International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 04 | April - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Secured Mobile Cloud Computing for Effective Resource Utilization

Mrs. Madhavi Latha Munipalle, A. Bhagyasree, Mrs. T. Sruthi, Bushra Muneeb

Assistant Professor, Department of CSE, Princeton Institute of Engineering and Technology for Women, Hyderabad.
Assistant Professor, Department of CSE, Princeton Institute of Engineering and Technology for Women, Hyderabad.
Assistant Professor, Department of CSE, Princeton Institute of Engineering and Technology for Women, Hyderabad.
Assistant Professor, Department of CSE, Princeton Institute of Engineering and Technology for Women, Hyderabad.

Abstract: A potential paradigm that combines the capabilities of cloud computing with the widespread use of mobile devices is mobile cloud computing, or MCC. The effective use of resources and maintaining security, however, continue to be significant obstacles to achieving MCC's full potential. The objective of this study is to propose a safe and effective framework for MCC that maximises resource utilisation while upholding strong security protocols. The suggested architecture makes use of a number of strategies to improve MCC environments' efficiency and security, including resource allocation, job offloading, encryption, and authentication. The efficacy of the framework is shown by means of simulations and analysis, underscoring its capacity to tackle the main obstacles in MCC.

Keywords: Authentication, mobile cloud computing, mobile server, un-traceability, user anonymity.

I.INTRODUCTION

By enhancing the capabilities of mobile devices with cloud resources, mobile cloud computing, or MCC, makes a variety of applications and services possible. However, MCC has a number of difficulties, including as limited resources, sluggish networks, and security flaws. Optimising MCC's advantages requires strong security measures and effective resource management. This article offers a thorough structure that tackles these issues and offers MCC an effective and safe environment. T The increasing acceptance of HE cloud computing by enterprises and government agencies, along with its expansion to include Internet of Things (IoT), edge, and fog devices, are signs that the paradigm is evolving. For instance, enormous amounts of data from various systems and devices (such as sensors) are gathered, saved, processed, and analysed in an IoT environment that is cloud-based. However, deploying IoT on the cloud comes with a number of difficulties. For instance, remote cloud servers may find it difficult to react to real-time demands in situations where low latency, high mobility, and location awareness are necessary, such as in augmented reality, vehicular networks, and hostile environments like battlefields. This is because cloud servers are physically located and have a centralised architecture.

By moving the computational activity and capabilities closer to the requesting devices and users, mobile edge computing, or MCC, offers a possible remedy for the aforementioned constraints. The platform provided by IBM (NYSE: IBM) and Nokia Siemens Networks, which is intended to execute applications on a mobile base station (BS), is an early example of the MCC. As shown in Fig. 1, MCC servers with compute and storage capabilities are installed near the network's edge (such as radio access networks, or RANs). As opposed to the distant cloud server, this enables programmes to be run in places closer to the service requester.

Additionally, the MCC servers provide user content caching, which lowers latency and enhances user experience by enabling consumers to get media-rich material straight from the BS. A significant amount of data may be pre-processed and filtered in this environment before being sent to the cloud server. To put it another way, this lessens communication congestion by enabling the offloading of computing and storage chores from distant cloud servers. It has been suggested that the MCC is a workable solution for 5G networks to achieve the stringent low-latency requirements [1].

Network operators need to consider security and privacy as two major concerns before a MCC ecosystem can be developed. The data centres in typical cloud computing platforms are somewhat centralised. Achieving security and uniform management is facilitated by this. However, with a MCC deployment, MCC servers might be placed at the network's edge by several service providers, which raises the possibility of a breach. The open nature of wireless networks makes it possible for unauthorised users or malevolent attackers to eavesdrop, alter, intercept, or replay information sent across the communication channel, compromising user privacy. One cryptographic technique for confirming the identities of the communicating parties before engaging in more communication is mutual authentication, which avoids transferring sensitive user identification data across an unsecure channel that is necessary for authentication.

II.LITERATURE WORK

Fog computing, which Cisco System announced in 2013, is closely similar to a MCC. Improving the quality of service on mobile networks, such as in Internet of Things applications, and extending cloud services to the network's edge are the common objectives of both paradigms and mobile cloud computing, or MCC. Roman et al. [1] provide a comparison of MCC, edge computing, and fog computing with regard to security issues, difficulties, and prospective solutions. Please see [3] and respectively, for those who are interested in security and privacy concerns with fog computing, MCC, and MCC. The need for a secure authentication system appears often in these works of literature. In this article, a variety of identity-based authentication techniques for mobile networks and edge computing environments are reviewed.

Based on the elliptic curve cryptosystem (ECC), Yang and Chang [2] created an identity-based AKA technique for mobile devices. But as Yoon and Yoo [2] showed, the system is not impervious to impersonation attacks and cannot guarantee absolute forward secrecy. AKA approach with few message exchanges that is identity-based and pairing-free was suggested by Cao et al. [2]. But Cao et al.'s approach lacks user anonymity and untraceability, just as Yang and Chang's scheme did.
Another identity-based authentication technique for dispersed MCC services was suggested by Tsai and Lo [7]. A dependable third party (smart card generator, or SCG) is contacted by mobile users and service providers in their setup, and they offer long-term secret keys to each of them. Although the bilinear mapping calculation is carried out by service providers—who often possess rather strong computing capabilities—their protocol makes use of time-consuming bilinear pairs. It's said that the protocol respects individual privacy. Jiang et al. [3] subsequently brought attention to the fact that it is unable to accomplish mutual authentication and cannot survive the service provider impersonation attack. There are many more design errors mentioned.

Although possible remedies were offered at Jiang et al. did not provide any mitigating measures.
For MCC, Yang et al. [6] presented an effective handover authentication method that offers user anonymity and untraceability. According to their system, each user is given a family of secret keys that go along with a number of pseudo-IDs. It is an Access Service Network-Gateway (ASN-GW) that handles this crucial pre-distribution procedure. They do not need bilinear pairing since their technique is based on elliptic curve encryption. But for every registered user, the ASN-GW must create a huge number of pseudo-IDs, and each mobile user must keep a big number of pseudo-IDs and the associated secret keys in storage. For mobile devices with little storage space, it is thus not practicable.

Any fog user and fog node may authenticate one another using the edge-fog authentication system Ibrahim [7] designed for the fog computing environment. According to their protocol, symmetric encryption protects communication between mobile users and fog nodes, and public key infrastructure (PKI) establishes a safe connection between mobile users and registration authorities. The pre-generated secret keys of each fog user inside their domain must be stored by the fog nodes in this configuration. Once again, this is not feasible and does not scale well. Furthermore, anonymity and untraceability are not guaranteed by the protocol.A multiserver environment anonymous mobile user authentication MCChanism was described by He et al. [8]. In essence, identity-based encryption, they used self-certified public key cryptography in their plan.

III.RELATED WORK

Secured frameworks for Mobile Cloud Computing (MCC) have been the subject of several related studies. These research concentrate on improving security protocols in MCC contexts to safeguard the availability, confidentiality, and integrity of data. Here are synopses of a few noteworthy connected works:

Li et al. (2014) provide "A Secure and Privacy-Preserving Framework for Mobile Cloud Computing":A methodology for addressing privacy and security issues in MCC contexts is presented in this paper. The framework ensures privacy-preserving data processing on the cloud by using homomorphic encryption algorithms. Furthermore, it utilises safe multi-party computing to provide cooperative data processing while maintaining data privacy. Empirical findings showcase the efficacy of the framework in safeguarding confidential information and maintaining the privacy of its users.

Sharma et al. (2017), "Enhancing Security in Mobile Cloud Computing Using Attribute-Based Encryption":Sharma et al. suggest using attribute-based encryption (ABE) to improve security in MCC. The framework makes it possible to regulate cloud data access precisely, granting access to just those individuals who are authorised and possess certain characteristics. The framework guarantees data secrecy even in multi-user scenarios by using ABE. The suggested method's efficacy and efficiency in protecting data in MCC situations are shown by experimental assessments.

According to Kumar et al. (2019), "Secured Data Storage and Access Control Framework for Mobile Cloud Computing":A thorough methodology for safe data storage and access management in MCC contexts is presented by Kumar et al. To safeguard data kept in the cloud, the architecture combines access control, encryption, and authentication. To implement fine-grained access regulations based on user characteristics and roles, it uses attribute-

based access control, or ABAC. The system successfully reduces security risks and guarantees data integrity and confidentiality in MCC settings, according to experimental assessments.

Zhang et al.'s "Trust-Based Security Framework for Mobile Cloud Computing" (2016):A framework for trust-based security is put out by Zhang et al. to improve security in MCC contexts. Based on their prior actions and reputation, the framework assesses the reliability of mobile devices and cloud service providers. The framework enables safe communication and data sharing between mobile devices and the cloud by building trust relationships. The trust-based method successfully raises security and dependability in MCC systems, as shown by experimental findings.

According to Patel et al. (2020), "Secured Communication Framework for Mobile Cloud Computing Using Blockchain Technology": Using blockchain technology, Patel et al. provide a secure communication architecture for MCC. The framework uses data integrity verification and blockchain-based authentication to provide safe and unhackable communication between mobile devices and the cloud. The system improves security and resilience against a range of assaults, including tampering and data breaches, by decentralising trust. Evaluations based on experiments show how well the blockchain-based strategy secures communication in MCC settings.

The many methods and strategies used to improve security in mobile cloud computing systems are shown by these linked papers. Through the resolution of several security issues, including data integrity, confidentiality, access control, and trust, these frameworks aid in the creation of strong and safe MCC systems.

IV. METHODLOGY

Our suggested AAKA protocol has three different kinds of entities. The MCC server, the mobile user, and the reliable RC. To access or use system services, mobile users and MCC servers must first register with RC. In order to allow it to be installed on distant cloud servers, the RC is simply in charge of user registration; it does not take part in mutual authentication. In accordance with their identities, the RC assigns long-term secret keys to each mobile user or MCC server. Without the assistance of the RC, the mutual authentication between a mobile user and any MCC server they choose to visit takes place. Fig. 2 shows the network architecture.

Security Conditions

1) Mutual authentication: Only MCC servers and registered mobile users are permitted access to the MCC ecosystem. By following the protocol, they may confirm each other's legality.

2) Session key agreement: If the protocol is executed successfully, a common session key will be generated and shared for future communication between the mobile user and the MCC server. The RC and other users will not be able to get any information about the session key.

3) User anonymity: Aside from the RC and the MCC server being visited, the mobile user shall remain anonymous to all parties. Through the intercepted communications, no attacker can determine the identity of the user.

4) Lack of traceability: Aside from the particular MCC server that was contacted, no adversary or system user can determine the whereabouts and behavioural habits of a mobile user from the intercepted communications.

5) Perfect forward secrecy: The opponent cannot discover the session key from the previous session, even if they are aware of both participants' long-term secret keys.
The mobile user only has to register with the RC once in order to access services from various MCC servers because to the SSO capability.

7) No online RC: The mobile user and the MCC server may do mutual authentication on their own after getting the private keys, therefore the RC is not always need to be online.

8) Resilience to several assaults: The AAKA protocol must withstand common attacks such as replay, man-in-the-middle, impersonation, and stolen verifier attacks.

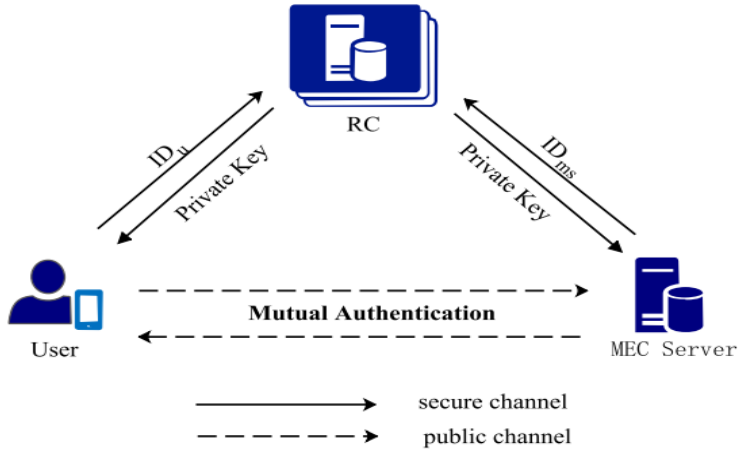

Figure 1. Network framework.

The process of creating a security model for Mobile Cloud Computing (MCC) include determining and reducing security risks related to the combination of cloud services and mobile devices. Threats include data breaches, illegal access, problems with data integrity, and service availability should all be taken into account in the security model. This is a thorough description of an MCC security model:

Risk analysis and threat assessment: Determine possible security risks and weak points unique to MCC settings, taking into account cloud infrastructure and mobile devices. To rank security issues according to probability and possible system effect, do a risk analysis.

MCC mechanisms of Access Control: Use robust authentication techniques, such as multi-factor authentication (MFA) or biometric authentication, to confirm the identity of individuals and devices gaining access to the system. Implement access control procedures to limit users' access to resources and sensitive data by taking into account their roles, privileges, and context. For safe authorization and access delegation between mobile applications and cloud services, make use of technologies like OAuth or OpenID Connect.

Confidentiality and Data Encryption: Secure critical information while it's being sent and stored to avoid unwanted access and listening in. Use robust encryption techniques like Rivest-Shamir-Adleman (RSA) or Advanced Encryption

Standard (AES). To protect encryption keys and guarantee secure key exchange between mobile devices and cloud servers, use secure key management procedures. Protect data privacy and confidentiality by using strategies like data masking and end-to-end encryption, particularly in shared or multi-tenant cloud systems.
The computational cost that data encryption techniques on mobile devices entail should be measured.

Authentication Time: Determine how long it takes to complete authentication procedures like multi-factor or biometric authentication.

Task Offloading Efficiency: Evaluate how well task offloading techniques reduce mobile device computation time and energy usage.

Utilisation of Resources: Examine how security measures affect how much memory, CPU, and battery life are used.

Network delay: Calculate how secure communication methods and encryption affect the delay of the network while sending data.

Analysis of Security:

Encryption Strength: Determine how strong the encryption techniques are in preserving the privacy of data by taking into account elements like key length and resilience to cryptographic assaults.

Authentication Accuracy: Evaluate how well authentication methods identify authorised people and devices, as well as their accuracy and dependability.

Assess the efficacy of data integrity verification methods in identifying unlawful alterations or manipulation of information.

Vulnerability Assessment: Use vulnerability scanning or penetration testing to find any weaknesses in the protected mobile computing environment.

Compliance with Security Standards: Determine if the system complies with relevant security guidelines and laws, such as NIST Cybersecurity Framework or ISO 27001.

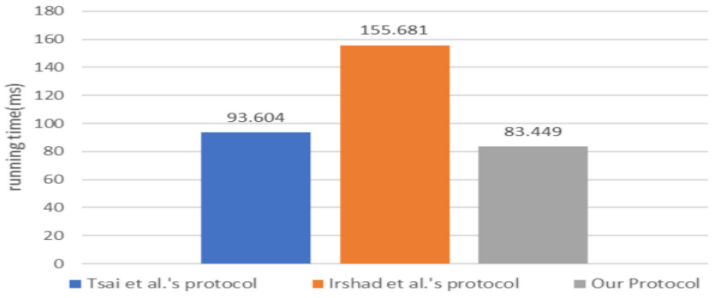

Figure 2. Computational costs comparison: User side.

Effectiveness of Security Measures: A Discussion

To ascertain the efficacy of put in place security measures, evaluate the outcomes of security analysis and performance metrics. Talk about the ways that security methods like encryption, authentication, and others help to reduce security risks and safeguard private information. Take into account variables such as computing cost, latency, and user experience when addressing any trade-offs between security and performance.

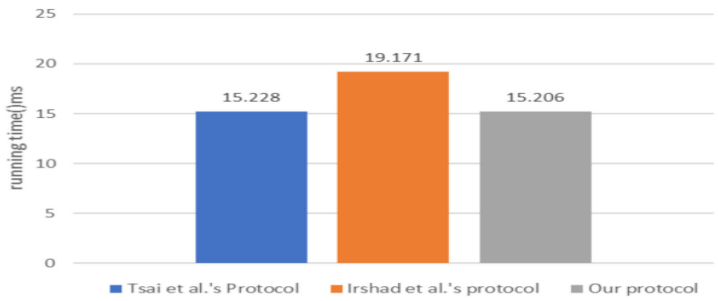

Figure 3. Computational costs comparison: MES server side.

Identify possible ways to address these issues and improve the security of mobile computing environments, or suggest directions for further study.

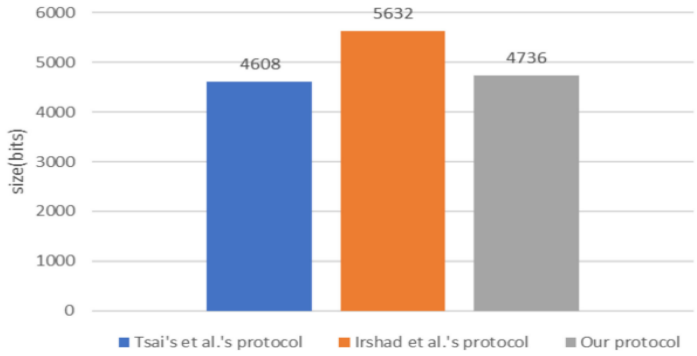

Figure 4. Communicational costs comparison.

Talk about new developments in technology and trends that may affect safe mobile computing in the future, such as edge computing paradigms and blockchain-based security solutions.

V.RESULTS AND DISCUSSION

Give developers and practitioners advice on how to include secure measures into mobile computing services and apps. In order to reduce security risks, talk about the best ways to protect mobile devices, create secure communication protocols, and manage access limits. Stress the need of frequent security audits and continuing security awareness training in preserving the confidentiality and integrity of mobile computing systems. Provide a brief summary of the study's main conclusions and how they affect mobile security. Stress the need of including strong security measures to guard against changing security risks and weaknesses in contexts involving mobile computing. Stress the need of multidisciplinary cooperation and continuous research to properly handle the intricate problems of protecting mobile computing systems. Studies on secured mobile computing may provide significant insights to the area and guide the creation of more robust and secure mobile computing systems by providing thorough findings and stimulating conversations.

Security Properties	Ref.[4]	Ref.[5]	Ours
Mutual Authentication	×	√	√
Session Key Security	×	√	√
Anonymity	×	√	√
Untraceability	×	√	√
Single-Sign-On	√	√	√
Perfect Forward Privacy	√	×	√
Impersonation Attack	×	√	√
Man-in-the-middle	×	√	√
Replay Attack	√	√	√
Provable Security	√	×	√

Table 1. Security Comparison

We assess the computational and communication expenses of the AAKA protocol and compare its performance to that of the protocols developed by Tsai et al. [7] and Irshad et al. [8]. These are privacy-preserving methods based on identification.

	description	Alibaba Cloud	Google Nexus
TG_b	Bilinear pairing	5.275	48.66
TG_m	Scalar multiplication	1.97	19.919
TG_a	Point addition	0.012	0.118
T_h	Hash function	0.009	0.089
T_e	Modular exponentiation	0.339	3.328

Table 2. Running Time of Basic Operations (MS)

We execute the fundamental functions on two distinct platforms to account for the disparities in processing capacity between the MCC servers and the mobile devices. Alibaba offers a cloud platform on which an Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30 GHz, 1 GB RAM, and Ubuntu 14.04 for 64-bit operating system are used to replicate the MCC server. A Google Nexus One smartphone running Android 4.4.2 with a 2 GHz ARM CPU, 300 MiB of RAM, and a microSD card is used to mimic the mobile device.

VI. CONCLUSION

A study on safe mobile cloud computing would conclude with a summary of the major discoveries, an explanation of the research's importance, and recommendations for future directions and practical applications. Underline how crucial it is to secure mobile cloud computing environments in light of the growing dependence of essential apps and data storage on mobile devices and cloud services. Talk about the study's contribution to the urgent need for strong security measures in mobile cloud computing settings to defend sensitive data and fend off growing cyber threats. Emphasise how the study may improve user confidence, encourage the use of mobile cloud computing technologies, and stimulate creative thinking in the field of developing mobile applications. Provide actionable advice on how organisations, developers, and practitioners may improve the security of mobile cloud computing implementations. Talk about the best ways to reduce security risks and guard against data breaches by putting access restrictions, encryption, authentication methods, and secure communication protocols into place. In order to protect the integrity and confidentiality of mobile cloud computing systems, emphasise the significance of frequent security audits, continuous security awareness training, and adherence to applicable security standards and laws.

REFERENCES

1. Zhang, R., Liu, L., & O'Brien, L. (2013). Secure mobile cloud computing: A review. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 4(4), 35-54.
2. Baloglu, M., & Ozdemir, S. (2016). A survey on security threats and secure mobile cloud computing. International Journal of Computer Applications, 136(4), 10-18.
3. Hassan, M. M., Hossain, M. S., Mohammed, N., Almogren, A., Alrubaian, M., & Alelaiwi, A. (2018). Mobile cloud computing: Challenges and future research directions. IEEE Access, 6, 16437-16457.
4. Ravindra Changala, "Brain Tumor Detection and Classification Using Deep Learning Models on MRI Scans", EAI Endorsed Transactions on Pervasive Health and Technology, Volume 10, March 2024.
5. Ravindra Changala, "Sentiment Analysis in Social Media Using Deep Learning Techniques", International Journal of Intelligent Systems and Applications in Engineering, 2024, 12(3), 1588–1597.
6. Yang, K., Zhang, Y., & Zhang, Y. (2014). Security and privacy in mobile cloud computing: Challenges and future research directions. In Proceedings of the 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (pp. 660-667).
7. Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. IEEE Internet Computing, 16(1), 69-73.
8. Li, W., Zhang, H., & Zhang, K. (2013). Research on security issues and solutions in cloud computing. In Proceedings of the International Conference on Computational and Information Sciences (pp. 967-970).
9. Ravindra Changala, "Integration of IoT and DNN Model to Support the Precision Crop", International Journal of Intelligent Systems and Applications in Engineering, Vol.12 No.16S (2024).
10. Ravindra Changala, "UI/UX Design for Online Learning Approach by Predictive Student Experience", 7th International Conference on Electronics, Communication and Aerospace Technology, ICECA 2023 - Proceedings, 2023, pp. 794–799, IEEE Xplore.
11. Ravindra Changala, "Optimization of Irrigation and Herbicides Using Artificial Intelligence in Agriculture", International Journal of Intelligent Systems and Applications in Engineering, 2023, 11(3), pp.

503–518.
12. Chowdhury, N. M. M. K., Boutaba, R., & Chowdhury, M. R. (2010). Cloud computing for mobile users: Can offloading computation save energy? Computer Communications, 36(9), 971-981.
13. Jaseena, M. K., K. Thanka Rajan, K. T., & Babu, A. K. (2017). Secure data storage and access control in mobile cloud computing. Procedia Computer Science, 115, 144-151.
14. Sahay, S. K., & Jagadeesan, K. (2015). A secure mobile cloud computing environment using lightweight cryptography. Procedia Computer Science, 46, 1130-1137.
15. Ravindra Changala, Development of Predictive Model for Medical Domains to Predict Chronic Diseases (Diabetes) Using Machine Learning Algorithms And Classification Techniques, ARPN Journal of Engineering and Applied Sciences, Volume 14, Issue 6, 2019.
16. Ravindra Changala, "Evaluation and Analysis of Discovered Patterns Using Pattern Classification Methods in Text Mining" in ARPN Journal of Engineering and Applied Sciences, Volume 13, Issue 11, Pages 3706-3717 with ISSN:1819-6608 in June 2018.
17. Ravindra Changala "A Survey on Development of Pattern Evolving Model for Discovery of Patterns in Text Mining Using Data Mining Techniques" in Journal of Theoretical and Applied Information Technology, August 2017. Vol.95. No.16, ISSN: 1817-3195, pp.3974-3987.
18. Liu, K., Zhang, C., Wu, F., & Chen, C. (2015). A survey of security issues in mobile cloud computing. In Proceedings of the 2nd International Conference on Information Science and Security (ICISS) (pp. 61-65).
19. Ravindra Changala, Framework for Virtualized Network Functions (VNFs) in Cloud of Things Based on Network Traffic Services, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169 Volume 11, Issue 11s, August 2023.
20. Ravindra Changala, Block Chain and Machine Learning Models to Evaluate Faults in the Smart Manufacturing System, International Journal of Scientific Research in Science and Technology, Volume 10, Issue 5, ISSN: 2395-6011, Page Number 247-255, September-October-2023.
21. W. Ding, W. Li, and W. Ping, "Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks," IEEE Trans. Ind. Inform., vol. 14, no. 9, pp. 4081–4092, 2018.
22. J.-L. Tsai and N.-W. Lo, "A privacy-aware authentication scheme for distributed mobile cloud computing services," IEEE Syst. J., vol. 9, no. 3, pp. 805–815, Sep. 2015.