# An Efficient Authentication Protocol for IoT Devices

**Ansari Maqsood Ahmed[1], Dr. Prasadu Peddi[2], Dr. Pathan Mohd. Shafi[3]**

*[1]Research Scholar, Shri JJT University, Jhunjhunu, Rajasthan*
*[2]Assistant Professor in the Dept. of Computer Science & Engineering, Shri JJT University Jhunjhunu Rajasthan*
*[3]Professor in MITSOE, MITADT University, Pune*

---

**Abstract -** *There is a requirement for individuals and organisations to interact over the Internet. In such cases, the user must go through the authentication procedure before being able to access the needed resource, information, or service. Kerberos is a well-known and reliable authentication mechanism that is supported by nearly every major operating system and network system.*

*We may include new authentication methods into Kerberos as they become available, as the extensibility aspect of Kerberos allows us to do so. However, due to the lack of source code for certain implementations and a lengthy standardisation process, expanding Kerberos is limited. Individuals are frequently required to work remotely [9].*

*Security is a very significant component in such an atmosphere. In this research, we offer a method for removing the majority of the most serious dangers associated with authentication over a public network. The main goal is to combine Kerberos with the public key system and location-based security. Kerberos enhancements are completed in three phases [28]. An Application Server is updated so that it may utilise the authentication service component, which contains a GPS parameter given by the user. Secure authentication employing public key security, single sign-on capability, dynamic authentication using physical location, and server auditability requirements are all part of the proposed solution [27].*

***Key Words***: Kerberos, Kerberos protocol, authentication method, big data security; public cloud; security threats; security vulnerabilities, Security in IOT devices; Lightweight algorithm, Security algorithm for IOT devices, dynamic authentication, server auditability

## 1. INTRODUCTION

For the security of computer systems, authentication is essential. It is difficult to judge whether an operation should be authorised without understanding of the principle seeking it. Traditional authentication mechanisms are ineffective in computer networks when attackers may intercept passwords by monitoring network traffic. It is critical to employ robust authentication techniques that do not reveal passwords. In such contexts, the Kerberos authentication system is ideally suited for user authentication. Kerberos is an authentication mechanism created at MIT (Massachusetts Institute of Technology). Section V compares the protocol to other current solutions and evaluates it in terms of computing time. The Kerberos protocol makes use of a trusted third party called the Key Distribution Centre (KDC) to negotiate shared session keys and mutual authentication between clients and services. Authentication is a critical component of fundamental security operations, and it is particularly important in the Internet of Things (IoT). Edge and fog computing have opened up new possibilities for IoT security and trust management [39].

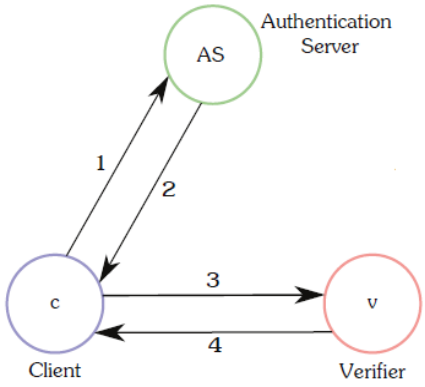


**Fig. 1.1** The basic Kerberos authentication protocol

Individuals and businesses both require and desire Internet communication. Before accessing the needed resource / information /service, the user must go through the authentication procedure. Kerberos is a well-known authentication system. It is desirable to include new authentication techniques into Kerberos as they become available. Extending Kerberos, on the other hand, is difficult due to a lack of source code for certain implementations and a protracted standardisation procedure. Employees working for numerous organisations, IT sectors, and support services now frequently use portable devices such as laptops. In many circumstances, they are required to work from home. Security is extremely important in such a setting. In this research, we present a method for removing the most serious risks associated with authentication and

authorisation over a public network. The main goal is to combine Kerberos with public key security and location-based security. Kerberos enhancements are completed in three phases. An Application Server has been upgraded to allow it to access the authorization service component and send it user-supplied GPS parameters [15].

Secure authentication employing public key security, single sign-on capability, and dynamic authorisation based on physical location, and server auditability requirements are all part of the proposed solution. Kerberos is included with all major computer operating systems and is well positioned to provide a universal solution to the problem of communicating parties' dispersed authentication and authorisation. Kerberos is unique among distributed security systems in that it may use a broad variety of security methods and processes. In recent years, Kerberos has progressed from a well-respected authentication standard to a key security infrastructure component; for example, Microsoft stated that Windows Primary Domain Controllers will support the protocol for authentication reasons [18].

Organizations, businesses, offices, and IT services all employ open and distributed architectures. Dedicated workstations and distributed or centralised servers are common components of such open & distributed settings. In an open environment, users must confirm their identification for each service they use, and servers must similarly prove their identity to clients. Authentication is the process of confirming a user's identity. Traditional Kerberos includes a centralised authentication server that authenticates users and servers. Kerberos may be enhanced or extended to make the authentication service more secure in open situations. To improve usability and performance, new authentication systems must integrate more readily into Kerberos without modifying the Kerberos fundamental security architecture [22].

In the age of IoT, resource-constrained devices face security and privacy issues. The concept of computer services that are available at any time, from any location, and on demand is characterised by seamless interactions across disparate Internet actors. This phenomena enables intelligent chips, sensors, or microcontrollers to be embedded into common things, allowing them to create, transmit, and exchange data. By connecting tiny, resource-constrained devices to the Internet, such computing speeds up technological progress, allowing new services to emerge that need smooth interactions and integrations with existing technologies, infrastructures, and services [45].

The Internet of Things (IoT) refers to the connection of tiny, common things and devices to the Internet, a phenomena that is expected to link billions of small, resource-constrained objects to the Internet in the near future. The heterogeneous mix of devices that were not previously linked, ranging from wireless sensors to smart home appliances and other gadgets, is likely to alter Internet technology and favourably influence our everyday lives by introducing new and tailored services [46].

To develop secure IoT, security must be by design, which means that security and privacy aspects must be thoroughly researched and analysed from the start of the development process to give the respective technologies a competitive advantage in the market, as security and privacy provided by ecosystem products are among the top concerns for end users. IoT devices are subject to security and privacy assaults, which are the consequence of ongoing pressure to get goods to market quickly and beat the competition, which reduces design time and costs. Finally, the items haven't been adequately examined and evaluated in order to uncover serious hazards specific to their working contexts. Various methods have been developed throughout the years to address security and privacy concerns in the realm of resource restricted devices. The creation of efficient and safe protocols for IoT devices with limited resources is a pressing requirement [44].

Even when the individual devices are physically hacked, our suggested method enforces parameter expiry, which is a key element in increasing the security of the IoT. As a result, our recommended solution is a token-based authentication mechanism that is comparable to Kerberos [17].

## 2. RELATED WORK

When methods based on public key encryption are used, authenticating mobile computing users can use a large amount of processing and communications resources. The user may experience unsatisfactory response times as a result of these resource needs [42]. By analysing the service time of a "skeleton" implementation and developing a closed queuing network model, the adaptations of the public key enabled Kerberos network authentication protocol to a mobile platform in this study. Between the client and the server, Kerberos adds a proxy server to minimise potential performance issues and provide functionality [21].

Kerberos authentication (RFC1510) should be enhanced to include public-key cryptography. Integrating public-key cryptography (PKC) into Kerberos is at the forefront of proposed improvements to the original Kerberos standard, alongside projects such as IPv6 compatibility and smart-card hardware authentication. The advantages of PKC will increase the Kerberos framework's scalability and security. Despite the fact that this upgrade has not yet finished the Internet Standards Process (RFC 2026), several firms have already included it in their products [29].

Data sharing across a public network necessitates, for the most part, a crucial security mechanism that allows both sender and receiver to mutually authenticate using distinct

identifying characteristics, with secret shared key computation playing a critical role. The author provides a cryptographic computation of the shared secret key, which enables mutual authentication and confidentiality services across unsecure public networks. The simulation result demonstrates that the protocol is feasible and provably safe when using the typical cryptographic assumptions. As a result, the proposed cryptographic system is incredibly simple, useful, and resistant to known threats [33].

Using elliptic curve cryptographic operations, the enhanced Kerberos authentication system for wireless communication. The proposed protocol provides the power of public key cryptography while adding just 68.7 milliseconds to regular Kerberos without employing pre-computation tables for a 160-bit curve and scalable architecture, compared to 57.3 milliseconds for the same key length using a bespoke curve library [10]. Using pre-computation tables, these times are reduced to 55.8 and 51.6 milliseconds, respectively. The proposed protocol uses less bandwidth than previous Kerberos alternatives that use public key cryptography. The results were achieved using a 206 MHz 32-bit StrongARM1 CPU. The Kerberos protocol, which is supported by ECC, might be an essential alternative among other user authentication protocols for wireless networks because of its bandwidth efficiency and quick execution speed [29].

Identity authentication and key negotiation security is a critical component of LAN (Wireless Local Area Network) security. Wireless Key Exchange (WKE), a novel authentication and key exchange mechanism for WLAN, is presented. At the same time, the BAN logic (a set of principles for constructing and analysing information exchange protocols) is utilised to define and establish WKE's security. Finally, we merge the WKE and Diffie-Hellman exchange in Mobile IP for WLAN key negotiation [12].

Kerberos is a well-known authentication protocol. It is desirable to include new authentication techniques into Kerberos as they become available. Extending Kerberos, on the other hand, is difficult due to a lack of source code for certain implementations and a protracted standardisation procedure. Extensible Pre-Authentication in Kerberos (EPAK) is a Kerberos extension that allows several authentication techniques to be loosely connected with Kerberos without requiring further Kerberos modifications [43].

Two authentication techniques for open systems that have been developed as Kerberos extensions using EPAK are shown to demonstrate the framework's usefulness. These additions demonstrate how EPAK adds flexibility to Kerberos while keeping backwards compatibility [4].

By implementing access control measures, secure environments safeguard their resources from illegal access. As a result, when it comes to strengthening security, text-based passwords are insufficient. It is necessary to have something that is both secure and user-friendly. Image Based Authentication (IBA) is useful in this situation. IBA wraps Kerberos Protocol and gives clients a totally unique and safe authentication mechanism to use [3].

Sensor nodes sense data, process it, communicate information, and collaborate with other sensor nodes and end users in centralised Wireless Sensor Network (WSN) applications in distributed Internet of Things (IoT) architecture. It is critical to build secure links for end-to-end communication with adequate authentication in order to ensure the trustworthiness and accessibility of dispersed IoT. By inventing a two-phase authentication protocol that allows sensor nodes and end-users to verify each other and begin secure connections, the authors propose an implicit certificate-based authentication method for WSNs in dispersed IoT applications [26].

In today's e-commerce applications, a single smart card can provide access to a variety of services in a multi-server communication environment. However, this sort of system has a significant security flaw in that the user constantly uses the same identity across several services, making the system open to a variety of assaults. To address the security issue, we propose a security token service for a safe multi-server authentication technique in a communication network utilising a single electronic identification card. Privacy, secrecy, and authentication are some of the security considerations that must be handled with cloud computing. The author proposes a safe authentication and key distribution technique. They picked the Kerberos 5 protocol, which is one of the most well-known authentication and key distribution systems, for this purpose. The use of biometric data provides a non-repudiation approach that can solve password-based authentication's limitations, such as users' proclivity to use an easy password [2].

## 3. PROPOSED SCHEME

In limited contexts, our suggested system extends the concepts of the standard Kerberos authentication protocol. We're curious about how the Kerberos authentication protocol uses context information, such as date and time, to ensure that authentication parameters are legitimate.

In effect, we steal several principles from Kerberos to improve the reliability and efficiency of our protocol in the IoT context.

Our proposed protocol uses authentication phase as shown in Figure 1.2

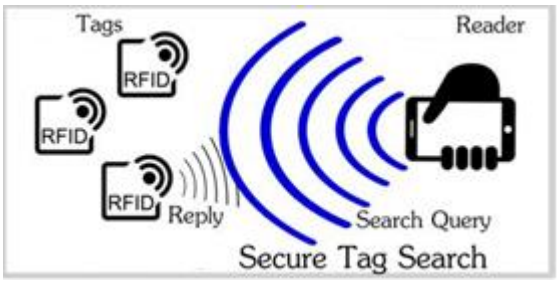


**Fig. 1.2** Authentication Phase

Reader Rj
The reader knows from phase A:
1) Authorized tag's list Lj = {(temp1j ;K1j ); (temp2j ;K2j ),….,(tempij ;Kij )},
2) Time window: WSj , and
3) Access rights: ARij received from the backend server
d01: Generate rj
d1 : WSj ;ARij ; rj
d2 : Hij ; ri
d11 : if (TZj > TSY S) & (TSY S > T0j )
{
d12 : K'ij = HMACidi (WSj || ARij ),
d13 : Generate ri,
d14 : Hij = HMACK'ij (ri || rj )
}
d21 : Search (∀ Kij ∈ Lj )
{
d22 : Calculate H'ij = HMACKij (ri || rj )
d23 : if (H'ij = Hij ) { # A Tag with valid Kij found in the list
d24 : Get system time tj
d25 : Calculate Vij = HMACKij (ri || tj )
d26 : KS = HMACKij (tj || ri || WSj )
d27 : if ( Kij ∈ Lj ) { # Tag not in the list
d28 : UNAUTHORIZED TAG; IGNORE
}
{
d29 : V'ij = HMACK'ij (ri || tj )
d30 : if (V'ij = Vij )
(Valid Vij authenticates reader)
Update TSYS = tj
d34 : KS = HMACK'ij (TSYS || ri || WSj )
}

**Fig. 1.3** Authentication Protocol for Very Constrained Devices

## 4. EVALUATION AND ANALYSIS

The comparison with other current methods demonstrates why our suggested model is not only difficult to break, but also increases cost efficiency, memory efficiency, and reduces compute stress [1], [5], [7], [41].

**Table -1:** Comparative table between existing and our proposed model

| Evaluation Criteria | Our Proposed Model | Existing Model |
|---|---|---|
| 1. Algorithms | Threshold | RSA |
| 2. Memory | Less | More |
| 3. Time | More execution time | Less execution time |
| 4. Security Level | More Secured | Less Secured |
| 5. Power Consumption | Less power consumption | More power consumption |
| 6. Structure | Better structure than RSA | Not better |
| 7. CPU Cycle | Needs less CPU cycles while processing | Needs more CPU cycles while processing |

Authentication is one of the most critical criterion for ensuring security. A weak authentication technique is used by a large number of apps.

Our architecture can manage safe authentication for a variety of additional apps from a central location. This model provides a dependable, straightforward, and simple-to-manage option for any application that requires this sort of service [37].

## 5. CONCLUSION

The Internet-of-Things (IoT) is still in its early stages. There are a number of intriguing outstanding challenges in the domain of privacy and security that need be thoroughly investigated in order to make authentication processes more efficient, useful, and safe for end users in the ubiquitous age. We will improve the suggested security protocol with methods to preserve user privacy in future work before doing extensive testing and review.

## REFERENCES

[1] "Publication Number : Title : Publication Date : NIST Interagency Report 8114 Report on Lightweight Cryptography March 2017 • Final Publication : https://doi.org/10.6028/NIST.IR.8114 ( which links to • Information on other NIST cybersecurity publications a," vol. 8114, no. March, 2017.
[2] D. A. F. Saraiva, V. R. Q. Leithardt, D. de Paula, A. S. Mendes, G. V. González, and P. Crocker, "PRISEC: Comparison of symmetric key algorithms for IoT devices," Sensors (Switzerland), vol. 19, no. 19, pp. 1–23, 2019, doi: 10.3390/s19194312.
[3] V. Vennela, "Lightweight Cryptography Algorithms for IOT Devices," Int. J. Res. Appl. Sci. Eng. Technol., vol. 9, no. VI, pp. 1678–1683, 2021, doi: 10.22214/ijraset.2021.35358.
[4] D. J. Rani and S. E. Roslin, "Light weight cryptographic algorithms for medical internet of things

(IoT) - A review," Proc. 2016 Online Int. Conf. Green Eng. Technol. IC-GET 2016, 2017, doi: 10.1109/GET.2016.7916703.
[5] V. K. Sarker, T. N. Gia, H. Tenhunen, and T. Westerlund, "Lightweight Security Algorithms for Resource-constrained IoT-based Sensor Nodes," IEEE Int. Conf. Commun., vol. 2020-June, 2020, doi: 10.1109/ICC40277.2020.9149359.
[6] M. Arogia Victor Paul, T. Anil Sagar, S. Venkatesan, and A. K. Gupta, "Impact of Mobility in IoT Devices for Healthcare," Lect. Notes Data Eng. Commun. Technol., vol. 21, pp. 243–261, 2019, doi: 10.1007/978-3-319-93940-7_11.
[7] T. Nandy et al., "Review on Security of Internet of Things Authentication Mechanism," IEEE Access, vol. 7, pp. 151054–151089, 2019, doi: 10.1109/ACCESS.2019.2947723.
[8] N. Samir et al., "ASIC and FPGA Comparative Study for IoT Lightweight Hardware Security Algorithms," J. Circuits, Syst. Comput., vol. 28, no. 12, 2019, doi: 10.1142/S0218126619300095.
[9] A. Pirzada and C. McDonald, "Kerberos assisted authentication in mobile ad-hoc networks," CRPIT '04 Proc. 27th Conf. Australas. Comput. Sci., pp. 41–46, 2004, [Online]. Available: http://dl.acm.org/citation.cfm?id=979928.
[10] A. Lohachab, "Journal of Information Security and Applications ECC based inter-device authentication and authorization scheme using MQTT for IoT networks," J. Inf. Secur. Appl., vol. 46, pp. 1–12, 2019, doi: 10.1016/j.jisa.2019.02.005.
[11] N. Saxena, B. J. Choi, R. Lu, and S. Member, "Authentication and Authorization Scheme for Various User-Roles and Devices in Smart Grid," vol. XX, no. X, 2015, doi: 10.1109/TIFS.2015.2512525.
[12] W. Lardier, Q. Varo, and J. Yan, "Dynamic Reduced-Round Cryptography for Energy-Efficient Wireless Communication of Smart IoT Devices," IEEE Int. Conf. Commun., vol. 2020-June, no. Section III, pp. 0–6, 2020, doi: 10.1109/ICC40277.2020.9149305.
[13] M. O. D. Evices, "a L Ightweight R Econfigurable S Ecurity M Echanism for J Alal a L -M Uhtadi , D Ennis M Ickunas , and R Oy C Ampbell ," Ieee Wirel. Commun., no. April, 2002.
[14] K. Chatterjee and A. De, "A Novel Multi-Server Authentication Scheme for e-commerce Applications Using Smart Card," Wirel. Pers. Commun., vol. 91, no. 1, pp. 293–312, 2016, doi: 10.1007/s11277-016-3462-y.
[15] D. Hu, "An Improved Kerberos Protocol Based on Fast RSA Algorithm."
[16] M. Schukat, P. C. Castilla, and H. Melvin, "Trust and trust models for the iot," Secur. Priv. Internet Things Model. Algorithms, Implementations, pp. 237–268, 2016, doi: 10.1201/b19516-18.
[17] P. L. Hellewell, T. W. Van Der Horst, and K. E. Seamons, "Extensible pre-authentication in kerberos," Proc. - Annu. Comput. Secur. Appl. Conf. ACSAC, pp. 201–210, 2007, doi: 10.1109/ACSAC.2007.33.
[18] Z. Hu, Y. Zhu, and L. Ma, "An improved Kerberos protocol based on Diffie-Hellman-DSA key exchange," IEEE Int. Conf. Networks, ICON, pp. 400–404, 2012, doi: 10.1109/ICON.2012.6506591.
[19] T. K. Goyal, V. Sahula, and D. Kumawat, "Energy Efficient Lightweight Cryptography Algorithms for IoT Devices," IETE J. Res., vol. 0, no. 0, pp. 1–14, 2019, doi: 10.1080/03772063.2019.1670103.
[20] M. Tahir, M. Sardaraz, S. Muhammad, and M. S. Khan, "A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics," Sustain., vol. 12, no. 17, 2020, doi: 10.3390/SU12176960.
[21] S. Kallam, "Diffe-Hellman: Key Exchange and public key cryptosystems," 2015.
[22] T. S. Algaradi and B. Rama, "Static knowledge-based authentication mechanism for hadoop distributed platform using kerberos," Int. J. Adv. Sci. Eng. Inf. Technol., vol. 9, no. 3, pp. 772–780, 2019, doi: 10.18517/ijaseit.9.3.5721.
[23] H. Kim and E. A. Lee, "Authentication and Authorization for the Internet of Things," IT Prof., vol. 19, no. 5, pp. 27–33, 2017, doi: 10.1109/MITP.2017.3680960.
[24] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity Establishment and Capability Based Access Control ( IECAC ) Scheme for Internet of Things," 2012.
[25] G. A. Lewis and D. Klinedinst, "Authentication and Authorization for IoT Devices in Disadvantaged Environments," pp. 368–373, 2019.
[26] W. Ren, "Lightweight and Robust Schemes for Privacy Protection in Key Personal IoT Applications : Mobile WBSN and Participatory Sensing," 2016.
[27] Z. Hu, Y. Zhu, and L. Ma, "An Improved Kerberos Protocol based on Diffie-Hellman-DSA Key Exchange," pp. 400–404, 2012.
[28] M. B. B. A. Malar and J. Prabhu, "Trust based authentication scheme ( tbas ) for cloud computing environment with Kerberos protocol using distributed controller and prevention attack," 2020, doi: 10.1108/IJPCC-03-2020-0009.
[29] O. M. Erdem, "High-speed ECC based Kerberos Authentication Protocol for Wireless Applications," GLOBECOM - IEEE Glob. Telecommun. Conf., vol. 3, pp. 1440–1444, 2003, doi: 10.1109/glocom.2003.1258476.
[30] B. Rudra and D. S. Prashanth, Models and Algorithms for Energy. Springer Singapore, 2019.
[31] M. A. Rashid and H. H. Pajooh, "A security framework for iot authentication and authorization based on blockchain technology," Proc. - 2019 18th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. IEEE Int. Conf. Big Data Sci. Eng. Trust. 2019, pp. 264–271, 2019, doi: 10.1109/TrustCom/BigDataSE.2019.00043.
[32] K. Length and K. Length, "With His (Presumably Secret) Private Key. 2)," pp. 30–34, 2002.
[33] M. Sri Lakshmi and V. Srikanth, "A study on light weight cryptography algorithms for data security in IOT,"

Int. J. Eng. Technol., vol. 7, pp. 887–890, 2018, doi: 10.14419/ijet.v7i2.7.11088.
[34] L. Wei, Y. Chen, Y. Zhang, L. Zhao, and L. Chen, "PSPL: A Generalized Model to Convert Existing Neighbor Discovery Algorithms to Highly Efficient Asymmetric Ones for Heterogeneous IoT Devices," IEEE Internet Things J., vol. 7, no. 8, pp. 7207–7219, 2020, doi: 10.1109/JIOT.2020.2984775.
[35] L. Ding, Z. Wang, X. Wang, and D. Wu, "Security information transmission algorithms for IoT based on cloud computing," Comput. Commun., vol. 155, no. March, pp. 32–39, 2020, doi: 10.1016/j.comcom.2020.03.010.
[36] J. Yang, "An improved scheme of single sign-on protocol based on dynamic double password," Proc. - 2009 Int. Conf. Environ. Sci. Inf. Appl. Technol. ESIAT 2009, vol. 3, pp. 572–574, 2009, doi: 10.1109/ESIAT.2009.508.
[37] C. Science, R. Kumar, C. Science, E. Vvce, and C. Science, "Comparative Study of Various Lightweight Between IoT and Cloud," no. Icces, pp. 589–593, 2020.
[38] S. Sridhar and S. Smys, "Intelligent Security Framework for IoT Devices," Int. Conf. Inven. Syst. Control Intell., pp. 1–5, 2017.
[39] A. Harbitter and D. A. Menascé, "The performance of public key-enabled Kerberos authentication in mobile computing applications," Proc. ACM Conf. Comput. Commun. Secur., pp. 78–85, 2001, doi: 10.1145/501993.501995.
[40] S. Zareen, "Artificial Intelligence / Machine Learning in IoT for Authentication and Authorization of Edge Devices," 2019 Int. Conf. Appl. Eng. Math., pp. 220–224.
[41] I. Bhardwaj, A. Kumar, and M. Bansal, "A review on lightweight cryptography algorithms for data security and authentication in IoTs," 4th IEEE Int. Conf. Signal Process. Comput. Control. ISPCC 2017, vol. 2017-Janua, pp. 504–509, 2017, doi: 10.1109/ISPCC.2017.8269731.
[42] Y. Y. Du, H. Y. Ning, P. Yang, and Y. X. Cui, "Improvement of kerberos protocol based on dynamic password and "one-time public key," 2014 10th Int. Conf. Nat. Comput. ICNC 2014, pp. 1020–1025, 2014, doi: 10.1109/ICNC.2014.6975980.
[43] M. Backes, I. Cervesato, A. D. Jaggard, A. Scedrov, and J. K. Tsay, "Cryptographically sound security proofs for basic and public-key Kerberos," Int. J. Inf. Secur., vol. 10, no. 2, pp. 107–134, 2011, doi: 10.1007/s10207-011-0125-6.
[44] T. H. Vo, W. Fuhrmann, and K. P. Fischer-Hellmann, "How to adapt authentication and authorization infrastructure of applications for the cloud," Proc. - 2017 IEEE 5th Int. Conf. Futur. Internet Things Cloud, FiCloud 2017, vol. 2017-Janua, pp. 54–61, 2017, doi: 10.1109/FiCloud.2017.14.
[45] V. K. Sarker, T. N. Gia, H. Tenhunen, and T. Westerlund, "Lightweight Security Algorithms for Resource-constrained IoT-based Sensor Nodes," IEEE Int. Conf. Commun., vol. 2020-June, 2020, doi: 10.1109/ICC40277.2020.9149359.
[46] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Two-phase authentication protocol for wireless sensor networks in distributed IoT applications," IEEE Wirel. Commun. Netw. Conf. WCNC, vol. 3, pp. 2728–2733, 2014, doi: 10.1109/WCNC.2014.6952860.

## BIOGRAPHIES

**Ansari Maqsood Ahmed** Research Scholar in Shri JJT University, Rajasthan. I have 21 years of experience in the field of Technical Education.

**Dr. Prasadu Peddi** having 4+ years of experience in IT industry and 8+ years of experience in Teaching. Reviewer for a web of science and springer series journal, Member in IEEE and International Association of Engineers Specialization.