie-Hellman protocol, the user's device and the content server come to an agreement on a shared session key. Data sent between the user's device and the content server is encrypted and decrypted using the session key.
- Session Key Update - The system periodically updates the session key to prevent unauthorised access

V. IMPLEMENTATION

Module 1: NETWORK MODEL

Step1:Define the network architecture, including the different network components and their relationships.

Step2:Specify the communication protocols used for data transmission between network components.

Data Flow Diagram for Network Model

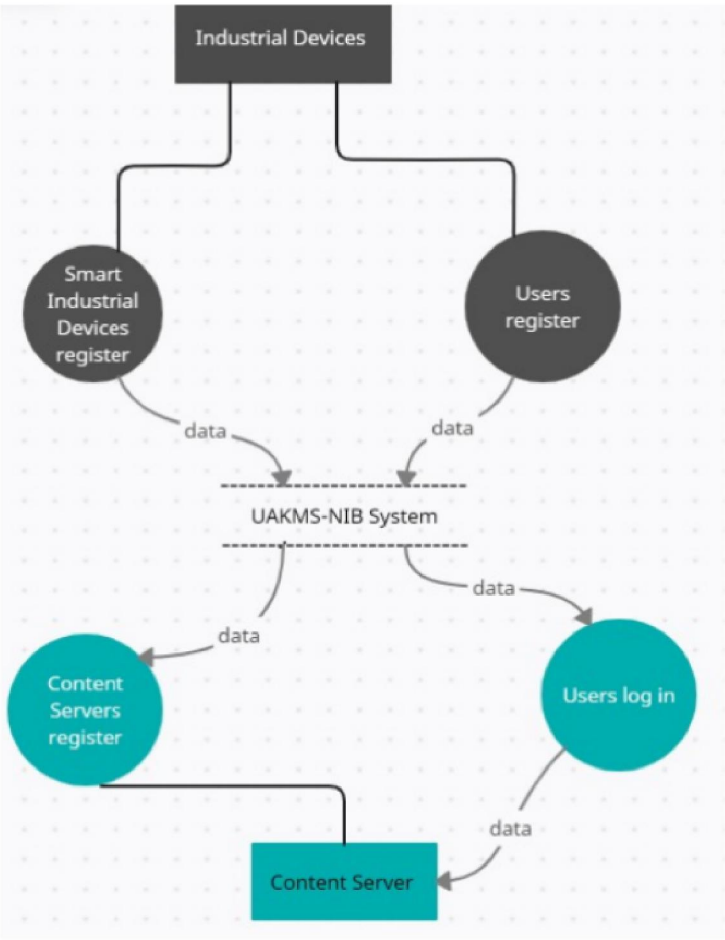

Fig 2 (DATA FLOW DIAGRAM FOR NETWORK MODEL)

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, May 2023

Module 2: THREAT MODEL

Step1:Identify potential threats to the network, including active and passive attacks.

Step2:Evaluate the likelihood and potential impact of each threat.

Step3:Develop strategies to mitigate or prevent each identified threat.

Data Flow Diagram for Threat Model

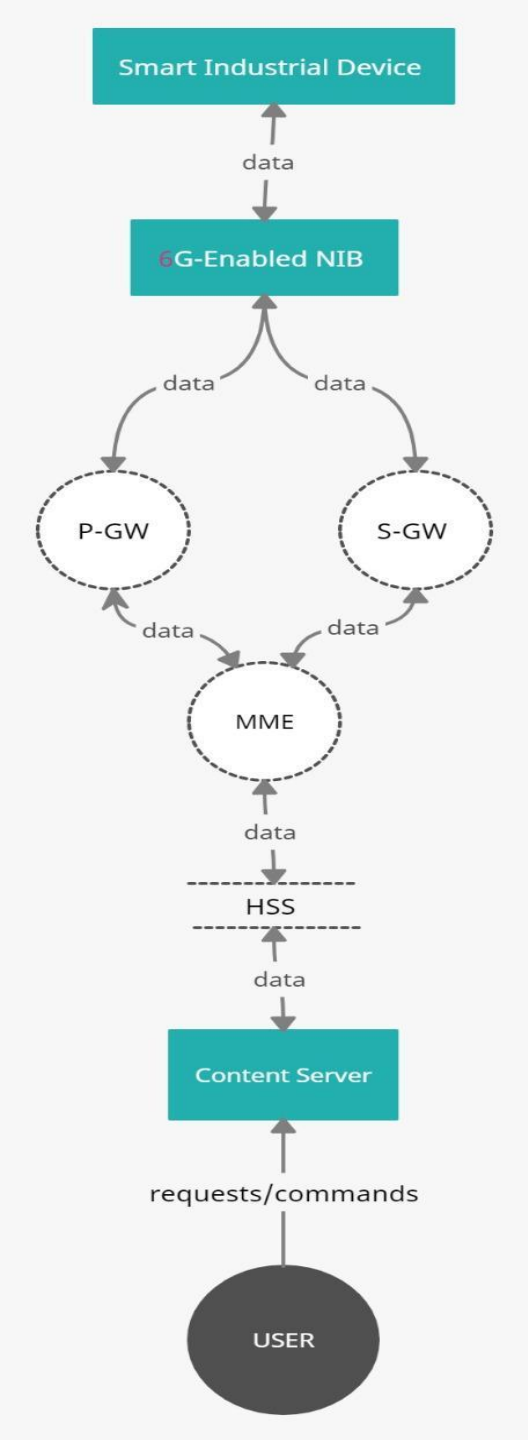

Fig 3(DATA FLOW DIAGRAM FOR THREAT MODEL)

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, May 2023

Module 3: THE UAKMS-NIB SCHEME OF WAZID ET AL.

A. Registration Phase

Step1:A user or device sends a registration request to the NIB.
Step2:The NIB generates a unique identifier and sends it back to the user or device.
Step3:The user or device stores the identifier for future use.

B. User Login and Authentication Phase

Step 1:The user or device sends a login request to the NIB.
Step 2:The NIB sends a challenge to the user or device.
Step 3:The user or device uses their stored identifier and a secret key to generate a response to the challenge.
Step 4:The NIB verifies the response and grants access if it is valid.

Activity Diagram

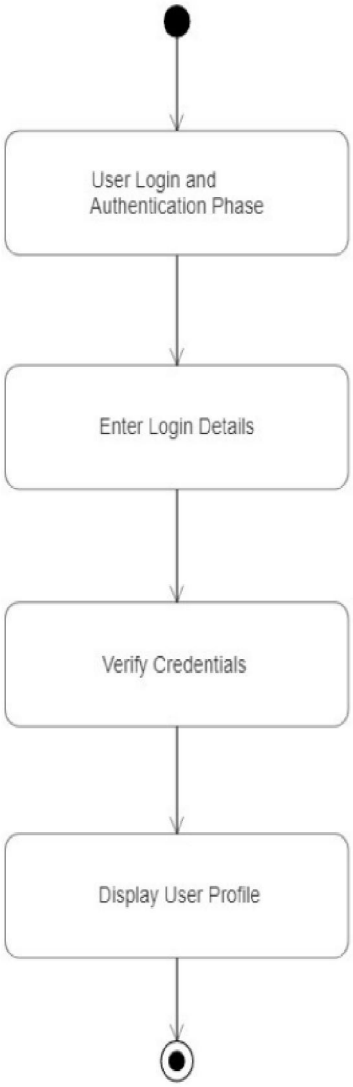

Fig 4 (Activity Diagram)

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, May 2023

Identity De-Synchronization

Smart Industrial Device Registration

Step 1:A smart industrial device sends a registration request to the NIB.
Step 2:The NIB generates a unique identifier and sends it back to the device.
Step 3:The device stores the identifier and uses it for future communication with the NIB.

Content Server Registration

Step1:A content server sends a registration request to the NIB.
Step2:The NIB generates a unique identifier and sends it back to the server.
Step3:The server stores the identifier and uses it for future communication with the NIB.

User Registration

Step1:A user sends a registration request to the NIB.
Step2:The NIB generates a unique identifier and sends it back to the user.
Step3:The user stores the identifier and uses it for future communication with the NIB.

Use Case Diagram

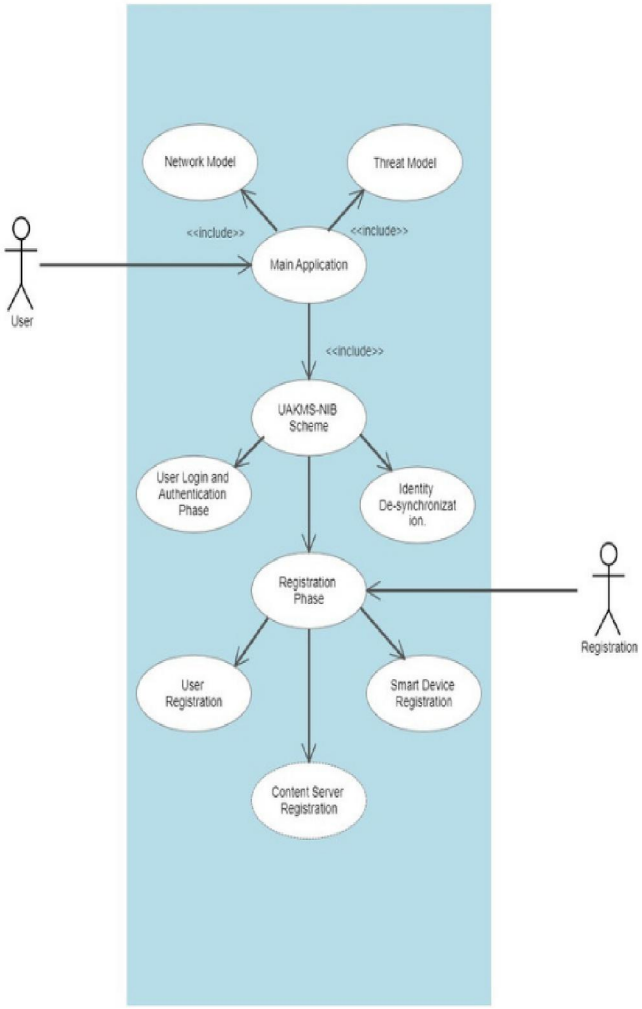

Fig 5(Use case Diagram)

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, May 2023

Collaboration Diagram

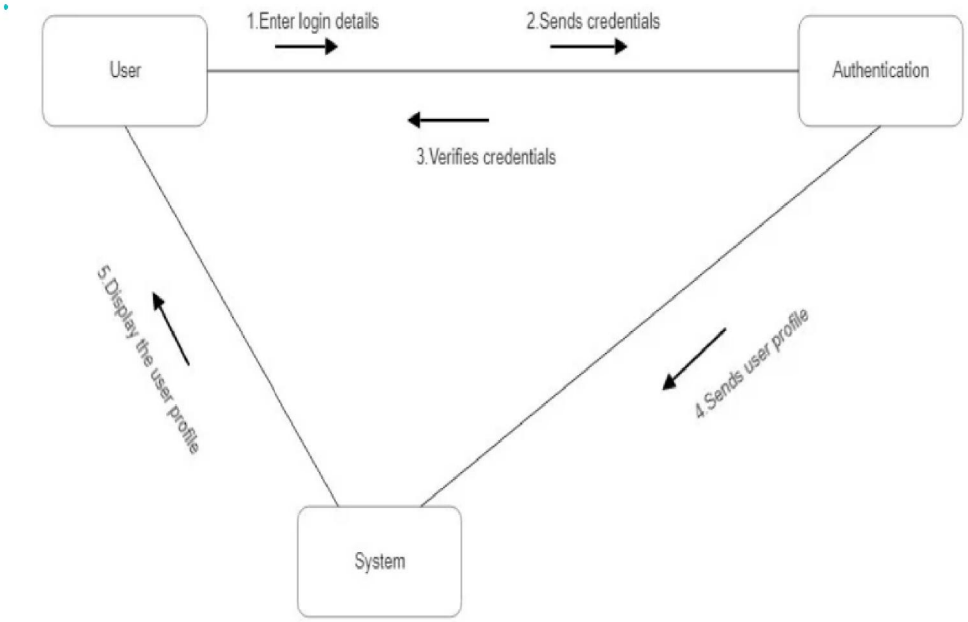

Fig 6

VI. CONCLUSION

To ensure the security of the communication system, an enhanced User Authenticated Key Management Scheme called iUAKMS-NIB must be created for 6G-based industrial applications. The 6G-enabled NIB technology is perfect for industrial applications due to its high level of flexibility and low latency. However, the current NIB apps' lack of adequate security measures can result in a number of aggressive and passive attacks. The proposed iUAKMS-NIB scheme provides a novel remote user authentication and key management solution that delivers better security than existing schemes. The analytical findings show the efficiency of the suggested plan, and it provides a viable security defence against potential 6G communication system threats. Thus, the development and implementation of iUAKMS-NIB can considerably boost the security industrial uses based on 6G.

REFERENCES

[1]. M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, ‘‘Toward 6G networks: Use cases and technologies,’’ IEEE Commun. Mag., vol. 58, no. 3, pp. 55–61, Mar. 2020.

[2]. S. A. Chaudhry, A. Irshad, M. A. Khan, S. A. Khan, S. Nosheen, A. A. AlZubi, and Y. B. Zikria, ‘‘A lightweight authentication scheme for 6G-IoT enabled maritime transport system,’’ IEEE Trans. Intell. Transp. Syst., early access, Dec. 22, 2021, doi: 10.1109/TITS.2021.3134643.

[3]. M. Pozza, A. Rao, H. Flinck, and S. Tarkoma, ‘‘Network-in-a-box: A survey about on-demand flexible networks,’’ IEEE Commun. Surveys Tuts., vol. 20, no. 3, pp. 2407–2428, Feb. 2018.

[4]. H. Yi, ‘‘A secure blockchain system for Internet of Vehicles based on 6G-enabled network in box,’’ Comput. Commun., vol. 186, pp. 45–50, Mar. 2022.

[5]. W. Saad, M. Bennis, and M. Chen, ‘‘A vision of 6G wireless systems: Applications, trends, technologies, and open research problems,’’ IEEE Netw., vol. 34, no. 3, pp. 134–142, May/Jun. 2020.

[6]. (Apr. 2020). 3G4G. Beginners: Network in a Box (NIB). [Online]. Available: https://www.slideshare.net/3G4GLtd/

[7]. (Apr. 2020). A. Networks. System Architecture Evolution (SAE) and the Evolved Packet Core (EPC). [Online]. Available: https://www.art izanetworks.com/resources/tutorials/sae_tec.html

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, May 2023

[8]. P. P. Ray, N. Kumar, and M. Guizani, ''A vision on 6G-enabled NIB: Requirements, technologies, deployments, and prospects,'' IEEE Wireless Commun., vol. 28, no. 4, pp. 120–127, Aug. 2021.

[9]. J.-S. Huang and Y.-N. Lien, ''Challenges of emergency communication network for disaster response,'' in Proc. IEEE Int. Conf. Commun. Syst. (ICCS), Nov. 2012, pp. 528–532.

[10]. Z. Shao, Y. Liu, Y. Wu, and L. Shen, ''A rapid and reliable disaster emergency mobile communication system via aerial ad hoc BS networks,'' in Proc. 7th Int. Conf. Wireless Commun., Netw. Mobile Comput., Sep. 2011, pp. 1–4.

[11]. M. Dohler and D. Simeonidou. (2021). From 5G To 6G Governance. [Online]. Available: https://bit.ly/3AWebvR

[12]. MUNTADHER ALSABAH 1, MARWAH ABDULRAZZAQ NASER 2, "6G Wireless Communications Networks A Comprehensive Survey", November 2, 2021.

[13]. TOOBA FAISAL, MISCHA DOHLER, (Fellow, IEEE), SIMONE MANGIANTE, AND DIEGO R. LOPEZ,. "BEAT: Blockchain-Enabled Accountable and Transparent Infrastructure Sharing in 6G and Beyond"