IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 5, May 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005327 |

An Effective Authentication Mechanism between Smart Grid Employees and Assets Using Location and Time-Based OTP

Susmitha Bhavanam, Shaik Shabreen, Tiyyagura Niharika, Polisetty Pujitha Sarvani, J.M Babu

UG Students, Dept. of C.S.E, Vasireddy Venkatadri Institute of Technology, Affiliated to Jawaharlal Nehru Technological University, Kakinada, A.P, India.

Associate Professor, Department of Computer Science and Engineering, Vasireddy Venkatadri Institute Of Technology, Nambur, Andhra Pradesh, India.

ABSTRACT: A smart grid is a network of electricity which enables a two-way flow of data and electricity with digital communications technology, that can react,detect and proact to changes inmultiple issues and usage. Smart grids usually have self-healing capacities that enables electricity consumers to become active participants. IoT authentication is a one such model for building trust in the identity of IoT devices and machines to secure or protect data and provide access control when information travels through an untrusted network such as internet. IoT devices use this kind of process to do role-based access control and to ensure that devices have only access and permission to do exactly what they require. In IoT applications such as smart grids, if any problem occurs in the network, an employee comes and solves the issue. But these employees are not properly authenticated. To achieve proper employee authentication, the device should automatically generate an OTP (One Time Password) based on time and location to the substation which is in turn received by that employee. Also, the device must be capable of maintaining a log in the substation, regarding the issues occurred and employees concerned. Hence, the output produced can be applied to IoT devices with proper communication, low computations, and high speed.

KEYWORDS: Smart Grid(SM),Internet Of Thngs(IoT),Two way flow of electricity, authentication,self- healing capability,role based access control,One Time Password(OTP),substation,log, computation,speed.

I. INTRODUCTION

The development of the mobile technologies, people can access Internet services ubiquitously by the hand-carried mobile devices. In the present-day-world, many mobiles are entitled with a GPS module for providing information about real-time location. The location prediction technique has been improvised with the assistance of the mature GPS technology. A precise location predication can facilitate the geo-encryption or geo-authentication to improve the security protection. These advantages are successfully applied to the security control mechanisms in network environments. On the other hand, the One Time Password (OTP) scheme has been applied to some important services, such as e-commerce transactions and online banking services. Such a mechanism of a volatile password can lessen the risk of password being stolen by unwanted persons and malicious users. In this project, we propose a solution that utilizes a time and location dependent OTP which can prevent permanent passwords from being sniffed for authentication while accessing the Internet application services in a mobile environment.

This solution which is proposed improves the user authentication and data security to a very large extent. This scheme can transparently authenticate users in a tolerant geometric region as well so that users do not need to manually type in their passwords. Meanwhile, such a location assisted authentication can reinforce the time-dependent only OTP scheme since the hackers are not easy to get exact time and location information about the users simultaneously. Besides, a Short Message Service (SMS) based mutual authentication schemewas also proposed for dealing with data breaches and security misjudgements. In this project,we briefly introduce the related works about prediction of location based on latitude and longitude values and location-based authentication with OTP.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005327 |

A smart grid is anetwork of electricity which enables a two-way communication which is two-way flow of electricity and data with digital communications technology which enables to react,detect and pro-act to changes in multiple issues and usage. Smart grids possess self-healing capability that enables electricity consumer to become active participants.

Smart grids became known over a decade ago and are essential in the digital transformation of the electricity sector. An introduction with definitions, trends, and essential characteristics of smart grids.Big data analytics and IOT technologies are important technology drivers in smart grids whereby analytics shift to the edge, as in edge computing. Smart grids rely on many advanced technologies but aren't just related to IT or even others technologies.

A smart grid is used for serving several purposes and the evolution ofsmart grids from traditional electric grids is driven by multiple factors like changes on the level of electricity production, evolutions in metering, decentralization, the advent of the involved 'prosumer', , the rise of microgeneration,changing regulations and microgrids, renewable energy mandates with more energy sources and new points where and purposes for which electricity is needed.An electrical grid is a network which is used for delivering electricity from places where it is generated like powerplants and substations and is transmitted to the final destinations where electricity is consumed likebusinesses, households, various other facilities and consumers in general.

II. RELATED WORK

Some of the existing methods of authenticating a person are

5.1.1 Password based authentication:

Passwords are very common methods that are used for authentication of devices. Passwords can possess different forms like a string of numbers, letters or special characters. However, passwords are more likely prone to attacks that degrades the effectiveness. On an average, a person can have about 25 different accounts online, but only 54% of the total users can use different passwords over their accounts.

Major fact is that there are multiple passwords that are to be remembered. As a result of it, most of the people choose convenience or comfort above security.Most people use simple passwords instead of creating reliable passwords because they are easier to remember.

Passwords have a lot of limitations and are not completely sufficient to protect online information. Hackers can easily track user credentials and sensitive information like passwords by running through all possible combinations till they seek a match.

5.1.2Multi factor authentication

Multi Factor Authentication (MFA) is one of the methods for authenticationthat requires one or more independent ways for identifying users.Examples of MFA include Captcha tests, codes generated from smartphones of user's,voice biometrics, fingerprints and facial recognition.

MFA authentication methodologies improve the confidence of users and employees by adding multiple layers of providing security.People have chances of losing their mobile phones or SIM cards and may not be able to generatecodes for authentication.

5.1.3Certificate-based authentication

Certificate-based authentication technologies are majorly used to identify machines,users and devices with the help of digital certificates. A digital certificate is basically an electronic document that is based on the idea of a driver's passport or a license.

The certificate in this scheme consists of the digital identity of a user likedigital signature and public key of a certification authority. They prove the ownership of a public key and are issued only by certification authority. When users signs in to a server, they are required to provide digital certificates. The server then verifies the credibility of the certificate authority and the digital signature.

5.1.4. Biometric authentication

Authentication using biometrics is a security process which relies on biological characteristics:

- Biological characteristics can be compared easilyfor authorizing various features that are saved inside the database.
- Biometric authentication also has the capability to control physical access when it is installed on doors and gates.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005327 |

- One can also add biometrics to your process of multi-factor authentication.

Biometric authentication technologies are also used commonly by governments ,consumers and private corporations like airports, national borders and military bases.As the technology is being adopted increasingly due to the ability to achieve a high rate of data protection without creating friction to users. Common biometric authentication methods include:

- **Facial recognition**: It matches different face characteristics of individuals by trying to gain access to an approved face stored that is stored inside the database. Face recognition is proved to be inconsistent while comparing faces that are kept at different angles or while comparing similar people like close relatives. Facial liveness like ID R&D's passive facial liveness prevents spoofing.
- **Fingerprint scanners**: are used to match unique patterns that are available on an individual's fingerprints. Some of the new versions of fingerprint scanners can also assess the vascular patterns present in people's fingers. These scanners are currently one of the most popular biometric technologies for day-to-day consumers, despite their periodic or frequent inaccuracies. This popularity can be solely attributed to devices with Mac OS like iPhones.
- **Speaker Recognition** —also known as voice biometrics, examines a speaker's speech patterns for the formation of specific shapes and sound qualities.Voice-protected devices usually depends on standardized words to identify or authenticate users, just like how a password works.
- **Eye scanners:** include technologies like iris recognition and retina scanners. Iris scanners project a bright light towards the eye and search for unique patterns in the coloured ring around the pupil of the eye. These patterns are now compared to the information that is approved and stored inside the database. Eye-based authentication may suffer inaccuracies if a person wears glasses or contact lens.
- **Token-based authentication:** Token-based authentication technologies allows users to enter their personal credentials or sensitive information like passwords once and receive a unique encrypted sequence of random characters in return. One can then use this token to access protected systems instead of entering credentials again and again. This digital token proves that you already had permission to access.

III. PROPOSED SYSTEM

The above authentication schemas are already existing and are also being used. They do have some short comes while working and it can be possible for the hacker or intruder to get access of the system. So, in order to avoid these kind of data attacks, we as a team of four proposed this system of authentication by generating OTP based on time and location. This particular feature is applied to an IoT application, i.e, smart grid. The already existing systems like authentication of employees based on identity cards, authentication based on mail Id's, authentication based on passwords do not provide much security. In order to overcome these limitations or drawbacks, we proposed this system adding an extra feature which is location.

OTP GENERATION

The current project works with authenticating the smart grid employees using OTP (one time password). The otp is sent to the mobile number that has been given to the employee and stored in the database of the employee details. The Otp is generated using the current time of the system and the current location the employee and one important thing is if the location of the smart grid and employee current location matches then only, he will be able to receive the otp or else he won't be able to receive the otp.

The advantages and security improvement of our proposed scheme in this sub-section, we discuss the advantages and security improvement of our proposed scheme.

1.An OTP based authentication scheme is difficult to be fabricated because the passwords that are generated are volatile. Hence, the malicious hacker finds it hard to guess the one-time-passwords.

2. The proposed scheme can provide a not only time dependent but also location-dependent OTP that is volatile and not reusable. That means even if an attacker intercepts the message, it is hard to disguise a legitimate user's location in terms of time and location factors.

3. If a user moves steadily, the user does not need to input his account and password. It is convenient for a user to transparently login the server without an explicit manipulation, such as manually typing in the username and password.

4. To enhance the precision of the location prediction, our scheme is developed based on the statistics of the recent movement and moving direction of the mobile device.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005327 |

IV. RESULTS

The following is the entire flowchart of the project demonstrated step by step.

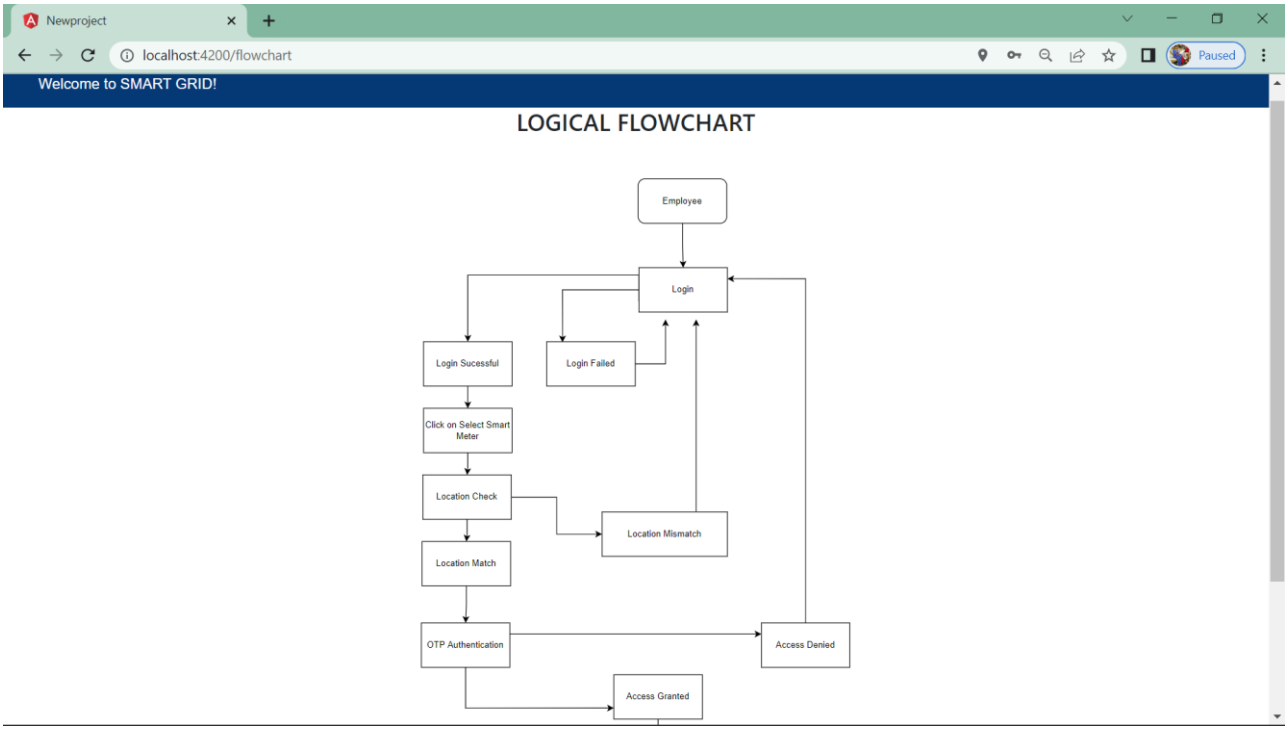

Fig 1:Flowchart of entire project

As observed from above figure, this is the total process of flow that happens in the enture project and the final output that is obtained from the project is either granting access or denying access to the smart grid employees.

V. CONCLUSION AND FUTURE WORK

Although there are many mobile applications existing in the present day world, the security issue is still the most dominating one for most of the users today. Nowadays OTP is mostly used for user authentication because OTP is volatile and non-reusable. The specifications like Europay MasterCard Visa Chip Authentication Program (EMV/CAP) describesmany benefits of using such technology. Many OTP authentication schemes were already been proposed for one-time usage.Butmany of them are time constrained. There is still scope for improvisations if we can add the location information into consideration in the mobile world. After studying some related research about the location prediction, location-based encryption and signatures, and mutual authentication. So, in this project, we proposed a time and location-based OTPscheme to authenticate users while accessing the application server in this paper. A time and location constrained OTP scheme helps to lessen the risk of passwords being stolen by unauthorized users so that it can make an attacker harder to break through. Meanwhile, if a user moves steadily, the user can get transparently authenticated without remembering the password. To supplement the possible flaws in the scheme that is already proposed, a SMS based mutual authentication mechanism is also proposed in the article to make up and get ourselves ready for the unexpected data breaches and misjudgements.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 5, May 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1005327 |

REFERENCES

[1] Three Phase Authentication Protocol for Smart Grid Communication
H Goel, A Gupta, H Jain, A Khandelwal… - … IEEE Conference on …, 2019 - ieeexplore.ieee.org

[2]Authentication and Authorization scheme for various user roles and devices in smart grid.N Saxena, BJ Choi, R Lu - IEEE transactions on Information …, 2015 - ieeexplore.ieee.org

[3] A cryptography and machine learning based authentication for secure data-sharing in federated cloud services environment..AK Singh, D Saxena - Journal of Applied Security Research, 2021 - Taylor & Francis

[4]Geo-location based QR-Code authentication scheme to defeat active real-time phishing attack..S Kim, D Choi, S Jin, S Lee - Proceedings of the 2013 ACM workshop …, 2013 - dl.acm.org

[5]https://www.researchgate.net/publication/220762594_Design_of_a_time_and_location_based_One-Time_Password_authentication_scheme

[6]https://www.thalesgroup.com/en/markets/digital-identity-and-security/technology/otp

[7]Three Phase Authentication Protocol for Smart Grid Communication H Goel, A Gupta, H Jain, A Khandelwal… - … IEEE Conference on …, 2019 - ieeexplore.ieee.org

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details