**ENHANCED SECURITY USING TWO-FACTOR AUTHENTICATION SCHEME IN SMART GRID**

Dr. B. Anvesh Kumar

Department of Computer Science

Vaageswari College of Engineering, Karimnagar, Telangana – India

Dr.V. Bapuji

Department of Computer Science

Vaageswari College of Engineering,Karimnagar,Telangana – India

1. **INTRODUCTION**

The usage of the IoT (IoT) has become widespread among various organizations. This has allowed for the creation of intelligent homes, communities, and constructions, among other applications. Many businesses have also recognized the advantages of incorporating IoT technologies. In addition, there are concerns about privacy and security when concealed or classified software is used alongside a small number of IoT devices and IoT technologies. The issues that arise are a direct consequence of the inherent limitations that are built into these technologies and pieces of equipment.

Distributed Denial of Service (DDoS) attacks have caused numerous notable incidents in the past. The instances mentioned above have brought attention to the significance of establishing suitable security processes for IoT (IoT) devices. Nonetheless, there are instances where certain norms are intentionally broken. Many industry professionals strongly believe that the most effective method for ensuring the safety of devices is by implementing two-factor authentication. According to Kandasamy et al. (2020), their investigation led them to the conclusion that this position aligns with all the findings they uncovered.

When it comes to ensuring the effectiveness of two-factor security, it is crucial to incorporate additional authentication alongside a password. The purpose of this process is to verify that user accounts have accurate and valid information. According to Landrock, it offers an extra level of assurance that is guaranteed to be effective. Using a smartphone application to enhance authentication mechanisms is crucial as it allows for additional security measures beyond the traditional method of logging in and providing a password. The organization's level of security has significantly increased as a result of implementing the system. One effective way to protect your account from unauthorized access by individuals who have obtained your login information illegally is to use two-factor authentication, also known as 2FA. The strategy mentioned can be employed as an effective means of deterring unauthorized access.

When performing the mentioned procedures, which may be subject to legislative rules, it is usually required to establish two-factor authentication, also referred to as 2FA. Depending on the strategy being executed, the specific order in which operations are carried out may vary. After successfully entering their login credentials, the particular user will be granted access to the selected website or service. The authorization will be granted immediately.

The password will be evaluated by the authentication service to determine its authenticity based on the specified criteria. After confirming and validating the user's password, the authority to apply the second factor technique will be granted. The procedure will be performed successfully as a result. In the second stage of the authentication method, the user is required to submit a unique code provided by the authentication provider. The computer is responsible for spreading this code, to be more precise.By implementing an additional component, such as a verification tool, individuals have the ability to improve the security of their information and reinforce the protection it provides. The method that was previously disclosed not only offers security against potential threats but also adds an extra layer of defence.

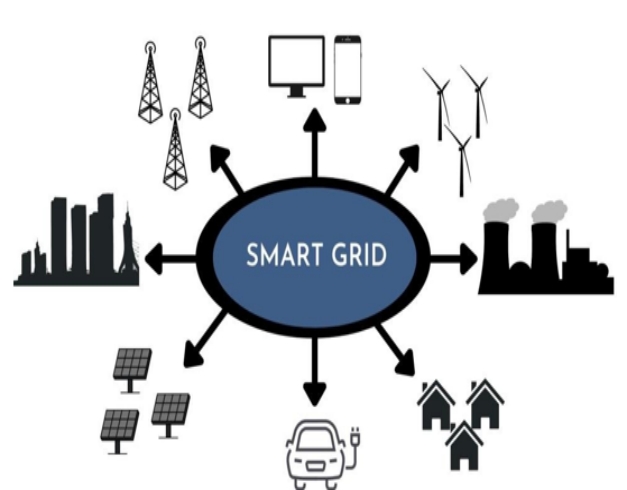


Figure 1. Smart infrastructure management for routine applications

According to De Souza et al. (2015), the formation of the IoT can be accomplished by a variety of techniques, including software development, interoperable systems, and legal initiatives. The long-term benefits of integrating the IoT into smart grid systems should not be underestimated. The IoT and smart grid technology convergence may hasten the development of networked devices such as smart meters and sensors. Similarly, this makes current technology equipment like laptops, smart displays, and communication devices easier to use.

The IOT (IoT) has simplified and access the transmission and receiving of data by smart grid service customers, producers, broadcasters, and distributors. The installation of cellular or cable lines is a realistic way to achieve this goal. The year is 2019, and Zhou and his team are present. Another advantage of this improvement is that it improves the IoT' ability to recognize and categorize data. By taking this strategy, the smart grid not only improves general stability, but also fortifies itself against the negative effects of disasters and rising demand for processing power.

The architecture represented in Figure 1 may supervise the execution of numerous applications at the same time. We are seeing the operation of an intelligent electrical grid. To ensure the correct identification of linked items, an extensive authentication method for IoT devices must be implemented. IoT devices must have unique and correct identifiers in order to connect to gateways or central servers. Administrators of information technology systems can efficiently oversee the actions of those devices in real time, thwart potentially harmful behaviors, and ensure safe connections by issuing a unique identifier to each device. In the case that a device exhibits aberrant behavior, an administrator can easily terminate the device's network connection.

1. **NEED FOR AUTHENTICATION IN THE IOT CONTEXT AND DESIGN CONSIDERATIONS**

More security and power management expertise is required in smart systems, especially in those where the majority of end devices are sensors. The use of these techniques is required by the use of sensors in various systems. The vast array of sensor-based systems that are currently in use has to be improved through the implementation of preventive measures. In order to safeguard verification processes against possible intrusions, a thorough security assessment is necessary.

Crash, chosen-plaintext, brute-force, Sybil, man-in-the-middle, replay, node capture, and message forging are some examples of attacks that fall under this category. Further focus is needed to properly handle the topic at hand, which is lowering DDoS threats. It is crucial to transfer as few messages as possible between verification partners in the event of a power outage. Since wireless communication has a restricted range, quick conversations are frequently required.

To develop successful IoT identification systems, a strong understanding of computational cost management is essential. The point made here is particularly relevant in situations where staff and resources are limited (Al-Naji and Zagrouba 2020). Verification systems depend on several strong cryptographic protocols and technologies to be efficient and secure. In IoT authentication systems, "scalability" often refers to the ability to support a large number of nodes and seamlessly add new ones without any setup or modifications.

Three essential elements fuel the IoT: software, a network, and sensor authentication. Without these components, networked devices could not integrate and operate with flawless efficiency. Software plays a crucial role in facilitating data flow and communication amongst IoT devices, enabling them to function together.

In addition, a stable network infrastructure is needed to facilitate data transfer between devices, allowing an IoT ecosystem to function smoothly. Lastly, sensor authentication guards against unwanted access or modification while preserving the security and integrity of data from IoT devices. In conclusion, the vast number of networked objects in IoT networks must be considered by recognition algorithms. "PUF" is gaining popularity in the hardware security space because of its better performance in comparison to software security solutions. Software is frequently less expensive than hardware in terms of cost. But software offers a complete security solution in addition to cost savings. It is imperative to carefully examine both feasible answers while taking the situation into account.

Devices connected to the IoT are frequently secured with single-factor authentication. The process of authenticating an object or person involves using previously collected data to confirm and validate their identification. Usually, the user's password and login information are needed for single-factor authentication. During our investigation, we found more cases where passwords and identities were stolen. There are numerous ways in which this knowledge could be used to harm someone. Security protections are significantly enhanced when two-factor authentication is combined with a login and password. Proof of ownership is essential when utilizing authentication, and it applies to both people and technology devices. Identity verification techniques that are considered the safest include biometrics and non-shareable passwords.

**3**.**EXISTING METHODS**

The security of the IoT is crucial for its ability to handle transactions efficiently and ensure prompt access to resources. In order to ensure the safe transfer of data to the websites users visit, it is crucial to establish a robust communication channel and ensure that every transaction is error-free. Cloud transactions are often considered to be a safer option for transmitting data because they typically employ robust security measures for authentication. In order to address the need for significant technological advancements, it becomes imperative to establish robust security protocols. Maintaining resource sharing security is crucial in order to ensure that only authorized users have access to resources. The creation of the smart grid idea was inspired by a significant study conducted by Xiao et al. (2018) on resource storage. In order to prevent further complications during the transaction, it is important to exercise caution when storing easily accessible goods.

Smart grids are capable of enhancing the efficiency of electrical networks by utilizing sensors and bidirectional communication. This functionality facilitates the ability to link consumers and vendors. The enhancement of sensor management can be achieved through the utilization of smart grids. These smart grids are designed to optimize the flow of data between individuals, resources, and various grids (Amin et al., 2018). Smart grids play a crucial role in optimizing data transmission. Smart grids have the potential to assist us in achieving this objective. The SG system has applications for three vital networks. There are three main types of networks: the Wide Area Network (WAN), the Neighborhood Area Network (WAN), and the Home Area Network (HAN). When the Smart Grid (SG) is integrated with the IoT (IoT), it has the ability to provide utility services while also ensuring the protection of consumer data.

Reduced accessibility ratios can be effective in mitigating the impact of denial-of-service (DOS) attacks. A decentralized strategy is more likely to succeed. SG's services are known for their high degree of efficiency and minimal energy inefficiency.

The Secretary of State utilizes the Kerberos authentication system in order to safeguard its members. The authentication process involves various methods such as biometric authentication, also known as fingerprint authentication, public key authentication (PKA), and one-time passwords (OTPs). The bundle being referred to also includes various biometric approaches, such as fingerprint authentication and other methods. According to a study conducted by Wang et al. (2018), it has been found that numerous authentication solutions are not effective when utilized in real-time scenarios. The researchers have reached a conclusion. When key-based authentication is not used, certain consequences can arise. In order to ensure security, it is important that each instance uses a unique password. This is because non-certificate authentication methods do not support multicasting. Therefore, using different passwords for each instance is necessary to maintain the integrity and confidentiality of the system. Multicasting requires a certificate to be completed.

The development of the two-factor authentication (2FA) system aimed to enhance the usability of secure multicasting services, enabling a wider range of individuals to make use of them. Safe key management systems utilize two-factor authentication as a form of authentication. To establish secure, reliable, and key-based authentication, it is crucial to begin with a fundamental step known as one-time authentication. The method being referred to involves the use of unique cryptographic keys for authentication. These keys are dynamic and require regular validation. In order to validate the users' credentials, the key is examined to determine if it grants significant access to resources (He et al., 2018). The verification process for the users' credentials is conducted in the following manner.

Password-protected methods are commonly utilized during system deployment. Due to the user session, the newly generated password is subject to limitations in terms of storage space and validity. In addition, it is worth noting that passwords have a time limit. The session-specific password is updated every time a user signs in or out. Das et al. (2018) thoroughly investigated the topic of password authorization. The investigation is also focusing on the password keyword. The availability of this feature is not restricted by location or time zone, as it can be accessed at any time. The process of providing credentials into distributed systems necessitates session-based user identity verification, which can make the process more complicated. To ensure that the correct login credentials are entered, it is important to follow the necessary steps and input the accurate information. When customers choose their own passwords, it may give the impression that the system is more intricate. However, this can also create an opportunity for unauthorized users to take advantage of it. In 2020, Wu and colleagues conducted their research. Password restrictions have gained popularity in certain locations, as they serve as a means to enhance security. However, due to concerns surrounding authentication, they have resurfaced as a topic of discussion. The difficulty of authentication is the reason for this. It seems that we may have made a mistake in our evaluation of the effectiveness of password rules.

Next, it is important to develop a hardware strategy. The device used by the user will verify their identity. In digital material, the strategy of validating identification and asserting exclusive ownership is commonly used, as stated by Almadhoun et al. (2018). Another way for users to authenticate is by using this method. In order to prevent unauthorized access to the device, a cryptographic system is implemented to verify each user. The reason for doing this is to ensure safety. The method described involves the utilization of multiple hash algorithms to substitute passwords with public key hash functions. This enables the facilitation of shared hardware access. The primary goal is accomplished. In 2020, Mahdi and other experts conducted research. Most microprocessor techniques utilize this method.

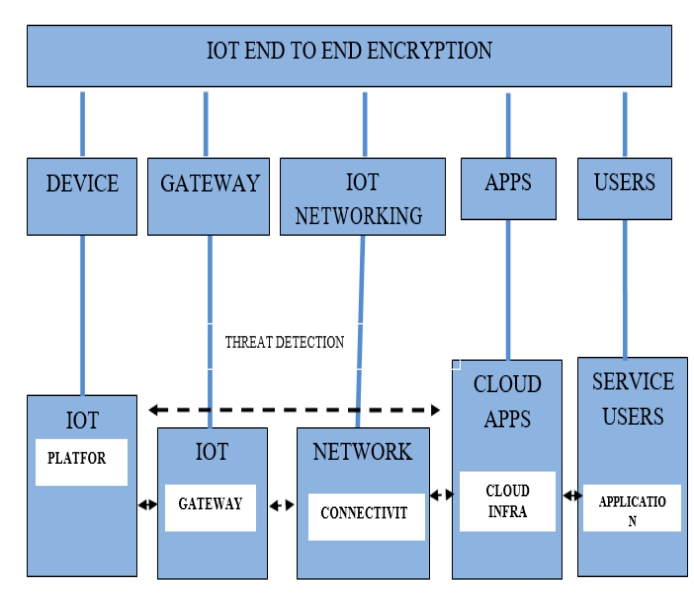


Figure 2. IoT Security: Implementing End-to-End Encryption

****

User accounts can be connected to several devices and password-protected using biometrics. You can create many access control and identification actions with this functionality. It permits the expansion of these endeavors. One alternative is to put these processes into practice. Numerous other identification systems are employed in addition to the above stated techniques. This field covers iris scanning, facial recognition, and biometric analysis. The Advanced Encryption Standard (AES) attempts to assess security and privacy, according to Kumari et al. (2018). This is the main objective of the AES(Advanced Encryption Standard). AES data storage is legally limited to a certain group of businesses. This is true given the context of the issue.

Symmetric-key encryption is used to store passwords. For this system to work, it only has to identify human and equipment deficiencies in a single scan. It supports both symmetric and asymmetric encryption, according to Shah and Venkatesan's (2018) research. Moreover, encryption key algorithms will be automatically included in its system. Amazing apparatus with blazingly quick video verification and recovery. This is primarily due to the fact that it requires little storage space and is rarely used. Furthermore, the authentication procedure employs essentially the same methods throughout.

Two encryption techniques verify the credentials of the system after credential verification. Although certificates are necessary for only one algorithm, the other also needs them. The final strategy and course of action must be agreed upon by all parties. You must first obtain an encryption certificate in order to authenticate properly. This certificate checks the digital signature of the user against predetermined criteria. Symmetric-asymmetric content can be decrypted with an asymmetric cryptographic key. All protocols and transactions are protected by encryption using the above-mentioned key.

The IoT, which safeguards all linked devices, makes complete security possible. Complete security is made possible by this. Complete safety is therefore feasible. In 2018, Tao et al. discovered three critical parameters related to IoT security. There is hardware, biometric, and signature security. Because these three themes are so important, we gave them a lot of attention. Authentication and a key agreement are necessary for data security. There is a connection between the two parts. To generate a session key, multiple network entities need to interact together. It is simple to grant permission to all parties and keep all communications private with this approach.

The efficacy of the current technique may be restricted by two issues. A significant increase in initially available processing capability is necessary for intelligent system integration. So, important security responsibilities remain unfulfilled (Braeken 2018). This is a result of the state of affairs. This study aims to address several intricately related problems by concentrating on currently used techniques.

**4. PROPOSED METHOD**

To ensure both system security and acceptable service availability, it is recommended to design a solution that incorporates two separate components for user authentication. By ensuring that both demands are fully addressed, this approach guarantees comprehensive resolution. All devices in the infrastructure have two-factor authentication, also known as 2FA, enabled. Achieving a secure gateway is accomplished by establishing a secure connection. The assessment of the efficiency of the system's security mechanisms is performed. The smart grid is responsible for managing all of these devices, ensuring that every internet-connected device in the IoT (IoT) is monitored and controlled. The use of the end-to-end (E2E) protocol has become widespread in encrypting all network-connected devices. The current way of doing things is like this. The purpose of this practice is to guarantee that identities are provided in a reliable way, while also preserving the confidentiality of the information they hold. In order to optimize the efficiency of the Grand and Revoke operations, it is necessary to conduct an investigation into smart grid-connected devices. The reason for this is that the medication needs to be taken precisely as instructed by the healthcare provider. Two-factor authentication, also known as 2FA, is a security measure that mandates users to go through two separate verification processes in order to gain access to a platform or system. The significant benefit of this approach is that it surpasses traditional methods of authentication.

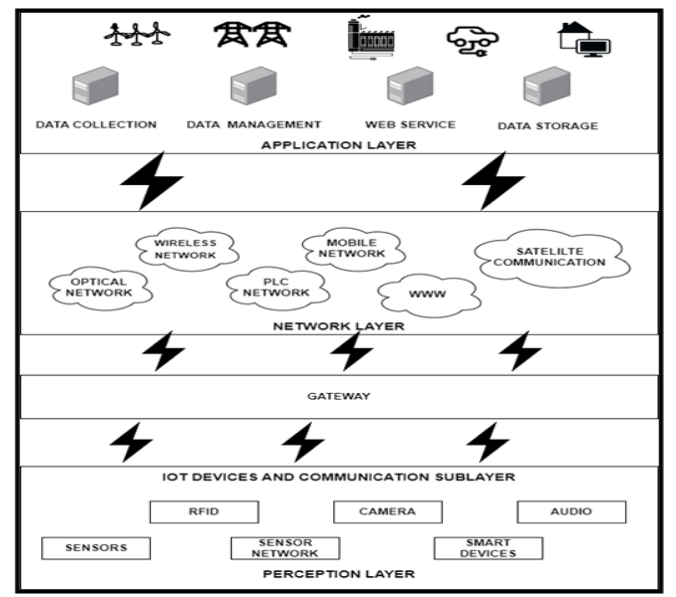
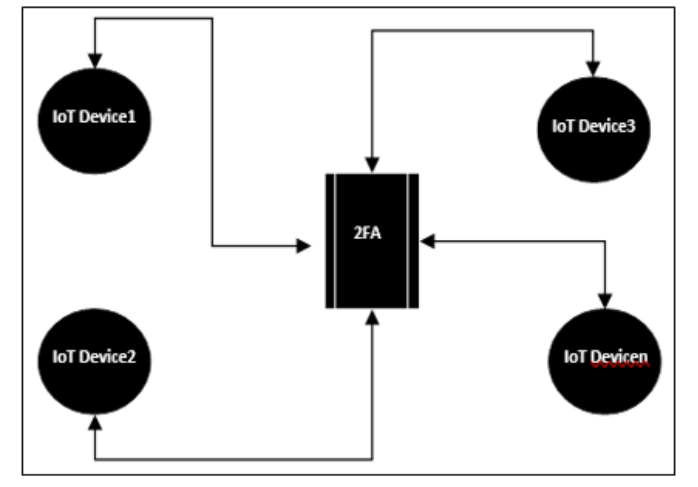


Figure 3. Smart grid-based interconnectivity of IoT devices

The book illustrates the organizational structure of the Smart Grid (SG) in Figure 3. The IoT (IoT) is a network of devices that can perform various activities efficiently. In the IoT, every device is connected through a complex electrical infrastructure and comes with its own specific set of operating instructions. Before starting, it is important to ensure that the name of the item is accurate. The statement remains valid when considering data from the IoT and Smart Grid.The effectiveness of IoT architectures relies heavily on the ability to identify devices. Every component of the device is assigned a unique number. If there are any significant alterations made to the device or serial number, it is necessary to reevaluate the registration. The conundrum stems from the expanding operations of the IoT (IoT). A distributed system is created by visually identical and interconnected IoT devices, each having defined functionality. These gadgets perform similar tasks. To accomplish our objectives, we implemented two-factor authentication. Figure 3,displays the outcomes of the deployment of the two-factor authentication system.

 Figure 4 . Additional security measures for IoT device connections

Limiting user access Authentication is impossible with IoT devices because they cannot store a private key. They believe PUFs must be used according to current literature protocols. More than two factors must be considered when forming protection. By using their real names, the devices increase security. An outsider can simply monitor IoT devices. Most solutions cannot ensure the privacy of IoT-connected devices due to this restriction. Even if differential design methods improve reliability, PUF manufacturing noise remains an issue. Noise can disrupt the transmission of one or more units per action, depending on the situation.

Khan and Salah (2018) report that the Smart Grid's global authentication process ensures data validity, secrecy, and integrity with a simple method. Grant and revocation and two-factor authentication help verify IoT devices. Combining multiple authentication mechanisms may work. Establishing a secure connection is the second step. After reviewing the reciprocal identification system's safety precautions, the device was chosen for the first step. Figures 5 and Figure 6, show two-factor authentication evolution. These data demonstrate technical advancement. The system verifies connecting devices and users, ensuring trustworthiness.

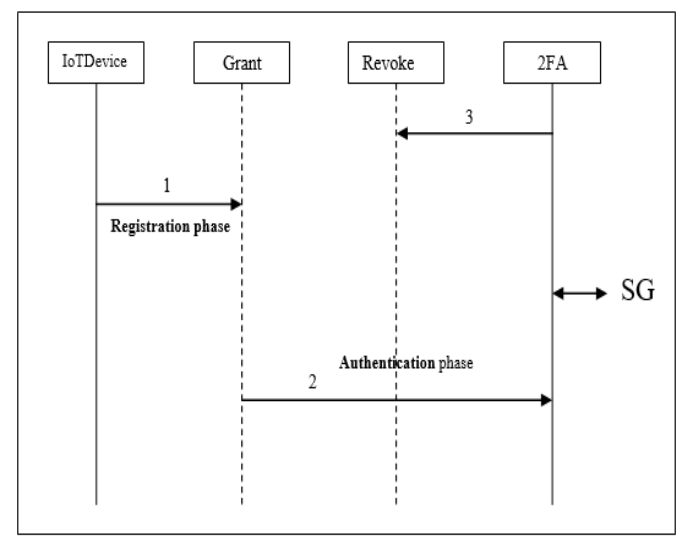
**Phase 1: Device enrollment**

Figure 5 . The grant phase is the phase that authenticates the device

**4.1.1 Device Registration: Grant Phase**

It has been discovered that traditional methods of authentication, including passwords and private keys, possess security vulnerabilities. These approaches depend on secrets that are widely known, rendering them susceptible to potential assaults. These authentication methods are less effective than alternative methods, leading to less favorable results. To gain access to the system via two-factor authentication, users are obligated to supply a password. Subsequent to the accurate input of their password, users are required to authenticate their identity by means of an additional device. "IoTD" is an abbreviation that denotes "IoT devices," whereas "U" symbolizes "users." Additionally, the initial and secondary credentials are combined to produce the acronym "PWD." It is imperative to implement a dependable password verification system in order to preserve the integrity of the authentication gateway and the device route. Equation 1 holds significance when contemplating authentication and registration with respect to the device and the user within its assigned domain.

𝑅i = ∑𝑛

𝑚 j=i

(𝑈i,j𝐼𝑜𝑇𝐷i,)

(4.1)

𝐼𝑜𝑇𝐷i = ∑(𝑈i𝑃W𝐷i) (4.2)

i=1

 Where Ri denotes the ith user's inscription, IoTDi denotes the user who confirmed the identity of the IoT device. i, using the password PWDi. When Ri balances IoTDi with Ui and PWDi, the device is successfully registered. This procedure is iterated for every IoT device that establishes a connection with the system. During the identification phase, all devices are connected to SG as soon as the initial stage is complete. After SG has verified both the password and the system, the system will be registered.

* + 1. **Revoke Phase**

If the device failed authentication, the revocation process ignored the system's SG registration. Despite having access, this was the situation. After being withdrawn from the system, the unauthenticated device is no longer at risk.

This book discusses the system's defense systems to deter invaders. Session keys are needed for user authentication, device communication, and secure channel communication. The key is needed for authentication. This info is generated during system registration. However, this will not effect link functionality after the session. After password authentication, the user will remain connected to the device throughout the session.

i=1𝑆i = ∑𝑛𝑈i𝑃W𝐷ic𝐼𝑜𝑇𝐷i (4.3)

Where 𝑆i is the session key for creating interconnection between the user and the session. The key is created by combining the user and their registered password where the user must have prior registration for the concerned IoT devices. The symbol c ensures the user 𝑈i has been registered with 𝐼𝑜𝑇𝐷i with password 𝑃W𝐷i.

With the extended session, the process leads to Phase 2 which ensures the device is based on the user profile:

**IoT Device - Grant Process**

Step 1: Two-factor authentication is utilized for each and every IoT device that is able to establish a connection to the Smart Grid.

Step 2: At the same time that the IoT device is being incorporated into the system, the Grant procedure will also begin.

Step 3: Once the authentication system file has been established, the Revoke process will begin immediately.

Step 4: In the event that the authentication attempt is successful, the Grant procedure will make it simpler to implement two-factor authentication for the purpose of secure group access authorization.

This is the following step, which involves verifying the identity of every user on their own individual gadget of choice. Through the beginning of a session, users are granted authorization to become members of the strategic group. The verification, the starting, and the registration phases make up the separation of the second phase into three discrete phases. When taken together, the first and second phases offer a channel that is both secure and efficient, allowing different systems to connect with one another and interact with one another.

**IoT Device - Revoke Process**

Step 1 Two-factor authentication connects each IoT device to the Smart Grid.

Step 2: The Revoke system verifies the user's identification by comparing the user, device, and session-id.

Step 3: SG requires two-factor authentication.

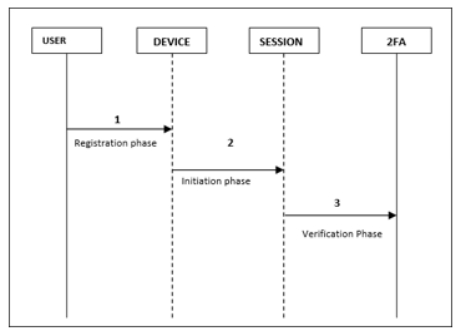


Figure 6 Smart Grid Sessions: One-Time Password vs. Two-Time Password

|  |  |  |
| --- | --- | --- |
| (Table 1) | 1FA | 2FA |
| Authenticating Device | Yes | Yes |
| Authenticating User | Yes | Yes |
| Authentication process | No | Yes |
| Verification process | No | Yes |

If you would like to assess the effectiveness of one-factor authentication (1FA) and two-factor authentication (2FA), please refer to Table 1. We are fully committed to acquiring this knowledge in order to achieve our goal of gaining a deeper understanding of the chosen course of action. For one-factor authentication (1FA) to work, both the user and the device need to provide legally authorized identification. The perception that the personal authentication process is ineffective is often attributed to the lack of attention given to it.

Table 2 Procedure for SG to grant and revoke with 2FA

|  |  |  |
| --- | --- | --- |
|  | **Grant** | **Revoke** |
| Authenticating Device | Yes | Yes |
| Authenticating User | Yes | Yes |
| Authentication process | Yes | Yes |
| Verification process | Yes | Yes |

Table 2 provides a contrasted picture of the Grant and Revoke procedures that can be referenced for reference. It is necessary for both the user and the device to demonstrate that they are legitimate recipients of the data in each of these instances. As a consequence of the authentication being saved in the Session component, which is an essential component for the deployment of two-factor authentication in SG, this scenario has come about.

After the process of mutual authentication, the server and device proceed to exchange the session key promptly. The methodology employed in this article has the capability to achieve session key unanimity. In order for the specified authentication mechanism to function properly, it is necessary for each session to be assigned a unique alias, known as an AID, which is obtained from the authenticating device. In order to ensure authenticity, it is necessary to complete this task. The AID that was used in the previous session will not be utilized again. The server has the ability to detect actions performed by IoT devices, making it a unique feature. In cases where the device encounters difficulties with synchronization, it will resort to utilizing a fabricated and inactive identity. The gadget must remove this identity from its data bank. The security technique mentioned involves the use of a unique session identifier to unintentionally bypass monitoring and identification. If you are looking for a methodical way to defend your privacy from angry family and friends, this approach can provide you with the necessary guidance.

The purpose of this strategy is to minimize the potential for an unauthorized individual to compromise the functionality or security of an IoT (IoT) device through physical means. The conductivity of the PUF can be affected by the equipment requirements, which can potentially decrease its usefulness. If the authentication approach is implemented, the PUF (Physical Unclonable Function) will need to navigate through additional complexity in order to achieve its goals. The statement indicates that the computer has knowledge of attempts to breach its software. The proposed method utilizes Physical Unclonable Functions (PUFs) to effectively prevent replication and cloning. The proposed approach ensures replication resistance by following this method. Please make sure to emphasize this fact.

* 1. **RESULTS AND EVALUATION**

We did a thorough examination of the simulation's outcomes and kept a close check on the entire job verification procedure. To successfully implement two-factor authentication (2FA), it is critical to prepare ahead of time, set aside funds for unanticipated delays, and create a budget to cover network and compute costs. Figure 7 depicts the increase in the number of IoT devices that have been integrated into the smart grid and provides a chronological overview of the trend. Every hour or so, a new technological advance is disclosed. The phrase "Device Id" refers to the unique identification established by an IoT (IoT) gadget whenever it connects to a social networking website. As a result of this, the item acquires a distinct and instantly recognizable personality. The Singapore Government has the jurisdiction to manage and regulate devices connected to the IoT only within a 100-meter radius. The use of distance as a measurement reduced the likelihood of encountering any problems or obstacles during the verification process dramatically.

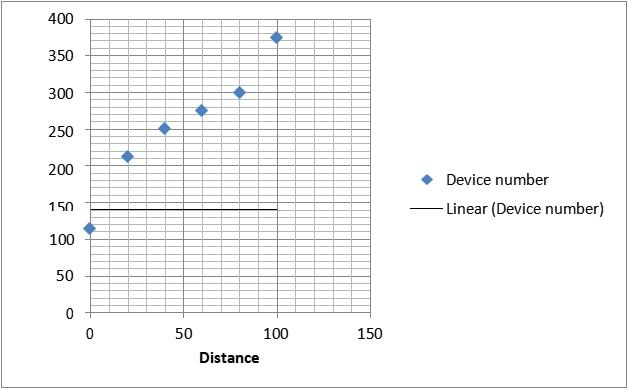


Figure 7. Total number of devices located within the SG Zone

Following the mutual authentication process, the server and device share the session key as soon as possible. The mechanism used in this article is capable of achieving session key unanimity. To ensure that the given authentication technique works successfully, each session must be issued a unique alias, known as an AID, which is retrieved from the authenticating device. This assignment must be completed in order to confirm authenticity. The AID used in the previous session will not be used again. The server can identify actions performed by IoT devices, which is a unique functionality. When the device meets synchronization issues, it will resort to using a created and inactive identity. This identification must be removed from the device's data bank. The suggested security approach involves the use of a unique session identifier to inadvertently bypass surveillance and identification. This strategy might give you with the required instruction if you are looking for a methodical manner to defend your privacy from furious family and friends.

The goal of this method is to reduce the possibility of an unauthorized individual physically compromising the functioning or security of an IoT (IoT) device. The equipment requirements can alter the conductivity of the PUF, thereby reducing its utility. If the authentication strategy is used, the PUF (Physical Unclonable Function) will have to deal with more complexity in order to achieve its aims. The phrase implies that the computer is aware of attempts to exploit its software. The suggested solution efficiently prevents replication and cloning by utilizing Physical Unclonable Functions (PUFs).

By using this mechanism, the proposed approach ensures replication resistance. Please make a point of emphasizing this fact.

|  |
| --- |
|  |
|  |  |

Figure 8.Average Device Count in the SG Zone

Figure 8 provides a visual representation of the relationship that exists between the extension of the range and the overall number of devices that are typically used. For the purpose of precisely determining the distance that exists between devices in a network, it is crucial to take into consideration not only the average distance that separates the devices but also the total number of devices that are present in the network. This is because taking into account both of these factors is necessary. When it comes to evaluating the volume of communication traffic, the most significant factor to consider is the distance that separates two sites. The suggested protocol takes use of the key-hash function and the challenge-response notion in order to validate the present state of communications, trace their origin, and ensure that their integrity is protected. During the course of their research, Cho et al. (2014) came to the realization that the recipient is able to verify the genuineness of the message by examining the outcome of the key-hash technique.

A representation of the delay is shown in Figure 9, which depicts the average delay that each network node experiences. Figure 9, also includes a representation of the delay. Two-factor authentication is widely considered to be the method that is the most dependable and effective, despite the fact that the number of electronic devices that are being used has increased. When SG was in the process of adopting two-factor authentication, they took into mind the additional work that would be necessary for communication. This was something that they took into consideration. In light of the fact that it makes use of dynamic principles, the program is able to make decisions on the addition or removal of devices.



Figure 9. Delays in the Average Cost of Communication

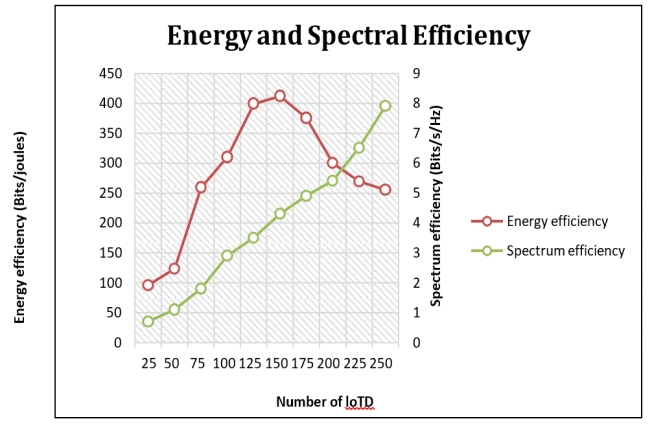
****

Figure 10. The efficiency of energy and spectrum utilization

Figure 10,shows how the suggested two-factor authentication approach might improve smart grid energy and power spectrum use. See the lower part of the figure for details. This is because two-factor authentication is being implemented. IoT-connected microgrids monitor power consumption, respond to quick energy pricing and distribution changes, and develop environmentally friendly and effective electricity consumption plans. Microgrids also reduce electricity costs. Microgrids also reduce electricity expenses.

These solutions require application patterns and real-time power efficiency statistics. Because these solutions must be developed, this is true. The system has not been significantly changed since its inception. This is because two-factor authentication has had little impact on power consumption and spectrum utilization. The system's lack of significant changes may explain the above behavior. Due to device certification process changes, new security and privacy safeguards have been applied. Many precautionary actions have been taken since its implementation.

**5.SUMMARY**

The purpose of this research is to look into Singapore's method for detecting intelligent IoT devices. Furthermore, the study intends to investigate the numerous repercussions that could result from using this strategy. The primary goal of this research is to better our understanding of the potential implications that may develop in the future. During the investigation, data on the vast range of possible outcomes that could result from the system's adoption will be obtained. Instead of using computer systems to calculate the average distance between devices, participants in the experiment concentrated on determining the communication overhead. As a result, the amount of time required was reduced. The above stated logic serves as justification for this. All SG Zone devices connecting to the network must employ two-factor authentication. This is because dual-factor authentication is designed to be used in this manner. The use of this method will substantially hasten the achievement of that goal. According to the acquired conclusion, the position is the best alternative for obtaining the highest realistic level of performance given the available resources. This result was reached as the number of devices and their mean distance from one another increased. When the material is considered with the findings, this is the inference that may be drawn from the study's findings. In the following section, we will look at how the growing number of devices in the system affects the system's working speed. Before installing smart grid equipment and implementing two-factor authentication, the average delay must be thoroughly evaluated. This is an extremely significant element that must be considered. Because the two-factor authentication system was specifically intended to work only with approved devices, reliability and security are trademarks of the verification procedure.

REFERENCES

1.Abbasinezhad-Mood, D., & Nikooghadam, M. (2018). Efficient anonymous password- authenticated key exchange protocol to read isolated smart meters by utilization of extended chebyshev chaotic maps. IEEE Transactions on Industrial Informatics, 14(11), 4815–4828

2.Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). IoT: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys and Tutorials, 17(4), 2347–2376.

3.Banerjee, S., Chunka, C., Sen, S., & Goswami, R. S. (2019). An Enhanced and Secure Biometric Based User Authentication Scheme in Wireless Sensor Networks Using Smart Cards. Wireless Personal Communications, 107(1), 243–270.

4.Banerjee, S., Odelu, V., Das, A. K., Chattopadhyay, S., & Park, Y. (2020). An efficient, anonymous and robust authentication scheme for smart home environments. Sensors (Switzerland), 20(4), 1–19.

5.Banerjee, S., Odelu, V., Das, A. K., Srinivas, J., Kumar, N., Chattopadhyay, S., & Choo, K. K. R. (2019). A Provably Secure and Lightweight Anonymous User Authenticated Session Key Exchange Scheme for IoT Deployment. IEEE IoT Journal, 6(5), 8739–8752.

6.Barbareschi, M., Bagnasco, P., & Mazzeo, A. (2015). Authenticating IoT Devices with Physically Unclonable Functions Models. Proceedings - 2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 3PGCIC 2015, 563–567.

7.Bendavid, Y., Bagheri, N., Safkhani, M., & Rostampour, S. (2018). IoT device security: Challenging “A lightweight RFID mutual authentication protocol based on physical unclonable function.” Sensors (Switzerland), 18(12).

8.Bhatt, A. P., & Sharma, A. (2019). Quantum cryptography for IoT security. Journal of Electronic Science and Technology, 17(3), 213–220.

9.Boddupalli Anvesh Kumar, Dr. V. Bapuji, **“**Enhanced authentication and key management scheme for securing data transmission in the Internet of Things”, International Conferences on Research and development in sciences,Pharmacy ,Education,law and Hunanities: The Fururistic Apporach on 5th

Feburary 2022.

1. Boddupalli Anvesh Kumar, Dr. V. Bapuji, “*Secure And Lightweight Authentication Protocols for Devices in Internet of Things”*, Tuijin Jishu/Journal of Propulsion Technology, Vol. 44, No.5, Pages: 2419-2427, ISSN: 1001-4055, December 2023.

<https://www.propulsiontechjournal.com/index.php/journal/article/view/2979/2043>

11.El-Hajj, M., Fadlallah, A., Chamoun, M., & Serhrouchni, A. (2019). A survey of IoT (IoT) authentication schemes. Sensors (Switzerland), 19(5), 1– 43.

12.Fakroon, M., Alshahrani, M., Gebali, F., & Traore, I. (2020). Secure remote anonymous user authentication scheme for smart home environment. IoT (Netherlands), 9

13.Gope, P., Amin, R., Hafizul Islam, S. K., Kumar, N., & Bhalla, V. K. (2018). Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment. Future Generation Computer Systems, 83, 629–637.

14.Gupta, A., Tripathi, M., Shaikh, T. J., & Sharma, A. (2019). A lightweight anonymous user authentication and key establishment scheme for wearable devices. Computer Networks, 149, 29–42.

15.Lee, H., Kang, D., Ryu, J., Won, D., Kim, H., & Lee, Y. (2020). A three-factor anonymous user authentication scheme for IoT environments. Journal of Information Security and Applications, 52, 102494.