

LIST OF ABBREVIATIONS

S.NO.	FULL FORM	Abbreviation
1	Smart Grid	SG
2	Distributed energy resources	DER
3	Internet of Things	IOT
4	Secure Hash Algorithm	SHA
5	Intrusion detection system	IDS
6	Network-based IDS	NIDS
7	Host-based IDS	HIDS
8	Diffie-Hellman key exchange	DH
9	Secure Sockets Layer	SSL
10	Transport Layer Security	TLS
11	Virtual private networks	VPN
12	Distributed denial-of-service	DDOS
13	Authentication and key exchange	AKE
14	Central service provider	CSP

INDEX

DECLARATION	2
CERTIFICATE	3
LIST OF ABBREVIATIONS	4
INDEX	5
ABSTRACT	6
MOTIVATION	7
CHAPTER 1: INTRODUCTION TO SMART GRIDS	8
CHAPTER 2 : TECHNOLOGIES USED	9
2.1 TWINE Algorithm	9
2.1.1 Why TWINE is best encryption algorithm for IOT devices and Smart Grid Technology	11
2.2 SHA-256 algorithm	12
2.2.1 Why SHA-256 algorithm and not any other hashing algorithm	13
2.3 Salting	14
2.3.1 Why Salting and Hashing using SHA-256	15
2.4 Intrusion detection system	17
2.5 Blockchain technology	19
2.5.1 Blockchain technology and IDS	20
2.6 Diffie-Hellman key exchange (DH)	21
CHAPTER 3 : PROPOSED APPROACH	22
3.1 How our proposed model is better than other models	23
3.2 Smart Grid website interface	24
RESULT :	28
CONCLUSION :	31
FUTURE SCOPE :	32
References :	33
BIBTEX:	34
Plagiarism Report	40

ABSTRACT

A smart grid(SG) is a modernized electrical grid that uses digital technology to improve the efficiency, reliability, and sustainability of the electricity supply. It is a sophisticated system that consists of various components, including sensors, communication networks, control systems, and advanced meters, that work together to enable two-way communication and data exchange between utilities and consumers.

One of the key features of a smart grid is its ability to sense and respond to changes in electricity demand and supply in real-time. This is achieved through the use of sensors and control systems that can automatically adjust the flow of electricity to match demand, reducing the need for costly and inefficient reserve capacity.

Smart grids also have the ability to integrate renewable energy sources, such as solar and wind power, into the electricity grid. This is important because it helps to reduce the carbon emissions associated with traditional fossil fuel-based electricity generation and contributes to a more sustainable energy system.

In addition, smart grids can improve the reliability of the electricity supply by detecting and preventing power outages, and by providing alternative power sources during outages. This is achieved through the use of advanced meters, which can provide utilities with real-time information about the state of the electricity grid and help them to identify and fix problems before they cause disruptions to the power supply.

Overall, the use of smart grid technology can help to modernize and improve the efficiency, reliability, and sustainability of the electricity system, which is increasingly important as the world's energy needs continue to grow.

MOTIVATION

Smart grid authentication technology is a key component of smart grids that helps to ensure the security and reliability of the electricity supply. There are several motivations behind the development and implementation of smart grid authentication technology:

1. **Security:** One of the main motivations for working on smart grid authentication technology is to enhance the security of the electricity grid. Smart grids rely on sophisticated communication networks and control systems to enable two-way communication and data exchange between utilities and consumers. These systems are vulnerable to cyber attacks, which could disrupt the power supply and potentially cause harm to the grid. Smart grid authentication technology helps to protect against these types of attacks by verifying the identity of devices and users accessing the grid, and by providing secure communication channels to prevent unauthorized access.
2. **Reliability:** Smart grid authentication technology can also help to improve the reliability of the electricity supply by ensuring that only authorized devices and users can access and control the grid. This can help to reduce the risk of errors or malfunctions caused by unauthorized access or tampering, which can disrupt the power supply.
3. **Compliance:** Smart grid authentication technology is also important for compliance with regulatory standards and requirements, such as those related to data privacy and security. By implementing robust authentication measures, utilities can ensure that they are meeting these requirements and protecting the sensitive data that is generated and transmitted on the smart grid.
4. **Customer trust:** The implementation of smart grid authentication technology can also help to build trust with customers by demonstrating that the utility is taking steps to protect their data and the electricity supply. This can help to improve customer satisfaction and build confidence in the smart grid.

Overall, the implementation of smart grid authentication technology is important for ensuring the

secure and reliable operation of a smart grid, which is essential for the efficient, reliable, and sustainable operation of the electricity system.

CHAPTER 1: INTRODUCTION TO SMART GRIDS

An updated electrical grid known as a "smart grid" makes use of cutting-edge technology to improve power supply reliability, sustainability, and efficiency. It integrates traditional power infrastructure with communication and control technologies to enable data sharing between utilities, customers, and distributed energy sources.

Smart grids have the following key features:

1. AMI uses smart meters to collect detailed information about energy consumption and provide it to utilities and consumers in real-time. It helps utilities manage the grid more efficiently and allows consumers to monitor and control their energy consumption.
2. Demand response: Demand response programs use smart grid technology to manage demand for electricity by encouraging consumers to shift their energy use to off-peak times or to use less energy during peak times.
3. Distributed energy resources (DER): Smart grids enable the integration of DERs, such as solar panels, wind turbines, and energy storage systems, into the grid. This allows utilities to tap into locally generated renewable energy and helps to reduce the reliance on fossil fuels.
4. Grid automation: Smart grids use advanced control systems to automatically adjust the flow of electricity on the grid to maintain balance and prevent outages.

Smart grids offer a number of benefits, including improved grid reliability, increased energy efficiency, and reduced greenhouse gas emissions. They also enable the integration of renewable energy sources, which is important for addressing climate change.

CHAPTER 2 : TECHNOLOGIES USED

2.1 TWINE Algorithm

TWINE is a lightweight encryption algorithm that was developed by researchers at Mitsubishi Electric Corporation in Japan. It is designed to be fast and secure, making it suitable for use in a variety of applications, including the Internet of Things (IoT) and smart grid systems.

TWINE encrypts data in 64-bit blocks because it utilises a 64-bit block cypher. It uses a 128-bit key, which makes it resistant to brute-force attacks. TWINE also includes a number of security features, such as a key schedule, a diffusion layer, and a nonlinear layer, which help to protect against various types of attacks.

TWINE is designed to be easy to implement and efficient, making it well-suited for use in resource-constrained environments. It is also highly resistant to side-channel attacks, which are attacks that attempt to gather information about the encryption key by measuring certain physical characteristics of the device, such as power consumption or electromagnetic radiation.

Overall, TWINE is a robust and secure encryption algorithm that is well-suited for use in a variety of applications, including smart grid systems.

TABLE II. PROPERTIES OF DIFFERENT BLOCK CIPHERS

<i>Block Cipher</i>	<i>Key Size (bit)</i>	<i>Block Size (bit)</i>	<i>No. of Rounds</i>	<i>Characteristics</i>
AES	128, 192, 256	128	10, 12, 14	Excellent security, Flexible
DES	64	64	16	Not very secure but flexible
3DES	112, 168	64	48	Good security, flexible
Blowfish	32-448	64	16	Excellent security, flexible
Twofish	128, 192, 256	128	16	Can't be broken remotely
Curupira	96, 144, 192	96	96, 144, 192	Less space required to store S-boxes
PRESENT	80, 128	128	32	Less gate count, less memory, Used for encrypting small amount of data
KATAN	80	32, 48, 64	256	Hardware oriented block cipher, inefficient software implementation, consumes too much energy, low throughput

TEA	128	64	32	Security can be enhanced just by increasing the number of iterations
Humming Bird	256	16	4	Suitable for RFID tags or Wireless Sensor Network, Low power consumption, High speed
SIMON	64~256	32~128	32~2	Excellent performance, easy to implement, flexible
TWINE	80,128	64	36	Ultra-lightweight, Enough speed
LED	64, 128	64, 128	-	Efficient hardware implementation, used for transmission of RFID tags
RECTANGLE	80	64	25	Hardware friendly, faster, gives high throughput

Figure 2.1 Properties of Block Ciphers

2.1.1 Why TWINE is best encryption algorithm for IOT devices and Smart Grid Technology

TWINE is a good encryption algorithm for use in IoT devices and smart grid systems because it is lightweight, fast, and secure.

One of the main benefits of TWINE is its lightweight design, which makes it well-suited for use in resource-constrained environments, such as those found in many IoT devices. It is designed to be easy to implement and efficient, which means that it can be used in devices with limited processing power or memory.

TWINE is also fast, which is important in IoT and smart grid systems where there may be a large volume of data to be encrypted and transmitted. This can help to reduce the risk of delays or bottlenecks in the transmission of data, which is critical for maintaining the reliability of the power supply.

Finally, TWINE is secure, with a 128-bit key length that makes it resistant to brute-force attacks. It also includes a number of security features, such as a key schedule, a diffusion layer, and a nonlinear layer, which help to protect against various types of attacks.

Overall, TWINE is a good choice for use in IoT devices and smart grid systems because it is lightweight, fast, and secure, making it well-suited for these types of applications.

2.2 SHA-256 algorithm

SHA-256 (Secure Hash Algorithm 256-bit) is a cryptographic hash function that produces a fixed-size output (256 bits) from any input data. It is one of a number of cryptographic hash functions that are widely used for data integrity checks and security applications.

A mathematical function called a cryptographic hash function takes an input, or "message," and generates a fixed-size output, or "hash value," that is specific to the input. The output is often referred to as a 'digest' or 'message digest'.

One of the key features of a cryptographic hash function is that it is computationally infeasible to generate the same hash value for two different input messages. This means that if even a single bit of the input message is changed, the hash value will be completely different.

SHA-256 is widely used because it is fast and secure. It is used in a variety of applications, including password storage, digital signatures, and data integrity checks. It is also commonly used in the mining process for certain types of cryptocurrencies.

Overall, SHA-256 is an important cryptographic hash function that is widely used for data integrity checks and security applications.

2.2.1 Why SHA-256 algorithm and not any other hashing algorithm

SHA-256 (Secure Hash Algorithm 256-bit) is a widely used cryptographic hash function that is considered to be secure and efficient. There are several reasons why it is often preferred over other hashing algorithms:

1. Fixed output size: SHA-256 produces a fixed-size output of 256 bits, which makes it easy to use and compare hash values.
2. Security: SHA-256 is considered to be a secure cryptographic hash function. It is resistant to collision attacks, which are attacks that attempt to find two different input messages that produce the same hash value.
3. Speed: SHA-256 is fast and efficient, making it well-suited for use in applications where performance is important.
4. Widespread adoption: SHA-256 is widely used and supported, which makes it easy to integrate into existing systems and technologies.

Overall, SHA-256 is a reliable and secure cryptographic hash function that is well-suited for a wide range of applications. It is often preferred over other hashing algorithms because of its fixed output size, security, speed, and widespread adoption.

2.3 Salting

Salting is a technique that is used to add an extra layer of security to data that is being encrypted. It involves adding random data, called a 'salt', to the input data before it is encrypted.

The purpose of salting is to make it more difficult for an attacker to crack the encryption by using pre-computed tables of common passwords or by using other types of attacks. By adding a unique salt to each piece of data, it becomes much more difficult for an attacker to use a pre-computed table or other attack method to crack the encryption.

Salting is often used in combination with other security techniques, such as hashing, to provide an extra layer of protection. For example, a password might be salted and hashed before it is stored in a database. This makes it much more difficult for an attacker to crack the password, even if they are able to obtain the hashed password from the database.

Overall, salting is an important technique that is used to add an extra layer of security to data that is being encrypted. It helps to protect against certain types of attacks and makes it more difficult for an attacker to crack the encryption.





				
Password	p4s5w3rdz	p4s5w3rdz	p4s5w3rdz	p4s5w3rdz
Salt	-	-	et52ed	ye5sf8
Hash	f4c31aa	f4c31aa	lvn49sa	z32i6t0

Fig 2.2 Salting

2.3.1 Why Salting and Hashing using SHA-256

Salting and hashing are two important security techniques that are often used in combination to protect passwords and other sensitive data.

Salting involves adding random data, called a 'salt', to the input data before it is hashed. This helps to protect against dictionary attacks, which are attacks that use pre-computed hashes of common words and phrases to try and guess passwords. By adding a unique salt to each password, it becomes much more difficult for an attacker to use a pre-computed hash table to crack the password.

Hashing is the process of generating a fixed-size output (or 'hash value') from an input data using a cryptographic hash function. Hashing is used to create a unique representation of the input data that cannot be easily reversed or reconstructed.

SHA-256 (Secure Hash Algorithm 256-bit) is a widely used cryptographic hash function that is often used in conjunction with salting to protect passwords and other sensitive data. To use SHA-256 for salting and hashing, you would follow these steps:

1. Generate a random salt value.
2. Append the salt value to the input data.
3. Hash the salted data using SHA-256 to produce a hash value.
4. Store the salt value and the hash value in a secure location, such as a database.

The same procedure would be repeated with the entered password, and the resulting hash value would be compared to the previously stored hash value. The entered password is regarded as being correct if the two hash values agree.

Overall, salting and hashing are important security techniques that are often used together to

protect passwords and other sensitive data. SHA-256 is a widely used cryptographic hash function that is well-suited for use in these types of applications.

Password: P455WORD

Salt: 4bh1n4v

Salted input: 4bh1n4vP455WORD

Hash (SHA-256): ba43cba8b2522a3c640b5078532f5c9a3bd8267e74ab8e4dc75e56a60cfe6de5

Fig 2.3 Salting and SHA-256

2.4 Intrusion detection system

An intrusion detection system (IDS) is a security system that is designed to detect and alert administrators of possible security breaches or unauthorized access to a computer system or network. IDS systems use a variety of techniques to monitor network traffic and detect suspicious activity, such as network scans, port scans, and attempts to access restricted areas of a network.

IDS systems can be divided into two categories: host-based IDS and network-based IDS (HIDS).

Installed on a network, a network-based IDS (NIDS) keeps track of all network traffic for any unusual activities. It analyzes packets of data as they pass through the network and looks for patterns or anomalies that may indicate an attempted intrusion.

A host-based IDS (HIDS) is installed on an individual computer or device and monitors activity on that specific device for suspicious activity. It analyzes log files, system files, and other data sources on the host to detect possible security breaches.

IDS systems can be configured to alert administrators when suspicious activity is detected, or they can be set to automatically block access to the network or system in response to an attempted intrusion.

Overall, an intrusion detection system is an important security tool that helps to protect computer systems and networks from unauthorized access and potential security breaches.

Intrusion Detection System (IDS)

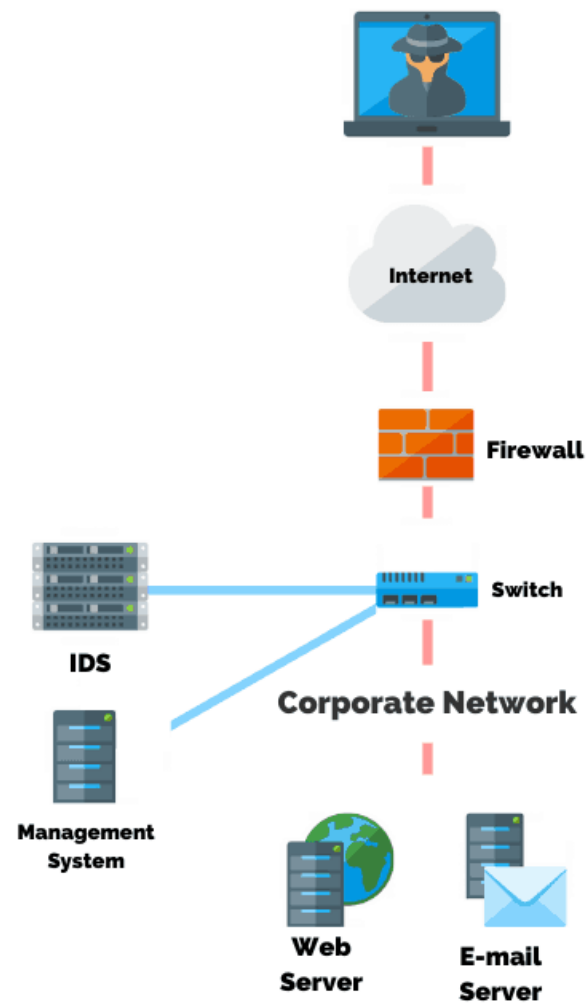


Fig 2.4 Working of intrusion detection system

2.5 Blockchain technology

Blockchain is a distributed ledger system that dispenses with the requirement for a central authority by enabling numerous parties to securely record and verify transactions. It is made up of a series of interconnected blocks, each of which contains a list of transactions.

Each block in the chain is linked to the previous block through the use of a cryptographic hash function, which allows the blockchain to maintain a secure and tamper-evident record of all transactions.

One of the key features of blockchain technology is its decentralized nature. Instead of being controlled by a single entity, a blockchain is maintained by a network of computers, known as nodes, that work together to validate and record transactions. This decentralized structure makes it difficult for a single party to alter the data on the blockchain, making it a secure and trustworthy source of information.

Blockchain technology has a wide range of potential applications, including the secure recording of financial transactions, supply chain management, and identity verification. It is also being explored for use in various industries, such as healthcare, real estate, and voting systems.

2.5.1 Blockchain technology and IDS

An intrusion detection system (IDS) is a system that monitors a network or computer system for unauthorized access or attacks. A blockchain is a decentralized, distributed ledger that records transactions on multiple computers, providing a secure and immutable record of those transactions.

One way that blockchain technology could be used in an intrusion detection system is by storing the logs of network activity on a blockchain. This would provide a tamper-evident record of all activity on the network, making it difficult for an attacker to cover their tracks or alter the log data.

Overall, the use of blockchain technology in an IDS has the potential to improve the security and reliability of the system, as well as make it more resistant to tampering or fraud. However, it is important to carefully consider the specific requirements and constraints of the IDS in order to determine if and how blockchain technology might be appropriately utilized.

2.6 Diffie-Hellman key exchange (DH)

A technique for securely transferring cryptographic keys over a public network is Diffie-Hellman key exchange (DH). It enables Alice and Bob to choose a secret key that they can both use to encrypt and decrypt messages between them.

The key exchange works as follows:

1. Alice and Bob both agree on a large prime number, p , and a primitive root, g .
2. Alice selects a secret integer, a , and calculates $A = g^a \bmod p$. She sends A to Bob.
3. Bob selects a secret integer, b , and calculates $B = g^b \bmod p$. He sends B to Alice.
4. Alice calculates the shared secret key, K , as follows: $K = B^a \bmod p$.
5. Bob calculates the shared secret key, K , as follows: $K = A^b \bmod p$.

Since the secret integers, a and b , are never transmitted over the network, it is difficult for an attacker who is listening to the communication to determine the shared secret key, K . This makes DH key exchange a secure method for exchanging keys over an insecure network.

Many cryptographic protocols, including Encrypt Sockets Layer (SSL) and Transport Layer Security (TLS), which are used to secure web connections, make extensive use of DH key exchange. It is also used in other applications, such as virtual private networks (VPNs), to establish secure communication channels.

CHAPTER 3 : PROPOSED APPROACH

We will setup smart meters in every house

Remark 1: We presume that the smart meter has a strong Physical Unclonable Function to ensure physical security.

Step 1: We will feed an inbuilt function in the smart meter that works on salted SHA-256 protocol and generates a different hashcode everytime. Our server knows the real password and the saltation that is being used

Step 2: from the User side the user requires two passwords in order to connect with our secure channel 1st is already fed in the device and the second one is the user password

We will use TWINE algorithm in order to encrypt the data and make it difficult for any hacker to intrude into our intranet

The user cannot connect to our secure channel using the normal internet they are required to connect to our network.

Not every device can connect to the smart meter. Smart meter contains a whitelist of MAC addresses that are allowed to connect

When the user is connected to our secure channel then only they can access our servers

Note : all users will be provided the passwords by Diffie-Hellman Key Exchange


An Intrusion detection algorithm will be employed in order to achieve extra security

3.1 How our proposed model is better than other models


This method of authentication is resistant to phishing attacks and cannot be compromised by a distributed denial-of-service (DDOS) attack due to the use of a captcha code on the login page. It is also difficult for an attacker to achieve hardware-level intimacy with the system and any attempt to do so would be further hindered by the use of an untamperable box to seal the hardware. Additionally, the server can only be accessed by those who are part of the network, making online cyber attacks impossible.

3.2 Smart Grid website interface

Sign up page:




Hi, Get Started




Sign up for Network

Already have an account? [Log in](#)


☐ I'm not a robot 

[Sign Up](#)

Sign in page:




Hi, Welcome Back



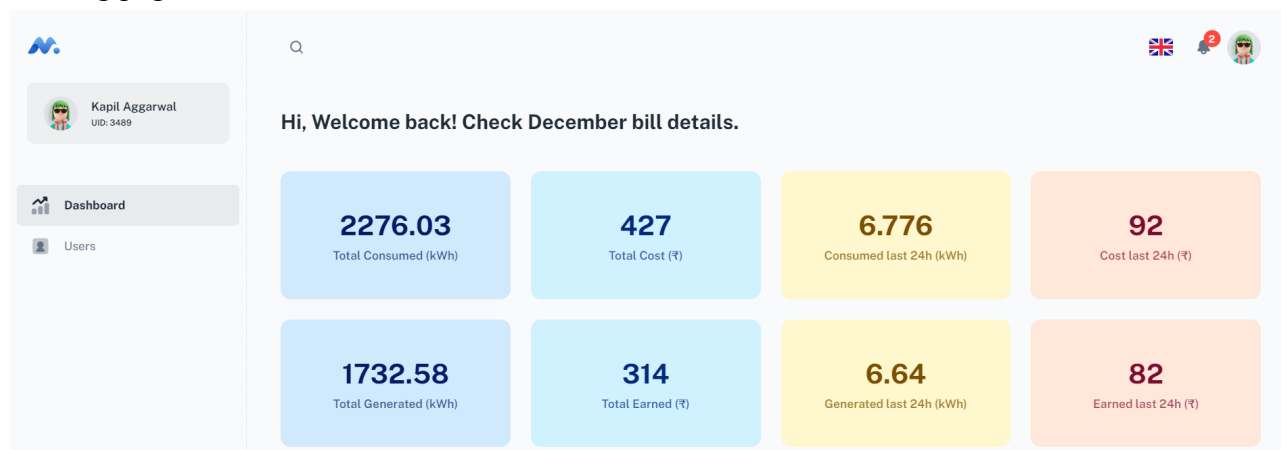
Sign in to Network

Don't have an account? [Get started](#)

☐ I'm not a robot 

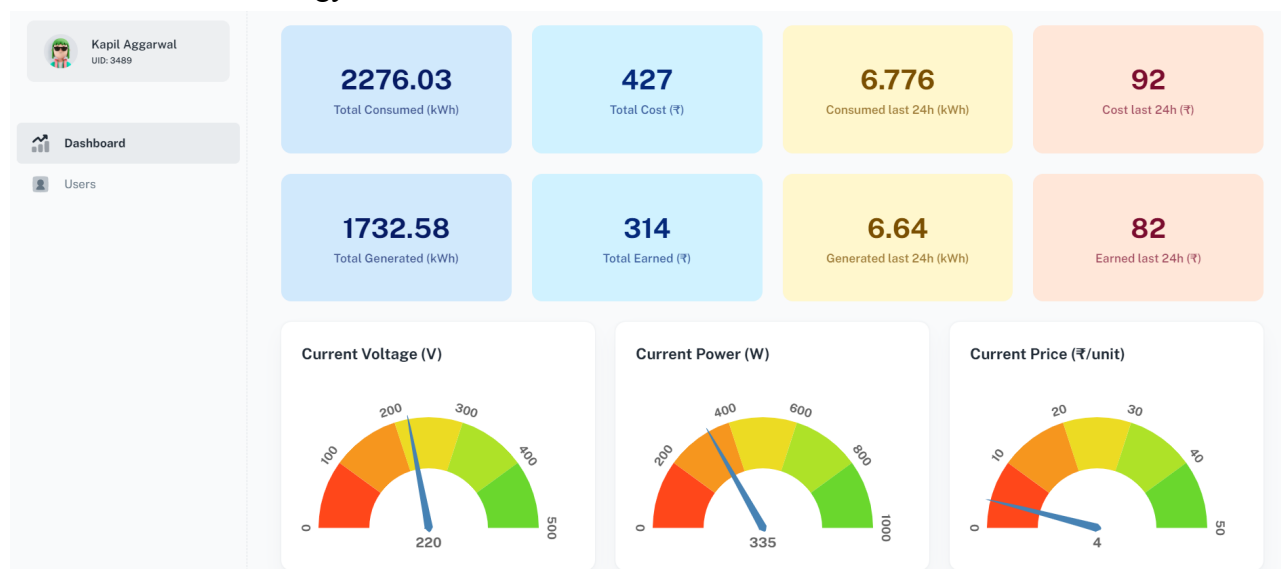
[Login](#)

Landing page:

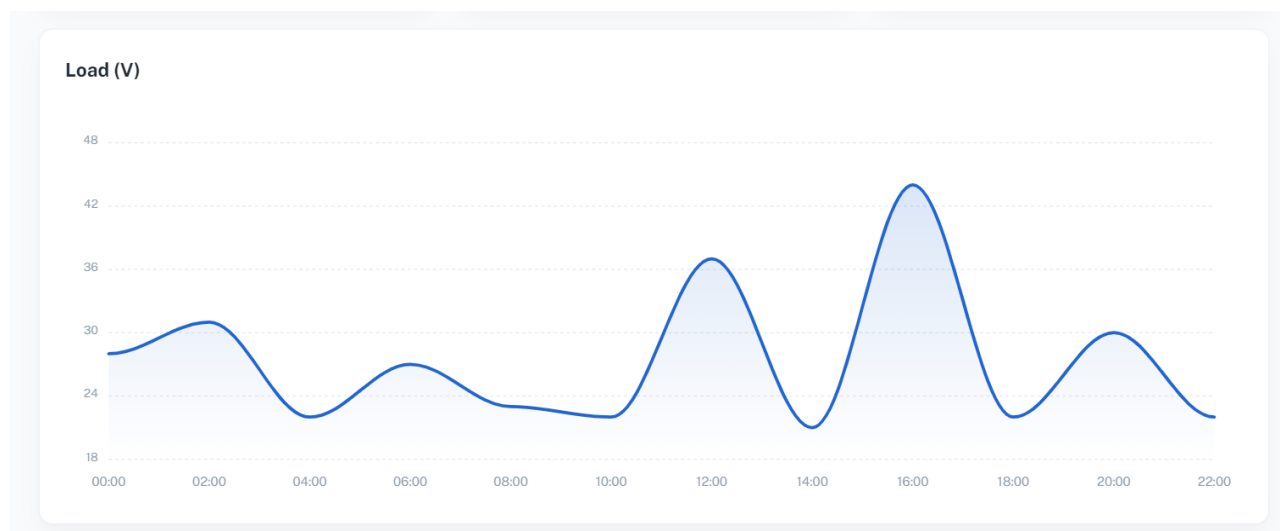


This page shows different parameters:

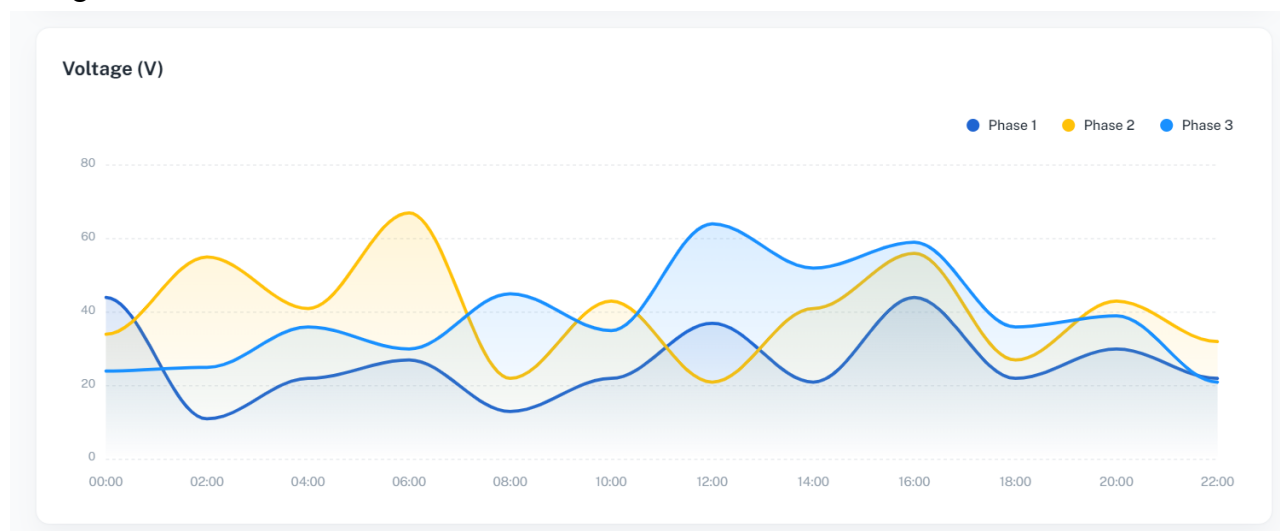
- Total energy consumed this month
- Total energy for the consumed power in this month
- Energy consumed in the last 24 hours
- Cost for the energy consumed in the last 24 hours



Load distributed on time scale:








Voltage consumed on the time scale:



Different users having access to user's network:

The screenshot displays a user management interface. On the left is a sidebar with a logo, a user profile for Kapil Aggarwal (UID: 3489), and navigation links for Dashboard and Users. The main area is titled 'Users' and features a search bar, a '+ New User' button, and a table of users. The table has columns for Name, Role, and Status. The users listed are Allison Thiel DVM (Banned), Alma Boyle (Active), Arthur Waters (Banned), Clayton Runolfsson (Banned), and Daryl Johnson (Banned). At the bottom right, there are pagination controls showing 'Rows per page: 5' and '1-5 of 24'.

<input type="checkbox"/>	Name ↑	Role	Status	
<input type="checkbox"/>	 Allison Thiel DVM	Viewer	Banned	⋮
<input type="checkbox"/>	 Alma Boyle	Viewer	Active	⋮
<input type="checkbox"/>	 Arthur Waters	Viewer	Banned	⋮
<input type="checkbox"/>	 Clayton Runolfsson	Viewer	Banned	⋮
<input type="checkbox"/>	 Daryl Johnson	Viewer	Banned	⋮

Rows per page: 5 1-5 of 24 < >

RESULT :

We compared the proposed model with the pertinent AKE schemes, including those developed for the SG system by Ashraf et al., Dariush et al., Vangala et al., Bera et al., Jangirala et al., Garg et al., and Odelu et al. To assess the effectiveness of the suggested model and the pertinent security measures, we take into account performance indicators like the computational and communication costs. We used the same hardware as the ARAP-SG Model, a Raspberry Pi-3 running Ubuntu LTS-16.4 with a quad-core CPU clocked at 1.2 GHz and 1 GB of RAM, to replicate SMy. Similar to that, a Core-i5 system with a 2.6 GHz processor, Ubuntu LTS-16.4 as the operating system, and 4 GB of RAM is used to simulate CSPz.

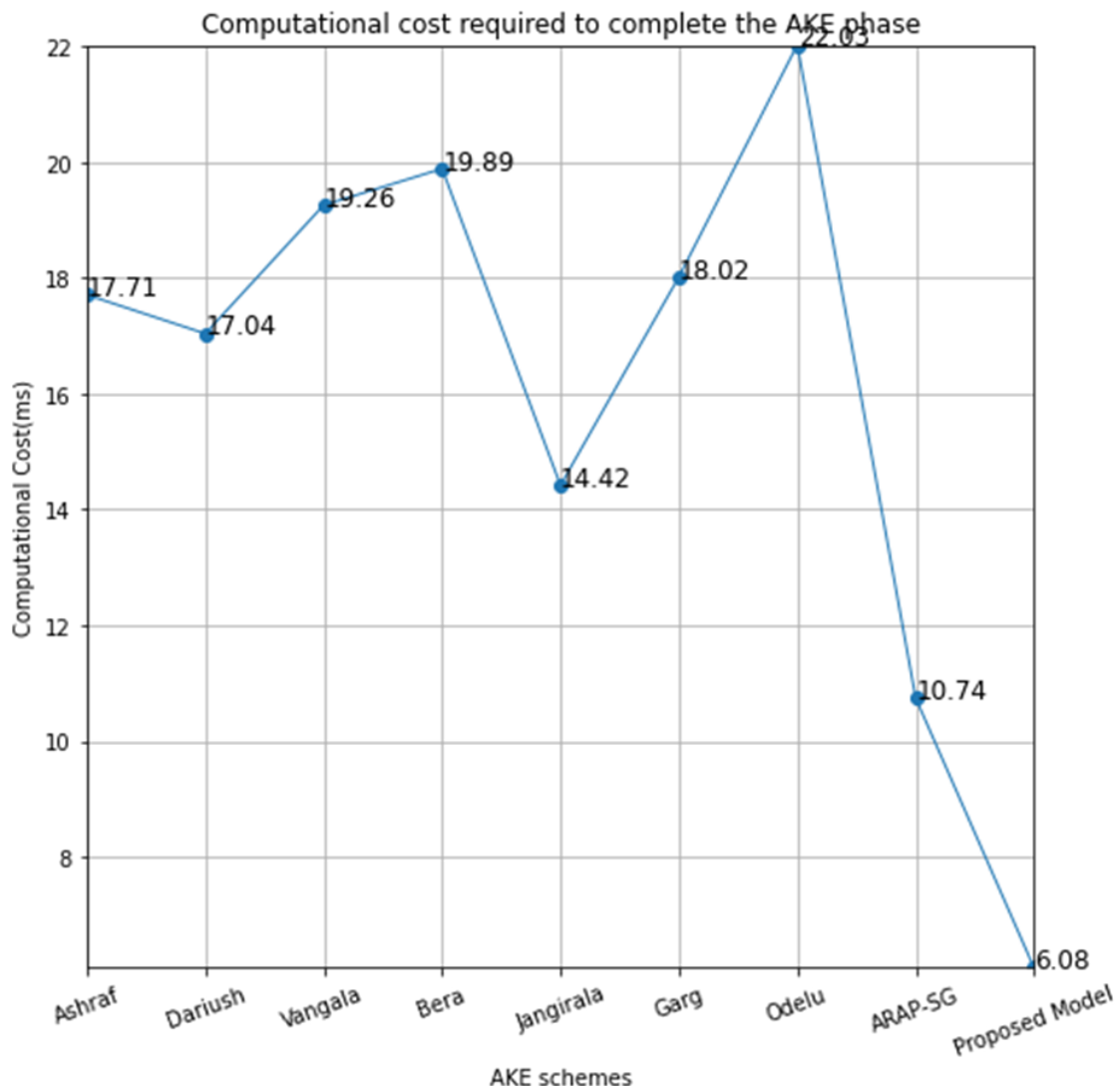


Figure 3.1

The above given chart explains the computational cost of our proposed model as compared to the computational cost of other research papers. Our model is having a significantly less computational cost which means it's really easy for our model to handle a huge user base using a significantly less powerful server system.

len(password)	len(Cipher text)
8	32
16	32
1000	32

len(password)	Computational time (sec)
8	0.85
16	0.99
32	1.03
256	1.04
512	1.12
1000	1.41
100000	4.18

Figure 3.2

Figure 3.2 shows the computational time required for processing the password of different lengths.

These passwords

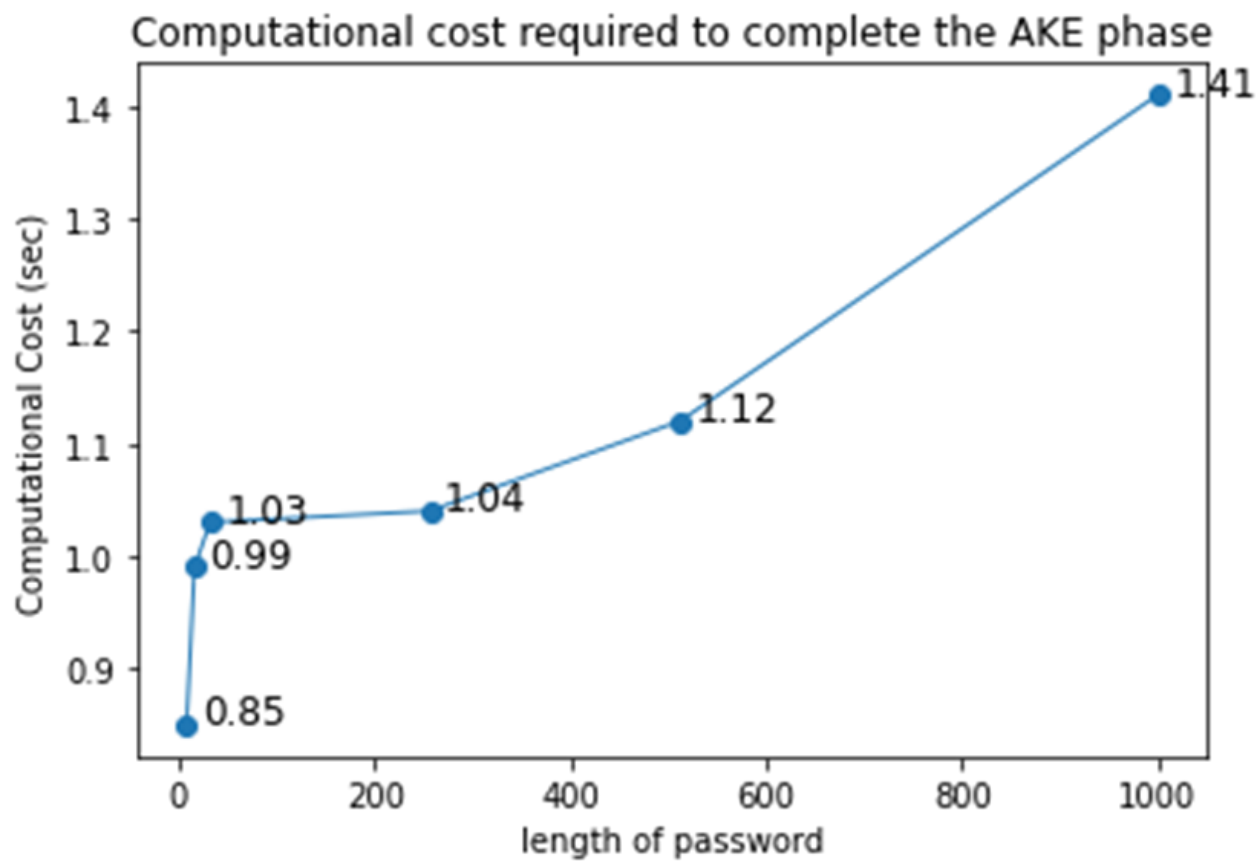


Figure 3.3

Figure 3.3 Is a Plotted Graph about the computational cost required for different length of passwords

CONCLUSION :

Internet of Things (IoT) devices frequently use an open channel to send sensitive data to a central server in the context of smart grids (SG). However, this channel is susceptible to a number of security concerns, such as information manipulation, which can impair the SG system's ability to function properly. In this study, we suggest the Secure Hash Algorithm (SHA)-based Secure Authentication and Key Exchange (AKE) protocol to safeguard the integrity of data sent between a smart metre (SM) and a central service provider (CSP) in SG systems. The proposed technique enables the CSP and SM to establish a session key following mutual authentication. We performed a ROM-based formal analysis to show the proposed protocol's security. Additionally, a preliminary security analysis revealed that the suggested protocol can withstand a number of security concerns that can impair the functionality of the SG system. In order to show how the suggested protocol has better security features while consuming less resources, we lastly compared it to an appropriate AKE protocol.

Internet of Things (IoT) devices frequently use an open channel to send sensitive data to a central server in the context of smart grids (SG). However, this channel is susceptible to a number of security concerns, such as information manipulation, which can impair the SG system's ability to function properly. In this study, we suggest the Secure Hash Algorithm (SHA)-based Secure Authentication and Key Exchange (AKE) protocol to safeguard the integrity of data sent between a smart metre (SM) and a central service provider (CSP) in SG systems. The proposed technique enables the CSP and SM to establish a session key following mutual authentication. We performed a ROM-based formal analysis to show the proposed protocol's security. Additionally, a preliminary security analysis revealed that the suggested protocol can withstand a number of security concerns that can impair the functionality of the SG system. In order to show how the suggested protocol has better security features while consuming less resources, we lastly compared it to an appropriate AKE protocol.

FUTURE SCOPE :

There is a lot of potential for further development and innovation in the field of smart grid authentication technology. Some potential areas of future research and development include:

1. **Advanced authentication methods:** There is ongoing research into the development of advanced authentication methods that can provide more secure and reliable means of verifying the identity of users and devices. These methods may include biometric authentication, such as fingerprint or facial recognition, or the use of blockchain-based systems to secure access to the smart grid.
2. **Secure communication:** Ensuring the security of communication between different components of a smart grid is essential for the overall security and reliability of the system. Future research may focus on the development of secure communication protocols and technologies that can protect against cyber threats and prevent unauthorized access to the smart grid.
3. **Integration with other technologies:** Smart grids are complex systems that consist of many different components, including sensors, control systems, and advanced meters. Future research may focus on the integration of smart grid authentication technology with these other components to create a more seamless and efficient system.
4. **Scalability:** As smart grids become more widespread, there is a need to ensure that smart grid authentication technology is scalable and can handle a large number of users and devices. Future research may focus on the development of scalable authentication solutions that can support the growing needs of a modernized electricity grid.

Overall, there is a lot of potential for further development and innovation in the field of smart grid authentication technology, which will be important for ensuring the secure and reliable operation of a modernized electricity grid.

References :

- [1] A Secure and Efficient Key Establishment Scheme for Communications of Smart Meters and Service Providers in Smart Grid
- [2] Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues
- [3] Cyber-security on smart grid: Threats and potential solution
- [4] Designing Anonymous Signature-Based Authenticated Key Exchange Scheme for Internet of Things-Enabled Smart Grid Systems
- [5] Fault-Tolerant and Scalable Key Management for Smart Grid
- [6] PALK: Password-based anonymous lightweight key agreement framework for smart grid
- [7] Correcting “PALK: Password-based anonymous lightweight key agreement framework for smart grid”
- [8] Privacy-Preserving Lightweight Authentication Protocol for Demand Response Management in Smart Grid Environment
- [9] An Identity Based Authentication Protocol for Smart Grid Environment Using Physical Unclonable Function
- [10] A Robust Access Control Protocol for the Smart Grid Systems
- [11] An Anonymous ECC-Based Self-Certified Key Distribution Scheme for the Smart Grid
- [12] Designing Blockchain-Based Access Control Protocol in IoT Enabled Smart-Grid System
- [13] Fault-Tolerant and Scalable Key Management for Smart Grid
- [14] LAKAF: Lightweight authentication and key agreement framework for smart grid network

BIBTEX:

```
@article{abbasinezhad2019secure,
  title={A secure and efficient key establishment scheme for communications of smart meters and service providers in smart grid},
  author={Abbasinezhad-Mood, Dariush and Ostad-Sharif, Arezou and Nikooghadam, Morteza and Mazinani, Sayyed Majid},
  journal={IEEE Transactions on Industrial Informatics},
  volume={16},
  number={3},
  pages={1495--1502},
  year={2019},
  publisher={IEEE}
}
```

```
@article{article,
  author = {Saklofske, Jon},
  year = {2019},
  month = {02},
  pages = {},
  title = {Playful Lenses: Using Twine to Facilitate Open Social Scholarship through Game-based Inquiry, Research, and Scholarly Communication},
  volume = {3},
  journal = {KULA: knowledge creation, dissemination, and preservation studies},
  doi = {10.5334/kula.11}
}
```



```
@article{article,
author = {Gowthaman, A. and Manickam, Sumathi},
year = {2015},
month = {01},
pages = {10921-10932},
title = {Performance study of enhanced SHA-256 algorithm},
volume = {10}
}
```

```
@article{kumar2019smart,
title={Smart grid metering networks: A survey on security, privacy and open research
issues},
author={Kumar, Pardeep and Lin, Yun and Bai, Guangdong and Paverd, Andrew and
Dong, Jin Song and Martin, Andrew},
journal={IEEE Communications Surveys & Tutorials},
volume={21},
number={3},
pages={2886--2927},
year={2019},
publisher={IEEE}
}
```

```
@article{gunduz2020cyber,
title={Cyber-security on smart grid: Threats and potential solutions},
author={Gunduz, Muhammed Zekeriya and Das, Resul},
journal={Computer networks},
volume={169},
pages={107094},
year={2020},
```

```

publisher={Elsevier}
}

```

```

@article{srinivas2020designing,
  title={Designing anonymous signature-based authenticated key exchange scheme for
Internet of Things-enabled smart grid systems},
  author={Srinivas, Jangirala and Das, Ashok Kumar and Li, Xiong and Khan,
Muhammad Khurram and Jo, Minh},
  journal={IEEE Transactions on Industrial Informatics},
  volume={17},
  number={7},
  pages={4425--4436},
  year={2020},
  publisher={IEEE}
}

```

```

@article{wu2011fault,
  title={Fault-tolerant and scalable key management for smart grid},
  author={Wu, Dapeng and Zhou, Chi},
  journal={IEEE Transactions on Smart Grid},
  volume={2},
  number={2},
  pages={375--381},
  year={2011},
  publisher={IEEE}
}

```

```

@article{khan2020palk,
  title={PALK: Password-based anonymous lightweight key agreement framework for
smart grid},

```

author={Khan, Akber Ali and Kumar, Vinod and Ahmad, Musheer and Rana, Saurabh and Mishra, Dheerendra},
journal={International Journal of Electrical Power \& Energy Systems},
volume={121},
pages={106121},
year={2020},
publisher={Elsevier}
}

@article{yu2020privacy,
title={Privacy-preserving lightweight authentication protocol for demand response management in smart grid environment},
author={Yu, SungJin and Park, KiSung and Lee, JoonYoung and Park, YoungHo and Park, YoHan and Lee, SangWoo and Chung, BoHeung},
journal={Applied Sciences},
volume={10},
number={5},
pages={1758},
year={2020},
publisher={Multidisciplinary Digital Publishing Institute}
}

@article{badar2021identity,
title={An identity based authentication protocol for smart grid environment using physical uncloneable function},
author={Badar, Hafiz Muhammad Sanaullah and Qadri, Salman and Shamshad, Salman and Ayub, Muhammad Faizan and Mahmood, Khalid and Kumar, Neeraj},
journal={IEEE Transactions on Smart Grid},
volume={12},
number={5},
pages={4426--4434},
year={2021},

```

publisher={IEEE}
}

```

```

@article{tanveer2021robust,
  title={A robust access control protocol for the smart grid systems},
  author={Tanveer, Muhammad and Kumar, Neeraj and Naushad, Alamgir and
Chaudhry, Shehzad Ashraf and others},
  journal={IEEE Internet of Things Journal},
  year={2021},
  publisher={IEEE}
}

```

```

@article{abbasinezhad2018anonymous,
  title={An anonymous ECC-based self-certified key distribution scheme for the smart
grid},
  author={Abbasinezhad-Mood, Dariush and Nikooghadam, Morteza},
  journal={IEEE Transactions on Industrial Electronics},
  volume={65},
  number={10},
  pages={7996--8004},
  year={2018},
  publisher={IEEE}
}

```

```

@article{chaudhry2021correcting,
  title={Correcting “PALK: Password-based anonymous lightweight key agreement
framework for smart grid”},
  author={Chaudhry, Shehzad Ashraf},
  journal={International Journal of Electrical Power \& Energy Systems},
  volume={125},
  pages={106529},
  year={2021},
  publisher={Elsevier}
}

```

}

@article{bera2020designing,

title={Designing blockchain-based access control protocol in iot-enabled smart-grid system},

author={Bera, Basudeb and Saha, Sourav and Das, Ashok Kumar and Vasilakos, Athanasios V},

journal={IEEE Internet of Things Journal},

volume={8},

number={7},

pages={5744--5761},

year={2020},

publisher={IEEE}

}

@article{wu2011fault,

title={Fault-tolerant and scalable key management for smart grid},

author={Wu, Dapeng and Zhou, Chi},

journal={IEEE Transactions on Smart Grid},

volume={2},

number={2},

pages={375--381},

year={2011},

publisher={IEEE}

}

@article{khan2021lakaf,

title={LAKAF: Lightweight authentication and key agreement framework for smart grid network},

author={Khan, Akber Ali and Kumar, Vinod and Ahmad, Musheer and Rana, Saurabh},

journal={Journal of Systems Architecture},

volume={116},

pages={102053},

year={2021},

```
publisher={Elsevier}  
}
```

Plagiarism Report

Smart-Grid Security

ORIGINALITY REPORT

7 %	4 %	6 %	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Muhammad Tanveer, Abd Ullah Khan, Habib Shah, Ahmed Alkhayyat, Shehzad Ashraf Chaudhry, Musheer Ahmad. "ARAP-SG: Anonymous and Reliable Authentication Protocol for Smart Grids", IEEE Access, 2021 Publication	1 %
2	www.jucs.org Internet Source	1 %
3	Alohali, Bashar Ahmed, and Vassilios G. Vassialkis. "Secure and energy-efficient multicast routing in smart grids", 2015 IEEE Tenth International Conference on Intelligent Sensors Sensor Networks and Information Processing (ISSNIP), 2015. Publication	1 %
4	www.wjscheirer.com Internet Source	<1 %
5	osp4diss.vlsm.org Internet Source	<1 %
6	Lecture Notes in Computer Science, 2005. Publication	<1 %

7	www.ijarcs.info Internet Source	<1 %
8	Wei Hu, Weiming Hu. "Network-Based Intrusion Detection Using Adaboost Algorithm", The 2005 IEEE/WIC/ACM International Conference on Web Intelligence (WI'05), 2005 Publication	<1 %
9	www.primeessayhelp.com Internet Source	<1 %
10	www.techtarget.com Internet Source	<1 %
11	www.zopper.com Internet Source	<1 %
12	epdf.pub Internet Source	<1 %
13	Jagger S. Bellagarda, Adnan M. Abu-Mahfouz. "An Updated Survey on the Convergence of Distributed Ledger Technology and Artificial Intelligence: Current State, Major Challenges and Future Direction", IEEE Access, 2022 Publication	<1 %
14	oaktrust.library.tamu.edu Internet Source	<1 %

15	"Democratizing Cryptography", Association for Computing Machinery (ACM), 2022 Publication	<1 %
16	"Security Designs for the Cloud, IoT, and Social Networking", Wiley, 2019 Publication	<1 %
17	nou.edu.ng Internet Source	<1 %
18	www.cdc.informatik.tu-darmstadt.de Internet Source	<1 %
19	Girish Ghatikar. "INTERNET OF THINGS AND SMART GRID STANDARDIZATION", Wiley, 2016 Publication	<1 %
20	Lecture Notes in Computer Science, 2003. Publication	<1 %

Exclude quotes On

Exclude matches Off

Exclude bibliography On