ISSN No:-2456-2165

Advanced System to Identify Users and Devices in IoT using Token-Based Authentication

B. Bamleshwar Rao
Research Scholar
AKS University, Satna, M.P., India

Dr. Akhilesh A. Waoo
Associate Professor
AKS University, Satna, M.P., India

Abstract:- A billion networked gadgets with sensors and communication devices make up the Internet of Things (IoT). Making IoT a smart terminal is a hot topic right now. By linking cloud services, gadgets can receive more precise information for daily use. It is difficult to verify and authorise billions of smart terminal devices using RESTful APIs, which access cloud services. Privacy and security issues arise from personal use of smart terminal devices. This article introduces a token-based authorization mechanism. The token provides a secure way for devices to access cloud resources. As a result of the high level of privacy, sensitive data are not easily disclosed by a third-party authentication centre. It also expires after a certain time or when the token count surpasses a certain threshold, reducing the chance of devices being compromised. In this article, we offer a framework for medical wearables. In the experimental research study, the advantages of this framework are explained. Keywords; Internet of things, Authentication System, WSN.

I. INTRODUCTION

The Internet of Things Wide Area Network (IoT WSN) has opened up numerous opportunities in a variety of fields, including healthcare, shipping, warehousing, and logistics, which have streamlined procedures for both consumers and enterprises. This extensive and quick development has resulted in the emergence of significant issues, which necessitate the development of high-security protocols for Internet of Things applications in order to protect the sensitive information of users. Security is now the most significant concern facing the Internet of Things WSN environment. Remote users can obtain data from IoT sensor nodes through the Internet when they are connected to an IoT WSN. For the first time, researchers have created practical procedures for integrating wireless networks into Internet of things environments. Sensor nodes are naturally resource-constrained devices in terms of processing capability, communication bandwidth, and storage capacity due to their small physical size and limited energy [1]. This is due to their small physical size and limited energy. As a result, developing a safe and efficient remote user authentication mechanism for Internet of Things WSN contexts is a difficult task. In Internet of Things environments, the security efficiency of remote user authentication is a critical consideration when it comes to delivering information securely [2]. Additionally, due to the limited energy availability of WSN resources, energy consumption, as well as computational and communication efficiency, are critical considerations. Additionally, because of the limited resources of the sensors, adding resourceful gateway nodes can assist [3] the sensors, can offer speedy on-demand delivery of information, and can handle the majority of the processing. When it comes to Internet of Things security, user or device authentication is a significant issue that must be taken into consideration.

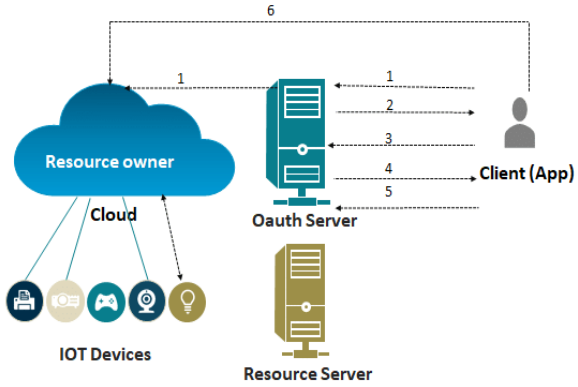

Fig. 1:Basic authentication system [7]

The majority of traditional authentication systems are based on a password, a smart card, or a combination of the two methods. At the moment, these protocols are ineffectual due to the fact that attackers have changed the approach of their attacks on Internet of Things devices. With the rise of biometric-based approaches that are difficult to replicate, such as those involving fingerprints, iris scanning, and facial patterns, the need for biometric-based approaches that are difficult to replicate has emerged as an additional factor that can improve the security of Internet-based applications.

II. RELATED WORK

The concept of security is not only vital, but it is also required for the successful implementation of a digital solution. For the time being, there is no definitive definition for strong authentication. Strong authentication is a method of increasing the level of security while still attempting to meet security requirements. [4] Security is not only crucial while purchasing, exchanging, or selling things or services; it is also critical when maintaining the integrity of information and systems. [5] Creating networks and communicating between PCs, servers, application software and mobile phones is also critical. Identification and authorization are two of the most important requirements for security [6]. In order to establish trust and verify user validity, most systems now rely on "static passwords." [7] The user selects a password that is simple to guess and remember, contains relevant information, or is used throughout the authentication procedure. Some users generate passwords based on what they are thinking about at the time. Strong passwords are difficult to remember and require a significant amount of time to manage. People like

ISSN No:-2456-2165

to keep their passwords in a journal or use a common password for everything; both of these practises are vulnerable to password leek. Weak authentication schemes can lead to access level vulnerabilities that can be exploited, making them liable for information leakage. Attack methods are also often specific to the targeted programme or system, although common tactics can be employed. In order to steal passwords, an attacker can use a variety of techniques such as spoofing, surfing, eavesdropping, brute forcing, prediction, profile research, and many others. These findings [8] lead to the conclusion that work necessitates an interactive security approach that should be unique for each identity. Token-based authentication is a system that requires the user to engage with the hardware in order for the authentication process to be completed. Most of the time [10], this hardware consists of software that is used to generate passwords and that is synced with the server application. When a user requests digital identification, the token utilises the password that is presented on the token. The introduction of a time stamp in a security token allowed for the integration of password variation and password updates over time.

III. PROPOSED METHODOLOGY

Authentication for mobile phones is discussed in this work, and we suggest a universal authentication architecture. It is necessary to have strong authentication procedures in place before using a mobile token as a security token. These represent an attempt to reduce the cost and effort associated with strong authentication through the use of security token services. The following mechanism can be implemented [11] using the proposed system. SMS-based Dynamic Password: This is a password that is generated by SMS. In this strategy, the user sends the server his or her user id and four-digit static passwords in order to get the dynamic password. The server validates the request in terms of user information and passes it on to the password algorithm for the development of a dynamic password. Password algorithm generates a unique dynamic password for each individual user with the assistance of a static password. Following that, the system stores it in the VPR together with the user id for the current session and delivers it to the user by SMS. To obtain access to the programme, the user must now submit this dynamic password along with their user id. The system compares the requested password with the previously saved one and redirects the user to the main application access. Replay attacks are possible because VPR stores dynamic passwords for verification, making it open to such attacks. To get around this, we set a session time for each entry. However, because VPR updates every minute, we decided to set a session time for each entry [12]. The VPR session timeout is three minutes, and the system runs an updating service on a minutely basis, which deletes any obsolete values from the VPR. In layman's terms, the whole lifespan of a dynamic password is three minutes. SIM Based Authentication: This is a technique in which both the request for a dynamic password and the response are sent over SMS. The IMSI number, which is unique to each mobile phone and is used to identify the device, is used in this suggested approach to identify the device.

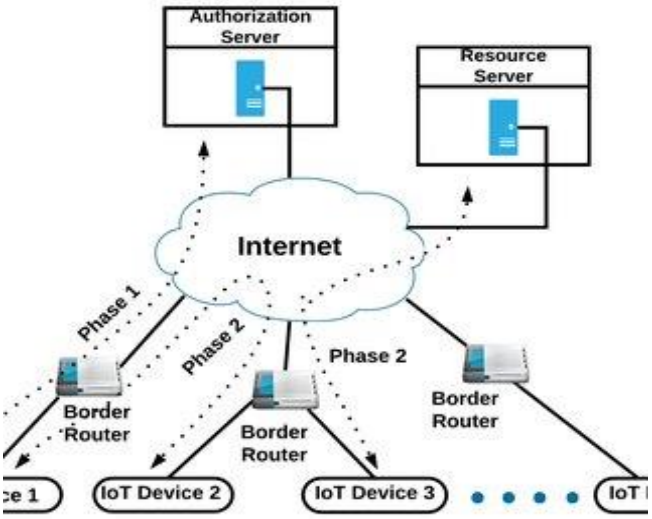

Figure 2; Advanced authentication scheme [10]

The IMSI number is recorded on the SIM card, which is then placed into the mobile phone. This number is likewise saved in the server database together with the user's information. Access to the programme is gained by sending four-digit static passwords along with a registered SIM card to the application server through text message. Following that, the server determines its IMSI number and retrieves a static password from its containment. At this point, the server identifies the presence of an IMSI number in the user's data and passes the static password along to the password algorithm. Following that, the password algorithm returns a dynamic password of 24 bits to the application server, which stores it in the VPR and sends it to the desired SIM via text message. Now, the user must provide a user id and a dynamic password in order to obtain access to the programme. The second way is more secure and authentic [13] than the first since it verifies the required SIM identifier in conjunction with a static password, whereas the first approach does not. However, because the application server must additionally detect the IMSI number and read the requested number, the implementation cost and complexity of this approach are increased as a result.

- The user is the most important part; he or she wishes to gain access to an application and establish a connection with an application or node using any network technology.
- The proposed algorithm design for generating dynamic passwords for each digital identification procedure is referred to as the password algorithm.
- The GSM server or SMS gateway assists in the generation of SMS messages that are used to send dynamic passwords to the user.

It is a temporary register that is used to hold the username and dynamic password for the current session in which it is being utilised [14].

The security architecture for strong authentication is depicted in Figure 1.

In this paper, we provide an overview of token-based strong authentication and discuss its applications. The

following is the sequence of events that takes place during strong authentication:

- The user submits a URL request to the application server, which sends the user's general identification (i.e., user id and static password) to the server.
- The application server will search for the existence of the user in the database and determine whether or not the user has authorisation.
- After that, it transmits the password request as well as the static password to the password algorithm, which then generates a dynamic password for the specific user. The technique generates a 24 bit (8-digit) dynamic password for digital identification by taking the seed value, the timestamp, the date, and the static password into consideration.
- At this point, the application will save the dynamic password in the Virtual Private Registry.
- 5 Afterwards, the server transmits a dynamic password to the user over a GSM modem or SMS gateway.
- Following that, the user obtains the dynamic password from his or her mobile phone.
- After that, it sends an identification request that includes a user name and a dynamic password.
- At this point, the server compares the given password with the one that was previously saved in VPR.
- Access would be provided following the receipt of valid verification.

IV. RESULTS ANALYSIS

Presented in this part are experimental data obtained from a prototype implementation of the mechanism under consideration. Comparative results of security tokens and mobile phones. for many factors of interest [15]. Java was used to develop a system for managing employees. The service of an SMS gateway was contracted in order to communicate the dynamic password to the user. Each SMS is charged at a rate of three rupees per text message. SMS service was integrated into the application through the usage of the smslib API. The MySQL 5.0 database was used to create the VPR and the user database. The entire programme was installed on a Linux-based web server and tested with a database of 1400 employees. A total of 8000 user requests were sent at various times and dates throughout the week, and it was discovered that the generated password was different each time due to the varying times and dates. Aside from that, the three-minute session period raises the security level and makes it difficult to hijack sessions or launch repeat attacks on them. It was necessary to create a prototype model for the password algorithm in order to check for recurrence of the password and to produce more than 1000 dynamic passwords. A static password array with more than 1000 passwords was formed and stored in a database. The prototype model creates more than 1000 dynamic passwords that are all distinct from one another. When we looked at the raw output from the model during its execution, we discovered that the seed value introduces a significant amount of randomness when different users have the same static password and they request at the same time on the same day. Furthermore, this evaluation considers the results of a comparison between a security token and a mobile phone. Comparative investigation of the suggested model and mechanism, as well as an examination of mobile phones and security tokens, was carried out for this comparison. These are the key security properties covered in this study, and they are called parameters.

V. CONCLUSION

Any digital solution's success is contingent on the successful implementation of security measures. Authentication is the process of determining whether or not the person attempting to access the account is legitimate. This study investigates the possibility of using a mobile phone instead of security tokens for strong authentication in order to improve security. It is no longer safe to use a static password because it is readily compromised by attackers. Although it is possible to readily increase the authentication strength of a security token, the additional cost, single use, and server synchronisation become the most significant drawbacks. Furthermore, a hardware token is issued to each user for their respective account, resulting in an increase in the number of tokens carried and an increase in the cost. Both the client and the organisation have suffered as a result of the manufacturing and maintenance of these products. Because we know that the vast majority of individuals have a mobile phone, the work presented an authentication architecture that would allow mobile phones to replace security tokens while also introducing dynamic interaction on demand. We suggested a password technique that generates a 24 bit (8 digits) dynamic password for each request in order to boost the randomness of the sequence and to produce dynamic passwords more quickly. The proposed mechanism establishes a standard for implementing two-factor authentication using a mobile phone. Both mechanisms make use of a GSM gateway to send dynamic passwords to mobile phones through SMS. Without a doubt, it also features a low cost that is reasonable in exchange for the high level of verification.

REFERENCE

[1.] W. S. Hathal, H. Cruickshank, P. Asuquo, Z. Sun and S. Bao, "Token-based lightweight authentication scheme for vehicle to infrastructure communications," Living in the Internet of Things (IoT 2019), 2019, pp. 1-6, doi: 10.1049/cp.2019.0173.

[2.] J. Aski, S. Gupta and B. Sarkar, "An Authentication-Centric Multi-Layered Security Model for Data Security in IoT-Enabled Biomedical Applications," 2019 IEEE 8th Global Conference on Consumer Electronics (GCCE), 2019, pp. 957-960, doi: 10.1109/GCCE46687.2019.9015217.

[3.] M. Dammak, O. R. M. Boudia, M. A. Messous, S. M. Senouci and C. Gransart, "Token-Based Lightweight Authentication to Secure IoT Networks," 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2019, pp. 1-4, doi: 10.1109/CCNC.2019.8651825.

[4.] Ali, Y. -D. Lin, C. -Y. Li and Y. -C. Lai, "Transparent 3rd-Party Authentication with Application Mobility for 5G Mobile Edge Computing," 2020 European Conference on Networks and Communications

(EuCNC), 2020, pp. 219-224, doi: 10.1109/EuCNC48522.2020.9200937.

[5.] E. Al Alkeem et al., "An Enhanced Electrocardiogram Biometric Authentication System Using Machine Learning," in IEEE Access, vol. 7, pp. 123069-123075, 2019, doi: 10.1109/ACCESS.2019.2937357.

[6.] N. Alamri, C. E. Chow, A. Aljaedi and A. Elgzil, "UFAP: Ultra-fast handoff authentication protocol for wireless mesh networks," 2018 Wireless Days (WD), 2018, pp. 1-8, doi: 10.1109/WD.2018.8361684.

[7.] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi and K. Salah, "A User Authentication Scheme of IoT Devices using Blockchain-Enabled Fog Nodes," 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), 2018, pp. 1-8, doi: 10.1109/AICCSA.2018.8612856.

[8.] M. Naveed Aman, S. Taneja, B. Sikdar, K. C. Chua and M. Alioto, "Token-Based Security for the Internet of Things With Dynamic Energy-Quality Tradeoff," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2843-2859, April 2019, doi: 10.1109/JIOT.2018.2875472.

[9.] T. Emadinia, F. Fatemi Moghaddam, P. Wieder, S. Dabbaghi Varnosfaderani and R. Yahyapour, "An Updateable Token-Based Schema for Authentication and Access Management in Clouds," 2019 7th International Conference on Future Internet of Things and Cloud (FiCloud), 2019, pp. 50-56, doi: 10.1109/FiCloud.2019.00015.

[10.] Naveed Aman, Muhammad et al. "Token-Based Security for the Internet of Things With Dynamic Energy-Quality Tradeoff." *IEEE Internet of Things Journal* 6 (2019): 2843-2859.

[11.] W. Yang, S. Wang, K. Yu, J. J. Kang and M. N. Johnstone, "Secure Fingerprint Authentication with Homomorphic Encryption," 2020 Digital Image Computing: Techniques and Applications (DICTA), 2020, pp. 1-6, doi: 10.1109/DICTA51227.2020.9363426.

[12.] S. K. Datta and C. Bonnet, "Securing IoT Platforms," 2019 IEEE International Conference on Consumer Electronics (ICCE), 2019, pp. 1-2, doi: 10.1109/ICCE.2019.8661966.

[13.] M. A. Kiran, P. Yogeshwari, K. V. Bhavani and T. Ramya, "Biometric Authentication: A Holistic Review," 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on, 2018, pp. 428-433, doi: 10.1109/I-SMAC.2018.8653751.

[14.] C. Huegel Richa and A. A. Fröhlich, "Low-Latency Secure Roaming in V2I Networks," 2018 VIII Brazilian Symposium on Computing Systems Engineering (SBESC), 2018, pp. 31-37, doi: 10.1109/SBESC.2018.00014.

[15.] Banerjee and M. Hasan, "Tap Based User Authentication on Smartphones for Visually Impaired People," 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2018, pp. 1-7, doi: 10.1109/ICCCNT.2018.8494056.

[16.] D. Chattaraj, M. Sarma, A. K. Das, N. Kumar, J. J. P. C. Rodrigues and Y. Park, "HEAP: An Efficient and Fault-Tolerant Authentication and Key Exchange Protocol for Hadoop-Assisted Big Data Platform," in IEEE Access, vol. 6, pp. 75342-75382, 2018, doi: 10.1109/ACCESS.2018.2883105.

[17.] L. Chen, "A Multimodal Biometric Recognition System based on Finger Snapping and Information Fusion," 2020 5th International Conference on Information Science, Computer Technology and Transportation (ISCTT), 2020, pp. 84-100, doi: 10.1109/ISCTT51595.2020.00024.