iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** XII **Month of publication:** December 2024

DOI: https://doi.org/10.22214/ijraset.2024.65721

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue XII Dec 2024- Available at www.ijraset.com

Authentication in IOT

Om Umesh Abhang, Prof. Sonal Chanderi
Member, Keystone School of Engineering

Abstract: ***With the expansion of the Internet of Things (IoT), there is an increasing demand for reliable approaches to authenticate users to maintain safety from unauthorized access. Special consideration should be given to IoT devices from home appliances to industrial equipment that have limited computation capabilities. In the present work, the various types of authentications in IoT such as passwords, tokens, biometrics, and device-based authentication are surveyed. Further, we also discuss the limitations of these methods and specify some of the new technologies coming up including AI and blockchain which can enhance IoT security. : IoT, User Authentication, Security, Connected Devices***
Keywords: IoT, User Authentication, Security, Connected Devices

I. INTRODUCTION

The Internet of Things IoT is a coated network of devices such as smart home systems, industrial machines, and wearable gadgets that exchange information among themselves via the Internet. Consequently, as more and more IoT devices are purchased and used in the daily lives of people, the very protection of these devices from being accessed by unwanted users gains priority. One of the major aspects of security in IoT is user authentication, the capacity to identify only the authorized people and devices accessing the system. Nonetheless, the size as well as capacities of the IoT devices are relatively small in terms of factors like memory storage and processing capabilities. That is the reason why there is a challenge when it comes to conventional security mechanisms since it is difficult to apply measures such as complex passwords or encryption that would require additional computing resources. Furthermore, when it comes to the use of IoT devices, they are used in various sectors ranging from the home to big industries therefore one form of authentication may not work for everyone. To cope with these drawbacks, several types of authentication methods have been invented, those include password-based authentication, token-based authentication, biometric authentication, and device authentication. All these methods do have their advantages and disadvantages relative to the context they are used. This paper investigates these methods and addresses the phenomenon known as IoT authentication, including prospects of new IoT systems that would enhance the security and dependability of IoT systems.

II. TYPES OF AUTHENTICATIONS

In the context of IoT, there are different methods of validating the identities of people or devices that use the system for the purpose of system security. Each method including password authentication and biometric authentication comes with its advantages and disadvantages based on the level of security and the degree of usability. Let's discuss each of these methods in depth:

A. Password-Based Authentication

Thus, the primary means of authentication is the use of a username and password. It is simple and convenient; however, it is a weak area as well because passwords are very easy to steal or guess as they can be attacked by brute forces and other hacking techniques. This method may not be very secure especially when it comes to IoT devices which may have memory or processing constraints.

B. Token-based Authentication

To prevent this kind of theft, users are provided with a temporary code (or a "token") for example on their phone or in their email which needs to be entered together with the username and password. This way your password can be stolen, but not because the token will be available to the thief. Nevertheless, it calls for users to go through many steps in certain cases which is of course not a pleasant experience for many.

C. Biometric Authentication

In this case, Biometric verification refers to the use of various biometrics like the voice of the user, photographs, and fingerprints of the user among others to authenticate users. This method is very secure since it is difficult to impersonate an individual's biometrics. However, it does have some limitations – IoT.

III. ADVANTAGES

A. Enhanced Security

1) Authentication ensures that only authorized users and devices can access the IoT system, protecting against unauthorized access and data breaches.
2) It helps prevent cyberattacks such as hacking, phishing, and brute-force attacks, securing sensitive data transmitted between devices.

B. Data Privacy

1) By verifying the identity of users and devices, authentication helps maintain the privacy of personal and confidential information within IoT networks.
2) It ensures that only trusted users can access data, safeguarding personal information from unauthorized parties.

C. Preventing Device Hijacking

1) Authentication prevents attackers from hijacking or controlling IoT devices. For example, in a smart home system, authentication stops unauthorized users from taking control of devices like security cameras or door locks.

D. Improved Trust Between Devices

1) Device-to-device authentication ensures that only trusted IoT devices can communicate with each other, preventing malicious devices from infiltrating the network.
2) This helps maintain the integrity of communication between IoT devices in various applications, from smart homes to industrial systems.

E. Reduced Risk of Spoofing Attacks

1) Spoofing, where attackers impersonate a trusted device or user, is a common threat in IoT systems. Proper authentication methods like biometrics or device certificates can help minimize the risk of such attacks.

F. Compliance with Regulations

1) Many industries require compliance with security and privacy regulations, such as GDPR or HIPAA in healthcare. Implementing strong authentication methods ensures that IoT systems meet these regulatory requirements, avoiding legal issues and penalties.

G. Supports Scalability

1) As IoT networks grow, strong authentication methods allow for the seamless addition of new devices without compromising security. This is crucial for industries that rely on large-scale IoT deployments, such as smart cities and industrial IoT.

IV. DISADVANTAGES

A. Complex to Set Up

Getting strong authentication methods up and running can be a real headache, especially when you're dealing with a variety of devices. Each device may have different capabilities, making integration tricky and sometimes more expensive.

B. Limited Resources of Devices

Many IoT devices are pretty basic when it comes to processing power and memory. This can make it hard to implement advanced security features, like encryption or biometric scanning. Sometimes, to keep things simple, weaker security measures end up being used.

C. User Frustration

Stricter security measures, like two-factor authentication or biometric scans, can be a hassle for users. When people find these methods too cumbersome, they might skip them altogether or settle for less secure options, which defeats the purpose of having strong authentication in the first place.

D. Costly Implementation

Setting up solid authentication systems can come with a hefty price tag. For small businesses or startups, the cost of necessary hardware and software, along with ongoing maintenance, can feel overwhelming.

E. Single Points of Failure

If your authentication relies on a central server or a particular method (like biometric data), it creates a potential weak link. If that system gets compromised, every connected device could be at risk, and that's a scary thought!

F. Managing User Access

In large organizations, keeping track of who has access to what can become a logistical nightmare. Ensuring that only authorized people can use specific devices can take a lot of time and effort, leading to management headaches.

G. Risk of Phishing

Even with strong authentication in place, users can still fall for phishing scams. If someone tricks a user into giving away their login details, it can compromise even the best security systems.

V. APPLICATION

A. Smart Homes

The usage of devices such as smart locks and security cameras makes it impossible for any intruder to gain entry into the house since these devices require identity verification.

B. Healthcare Devices

Devices such as wearable health monitors or any other medical device are required to prohibit access to personal health records except to authorized users such as doctors.

C. Industrial IoT (IIoT)

Factories have machines checked using IoT devices. This helps gain access to systems without the permission of the operations, which guarantees the safety of operations.

D. Smart Cities

This is the case with the cities where IoT technology is used to control traffic lights, collection of waste, and so forth. Users who have been permitted to use the system should be the only ones who can change such settings.

E. Agriculture

Some aspects of IoT in farming include gauging crop and soil conditions. People who have been given permission are the only ones who can control the watering systems.

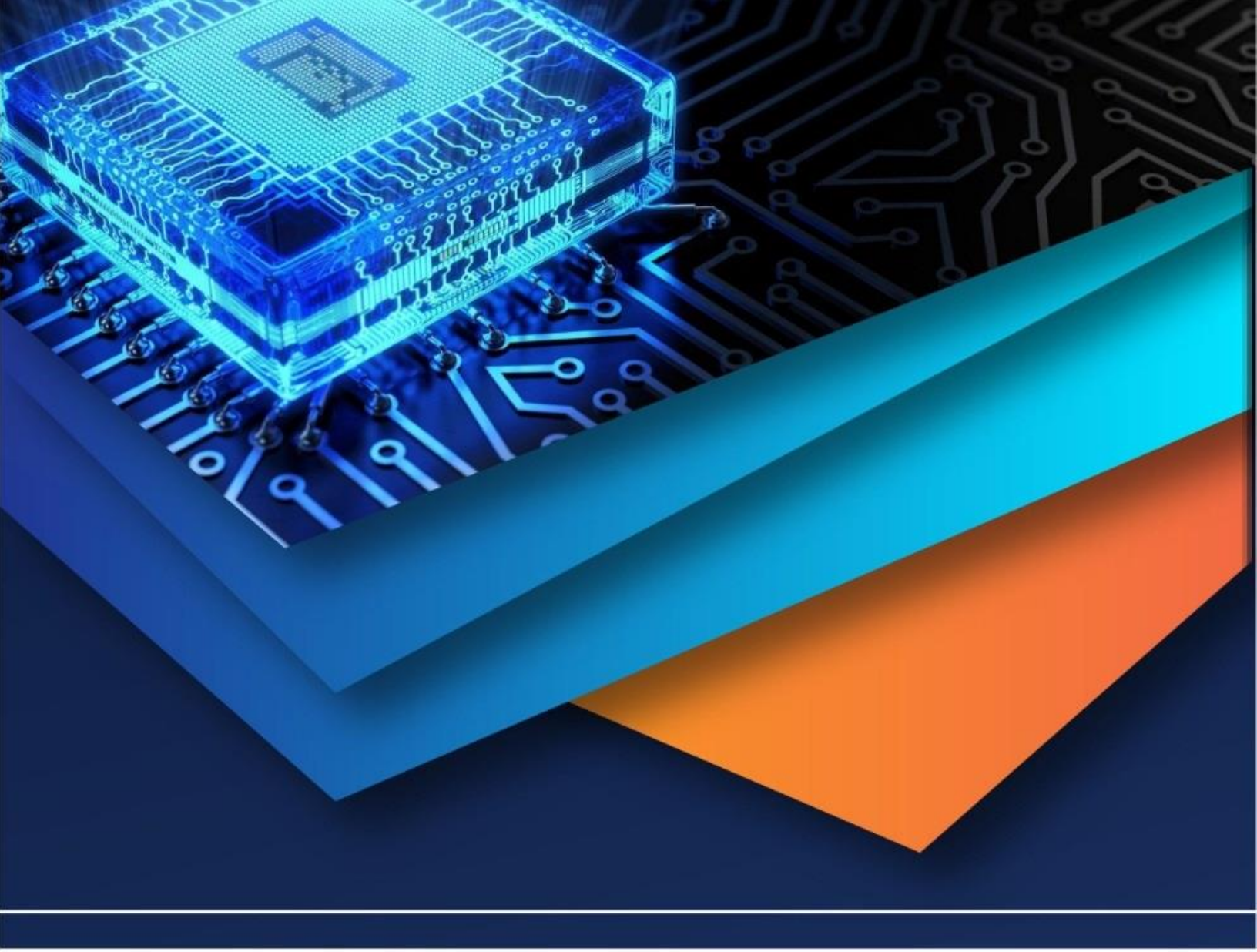
VI. CONCLUSION

User authentication in IoT is a critical component in ensuring the security and integrity of connected devices and networks. Due to the diverse nature and resource limitations of IoT devices, traditional authentication methods may not always be feasible. Implementing strong yet lightweight authentication techniques is essential to protect against unauthorized access and potential cyber threats. Solutions like biometric authentication, token-based methods, and device-to-device verification offer varying levels of security and adaptability, but each comes with its own set of challenges. As IoT continues to grow, adopting advanced and flexible authentication strategies will be crucial for creating safer and more resilient IoT ecosystems.

REFERENCES

[1] Zhigang Chen & Yuting Jiang (2023) A Survey on Zero-knowledge Authentication of things.
[2] Yan Chen & Shuiguang Deng (2021) A blockchain-Based Mutual Authentication Scheme for Collaborative Edge Computing.
[3] Junhui Zhao & Huanhua Hu (2024) Authentication technology in Internet of things and Privacy Security Issues in Typical Application Scenario.
[4] J. Mahesh , M. Bodisatwa & D. Somnath (2022) Biometric-based Secure Authentication for IoT Enabled Devices and Applications.
[5] Najila Al-Taleb & Rachid Zagrouba (2022) Authentication Scheme for IoT.

[6] Arwa Badhib & Amal Almrshed (2019) A Survey on Authentication Technique for the Internet of Things.
[7] Suraj Sharma & Abhishek Pandey (2017) Secure Authentication Protocol for IOT Architecture.
[8] Maha Saadeh & Azzam Sleit (2016) Authentication Techniques for the Inter-net of Things: A Surve
[9] King-Hang Wang & Chien-Ming Chen (2017) A secure Authentication scheme for Internet of Things



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY