iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** V **Month of publication:** May 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Collective Approach towards the Multidimensional Security of the Smart Grid with Cloud Computing

Yogesh Kasar[1], Vasimraj Tamboli[2]
[1]Department of Computer Science & Engineering,Shree Yash College of Engineering, BAMU
[2]Department of Computer Technology,Dr.VVP Institute of Technology and engineering,Polytechnic,Pravara nagar.

Abstract - As a smart grid is becoming a promising technology to control and save power generation and consumption, smart grid security should be a preliminary consideration to prevent from catastrophic failures. In this paper we consider the current scenario of the existing communication network, SCADA system and the security policy of the smart grid and try to use the current existing resources in optimize way so that they can gives us a powerful solution to build the smart grid with less resources and better strategy to use the current security solution. We also consider the Cloud computation power and give a proposed solution by using the existing data of the cloud to improve the immunity of the network to combat against the vulnerability and also focused on the secrecy of the data which will be uploaded to the cloud for further use. To make this communication reliable and secure on the existing network system we recommends Time Varying encryption system (TVES), NTP (Network time protocol) along with SHAMIR'S Secret Sharing Concept.
Key Words: Smart Grid, SCADA, Cyber Security, Cloud Computing, TVES, NTP, SHAMIR'S Algorithm.

I. INTRODUCTION

According to the Electric Power Research Institute (EPRI), one of the biggest challenges facing the smart grid development is related to cyber security of systems. According to the EPRI Report, "Cyber security is a critical issue due to the increasing potential of cyber attacks and incidents against this critical sector as it becomes more and more interconnected. Cyber security must address not only deliberate attacks, such as from disgruntled employees, industrial espionage, and terrorists, but inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. Vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the grid in unpredictable ways. [1]As other industry sectors are already experienced with arming automation systems with modern IT technology, electrical power industry is also facing the trend of integrating the electrical infrastructure with information Infrastructure, which is so-called "Smart Grid". The integration brings in tremendous cost and performance benefit to the power industry, as well as arduous challenges of protecting the automation systems from security threats from hackers. So that It is important to understand what "real time performance" and "continuous operation" of a power automation system really means and to recognize that power automation systems and applications were not originally designed for the general IT environment [2].In this paper we try to discover the use of the existing resources (TCP/UDP) and also trying to use the current networking solution in optimized way to full fill the requirement of the smart grid. In this paper we discussed about the current scenario of the security and the vulnerability about the current system. We also proposed the solution to improve the immunity of the communication system using cloud computing. Also trying to make the cloud more robust for availability and confidentiality from the disaster and attack. Here we proposed some techniques to make the data transfer more robust and uses of the cloud computing to make the smart grid more cheaper in cost.

II. CURRENT CYBER SCENARIO OF THE SMART GRID

Surprisingly, it is probably not possible to implement many of today's IT security mechanisms on the existing electrical power grid. The supervisory control and data acquisition systems used for system operation, not to the computer systems used for billing. The difficulty arises because most of the devices in the electrical power system were purpose-built and do not have extra capacity to perform security functions. [3]

A. Attack By Physical Media

Malicious media or devices may be inadvertently infiltrated inside the trusted perimeter by personnel. For example, USB memory sticks have become a popular tool to circumvent perimeter defences: a few stray USB sticks left in public spaces are picked up by employees and plugged into previously secure devices inside the trusted perimeter, enabling malware on the USB sticks to immediately infect the devices. Similarly, devices used both inside and outside the trusted perimeter can get infected

with malware when outside, and infiltrate that malware when used inside. Common examples are corporate laptops that are privately used at home over the weekend. [4]

B. Attack On Common Protocols

Smart grid components will use existing protocols, inheriting the vulnerabilities on the protocols. Common protocols may include TCP/IP, and remote procedure call (RPC).[5]

C. Attack By Cyber Consequences

Malware spreading and controlling devices: An adversary can develop malware and spread it to infect smart meters or company servers. Malware can be used to replace or add any function to a device or a system such as sending sensitive information or controlling devices.

D. Attack By Network

Perhaps the most common mechanism to penetrate a trusted perimeter is through a network-based attack vector. Exploiting poorly configured firewalls for both misconfigured inbound and faulty outbound rules is a common entry point, enabling an adversary to insert a malicious payload onto the control system.[4]

E. Attack On Cloud

As more companies move to cloud computing, look for hackers to follow. Some of the potential attack vectorcriminals may attempt include

1) *Denial Of Service (Dos) Attacks:* Some security professionals have argued that the cloud is more vulnerable to DoS attacks, because it is shared by many users, which makes DoS attacks much more damaging.When the Cloud Computing operating system notices the high workload on the flooded service, it will start to provide more computational power (more virtual machines, more service instances) to cope with the additional workload. Thus, the server hardware boundaries for maximum workload to process do no longer hold. In that sense, the Cloud system is trying to work against the attacker (by providing more computational power), but actually—to some extent—even supports the attacker by enabling him to do most possible damage on a service's availability, starting from a single flooding attack entry point. Thus, the attacker does not have to flood all *n* servers that provide a certain service in target, but merely can flood a single, Cloud-based address in order to perform a full loss of availability on the intended service.
2) *Cloud Malware Injection Attack:* A first considerable attack attempt aims at injecting a malicious service implementation or virtual machine into the Cloud system. Such kind of Cloud malware could serve any particular purpose the adversary is interested in, ranging from eavesdropping via subtle data modifications to full functionality changes or blockings. This attack requires the adversary to create its own malicious service implementation module (SaaS or PaaS) or virtual machine instance (IaaS), and add it to the Cloud system. Then, the adversary has to trick the Cloud system so that it treats the new service implementation instance as one of the valid instances for the particular service attacked by the adversary. If this succeeds, the Cloud system automatically redirects valid user requests to the malicious service implementation, and the adversary's code is executed. A promising countermeasure approach to this threat consists in the Cloud system performing a service instance integrity check prior to using a service instance for incoming requests. This can e.g. be done by storing a hash value on the original service instance's image file and comparing this value with the hash values of all new service instance images. Thus, an attacker would be required to trick that hash value comparison in order to inject his malicious instances into the Cloud system. The main idea of the Cloud Malware Injection attack is that an attacker uploads a manipulated copy of a victim's service instance so that some service requests to the victim service are processed within that malicious instance. In order to achieve this, the attacker has to gain control over the victim's data in the cloud system (e.g. using one of the attacks described above). In terms of classification, this attack is the major representative of exploiting the service-to-cloud attack surface It also can be expected that the heterogeneity, diversity, and complexity of smart grid components may introduce new vulnerabilities, in addition to the common ones in interconnected networks and stand-alone microgrids. The first-ever control system malware called Stuxnet was found in July 2010. This malware, targeting vulnerable SCADA systems, raises new questions about power grid security. One by one we will discuss the above issue and will recommend the remedy action to recover from the issues we discussed earlier. First we will discuss the effect of the attacks.
3) *Side Channel Attacks:* An attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack. Side-channel attacks have emerged as a kind of effective security threat targeting system implementation of cryptographic algorithms. Evaluating a cryptographic system's

resilience to side-channel attacks is therefore important for secure system design.

4) *Authentication Attacks:* Authentication is a weak point in hosted and virtual services and is frequently targeted. There are many different ways to authenticate users; for example, based on what a person knows, has, or is. The mechanisms used to secure the authentication process and the methods used are a frequent target of attackers. Currently, regarding the architecture of SaaS, IaaS, and Paas, there is only IaaS offering this kind of information protection and data encryption. If the transmitted data is categorized to high confidential for any enterprise, the cloud computing service based on IaaS architecture will be the most suitable solution for secure data communication. In addition, the authorization of data process or management for those data belonged to the enterprises but stored on the service provider's side must be authorized by the user side (enterprises) to instead of the service providers. Most user-facing services today still use simple username and password type of knowledge-based authentication, with the exception of some financial institutions which have deployed various forms of secondary authentication (such as site keys, virtual keyboards, shared secret questions, etc.) to make it a bit more difficult for popular phishing attacks.
5) *Man-In-The-Middle Cryptographic Attacks:* This attack is carried out when an attacker places himself between two users. Anytime attackers can place themselves in the communication's path, there is the possibility that they can intercept and modify communications.[6]

III.TYPES OF ATTACKS ON SMART GRID AND ITS SOLUTIONS

Here we will discuss about the four common type of attack which can affect the smart grid operation. And these attacks are.

A. *Attacks On Devices*

A device attack aims to compromise (control) a grid device.[10] AMI is one of the key technologies required to enable several of the Smart Grid characteristics, and it plays some role in all of them. For this reason, AMI must be viewed as a foundational-enabling technology for the Smart Grid. The Open Smart Grid Users Group formed an AMI security (AMI-SEC) task force in August of 2007 to address AMI security issues. AMI-SEC recently released a Security Specification and a Security Implementation Guide10 for AMI. These documents provide useful guidance; however, the current implementations of AMI are known to have significant security issues. A recent study by Good speed et al. identified several methods for attacking wireless devices used in AMI networks. The wireless devices are used in the smart meters located on the customers' premises. Since these devices are outside the utility's physical security perimeter, they are at high risk of compromise. Good speed documented how attackers can extract data from the memory of these devices including keys used for network authentication and how the device memory can be modified by an attacker to insert malicious software. Once the device is compromised it can be used to attack other parts of the Smart Grid by communicating through the network. Attacks that originate with an AMI wireless network device can lead to direct control systems compromise.Carpenter12 also documented many vulnerabilities in AMI devices including insecure data buses and Serial connections. Because the cost of Smart Meters is low, there is no significant barrier to entry for hackers interested in attacking AMI. AMI security, as it currently stands, is insufficient to protect the national power grid from attack by malicious and knowledgeable groups.[7]

B. *Attacks On Data*

A data attack attempts to adversarially insert, alter, or delete data or control commands in the network traffic so as to mislead the smart grid to make wrong decisions/actions.[6] to avoid the same situation we recommends the TVES TVES (Time varying encryption System) with NTP (Network Time Protocol) because the electric rates are charged according to different periods, the Smart Grid Meter needs to measure time accurately. In this work, we use the NTP for Smart Grid Meter Time Synchronization. The same region of data that the SGM Slave collected is uploaded to the SGM Master. Using the same SGM Master can guarantee the consistency of time. The question lies in NTP using the Internet to transmit the power consumption data. Encryption systems are generally required to provide a fixed ID and password for authentication. User authentication is a necessary security element in the open network environment, and the use of simple authentication information has major problems. One problem is that it is easy for attackers to guess passwords because users select their ID and password as information that is easy to memorize and to guess. In this research, we propose the Time Varying Encryption System to solve this problem. Let's see how it will protect the system

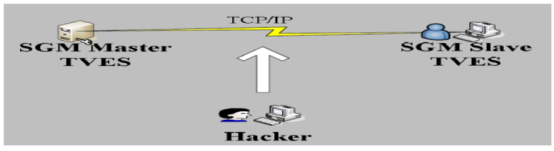


Fig 1 Attempt by hacker for the key

Decryption condition of TVES is like the following:

The hacker must get the timestamp packet of the SGM Master.

The hacker needs to run NTP in order to obtain the timestamp of the real time.

The hacker must be in the same subnet-mask network as the SGM Master.

The hacker cannot collect and analye network packets for decryption. The hacker must know the encryption method, but the encryption method (TVES) changes once every second.

If internal personnel divulge a secret, the 4 conditions described above are met. The hacker already knows to use Caesar to encrypt and has analyzed the Caesar encryption table (*A~Z, a~z, 0~9* and *!@#$%*). The content and sequencing of the Caesar encryption table all need to be the same as those of the SGM Master.

Even if all the preceding are right, the hacker needs to divide by the Time factor to obtain the correct measurement value. The encryption method changes once every second, so the hacker needs to finish the analyzing and code-breaking of the encryption method (TVES) in 1 second. The clock rate of the CPU is 3G Hz at present. Using the Brute-force attack method (Brute force attack: The attacker tries every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained.) requires at least 30 seconds. The computational process result is like the following. The conclusion is that it is impossible to code-break TVES with the Brute-force attack method. [8]

C. Attacks On Privacy

Private information by analyzing electricity usage data. In smart grid, electricity usage information is collected multiple times per hour by smart meters so as to obtain fine-grained information about the grid status and improve grid operation efficiency.[8] The dealing with single cloud providers is becoming less popular service with customers due to potential problems such as service availability failure for sometime and malicious insider attacks in the single cloud. So now single cloud move towards multiclouds, interclouds or cloud of clouds. We apply multi clouds concept using Shamir's Secret Sharing algorithm that reduce risk of data intrusion and loss of service availability for ensuring data.

1) *Data Integrity*: To maintain our data in cloud computing, it may not be fully trustworthy because client doesn't have copy of all stored data. To deal with this problem we can use the concept of multicloud concept and can also reconstruct the data later by the same.
2) *Data Intrusion*: Attacks on systems and data are a reality in the world we live in. Detecting and responding to those attacks has become the norm and is considered due diligence when it comes to security
3) *Service Availability*: Service availability is most important in the cloud computing security. Amazon already mentions in its licensing agreement that it is possible that the service might be unavailable from time to time. The user's web service may terminate for any reason at any time if any user's files break the cloud storage policy. In addition, if any damage occurs to any Amazon web service and the service fails, in this case there will be no charge to the Amazon Company for this failure. Companies seeking to protect services from such failure need measures such as backups or use of multiple providers. [9]

A concerted effort by the entire industry, the research community, and the policy makers is required to achieve the vision of a secure smart grid infrastructure. The electric grid is arguably the world's largest engineered system. Vital to human life, its reliability is a major and often understated accomplishment of humankind. It is the motor of the economy and the major driver of progress.[4] So that a small flaws in the system can make a tremendous loss to the economy. So we can try to make the system as robust as possible.

V. PROPOSED STRATEGY SECURED CLOUD BASED SMART GRID WITH EXISTING NETWORK

As we discussed about the security of the smart grid and we also talk about how to make this more strengthen so that it cannot be easily hack or which is invulnerable to attack like brute force and dictionary. We want to make our smart grid with existing network in which no need to make a new infrastructure to make communication of the smart meter and the substation and ultimately with the power plant. In our model we proposed a primary cloud which replaces the chain of the wireless communication device like Wi-Fi, ZigBee etc with existing broadband network. Here we consider every home has it broad band network along with electricity. So that no needs to develop extra communication infrastructure for the same. And a secondary

cloud will make communication with the various power plants and provide the essential data to the substation. So that with the existing networks. We are fulfilling the communication requirement of the smart grid.

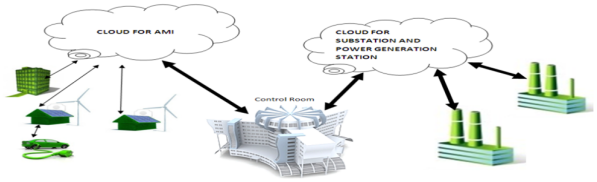


Fig 2. Cloud based communication of the smart grid

Now question comes to exist that if smart grid will use the existing communication network it will more vulnerable to attack and data can be tampered so what to do for the same. So we proposed some solution by which we can try to make it secure and hard to tamper the valuable data. In fig 2 we shows the cloud based infrastructure to maintain the data to reduces the chain of communication devices.

VI. OUR PROPOSED STRATEGY FOR STRENTEN THE SMARD GRID FROM VULNARABILITY USING CLOUD

Our proposed system gathered all the data about the attack and vulnerability from all the system from which it is connected and on the analysis of the gathered data the system is able to take decision and also combat to these type of attacks also update other system which are attached to the same system. If the nodes are connected to the cloud and any of the nodes detect the attack. It sends this log to the cloud and expert will find the remedy action on the attack and also update to every node connected to the system to combat against same type of attack. We can say the immunity of the system get stronger as it gets stuck by the attacks.

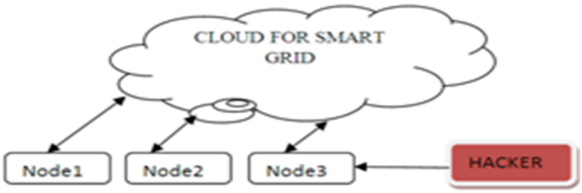


Fig 3.Cloud with gathered data inteligence

Inferring anomaly requires event construction using temporal detection. Correlation techniques by a temporal approach can be used to learn from characteristics of events. A combination of transaction-based models with combined hidden Markov mode land feature-aided tracking has been proposed to detect asymmetric patterns Enhancement of the previous frame work is required for two reasons :

Cyber infrastructure can be accessible by multiple users at different locations and there remains the possibility of simultaneous attacks upon multiple substations

There may be other combinations of cyber-attacks upon substations and the resulting impact is not captured or observed

In the below fig the highlighted portion can be replace with our above proposed solution for the better immunity of the network[11]. This is also called fusion centre. The fusion centre uses the collected information or previous data from each node to infer the malicious activities in smart grid communication network. More interestingly, knowing the existence of the defense mechanism, a smart adversary should manage to disguise its intention while accomplishing its attack. Conversely, the fusion center attempts to make the precision of attack inference as high as possible to reduce the network damage The fusion-based defence mechanism is specified as follows.

A. Vulnerability Attack

This type of attack is induced by the malfunction of a device or communication channel, or the desynchronization of feedback information Feedback information may be deteriorated by erroneous data delivery or unreliable channel conditions, which leads to an incorrect control process at the control centre. To handle the same situation we proposed the TVES system which we

discussed in section III(b)

B. Intentional Attack

If an adversary is able to have full understanding of the network topology, it can fully utilize the network structure to disrupt the network operations by paralyzing some fraction of nodes with the highest degree, known as intentional attack . Intentional attack can be implemented via coordinated denial-of-ser- vice (DoS) attack and contributes to network disruption due to node disconnections in the communication network. To tackle this problem we suggest the different cloud with different architecture in section V. Where we uses two cloud which are made by clouds and handle the data transmitted by Residential and Comercial zone. A fusion-based defense mechanism is proposed to defend intentional attack by utilizing the feedback information from each node for attack inference and defense reaction.[12]

Now we are try to give the answer to the questions we asked in section VI. To make the system more robust and available we can use TVES, Cloud Computing, Fusion Center and Shamir's Algorithm together so that the transmission of the data will be secured by TVES and the cloud will reduces the chain of the devices to transfer the data. We are going to answer the third question and that is. Is our data secured in others hand ? To answer this question we will not send the whole data to any cloud instead we split the data using Shamir's algorithm and reconstruct the data when needed even one of the cloud is not available at that time.

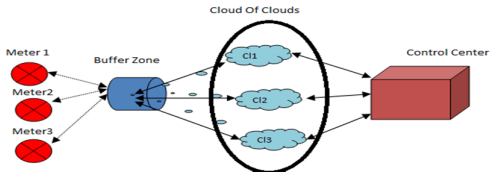


Fig 3. Proposed Multidimentional Security of the Smart grid data.

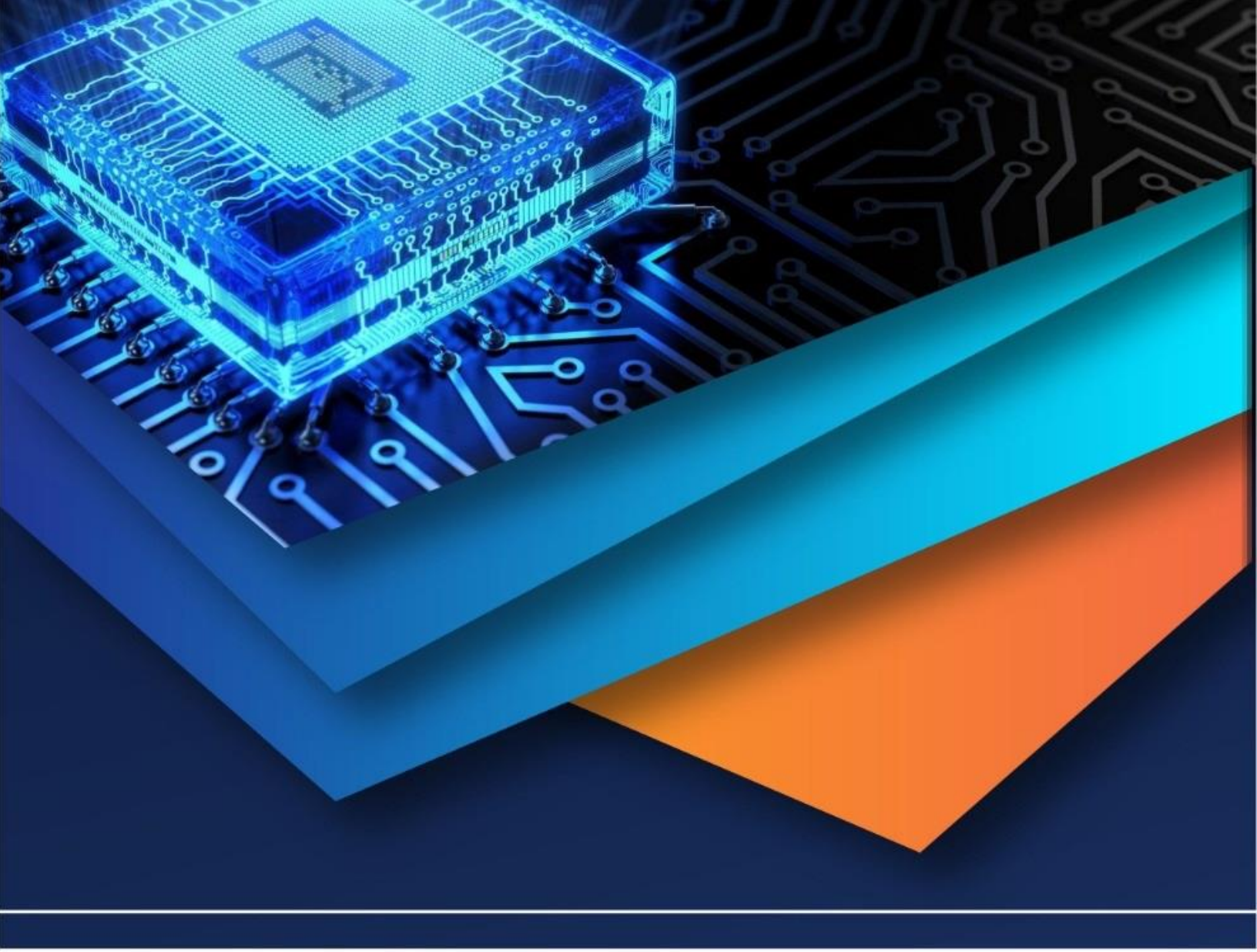
In Fig 3 we showing our proposed model where data transmitted by the meters are encrypted by TVES system and to avoid the bottleneck we shows the buffer zone where shamir's algorithm splits the data and send it to different no of cloud which have different vendors and architecture too.Once the data is stored it can be retrived by the control center when required even one of the cloud is not available.

VII. CONCLUSIONS

The purpose of this work is to show the recent trend on SMART GRID using single clouds and multi-clouds. Here we try to make the smart grid using existing resources and proposed the model using secret sharing algorithm and cloud. The algorithm we used "SHAMIR'S" generate their own secret sharing schemes and use secure channels using TVES to distribute data among themselves. The Shamir's secret sharing algorithm has a good abstract foundation which provides an excellent framework for proofs and applications. We also focused on the low cost infrastructure to transmit the data to the control center instead of using wireless data transmission devices chain.

REFERENCES

[1] Anthony r. Metke, randy l. Ek ," Security Technology for Smart Grid Networks " , IEEE Transactions on Smart Grid, Volume:1 , Issue: 1 , June 2010.
[2] Dong Wei , Yan Lu , " An integrated security system of protecting Smart Grid against cyber attacks", Innovative Smart Grid Technologies (ISGT), 2010
[3] Clements .S, Kirkham. H , " Cyber-security considerations for the smart grid" , Power and Energy Society General Meeting, 2010 IEEE
[4] NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, August 2010.
[5] Ajey Singh, Dr. Maneesh Shrivastava, "Overview of Attacks on Cloud Computing" , International Journal of Engineering and Innovative Technology (IJEIT)Volume 1, Issue 4, April 2012.
[6] "Study of Security Attributes of Smart Grid Systems - Current Cyber Security Issue" , U.S. Department of Energy, Idaho National Engineering and Environmental , April 2009.
[7] Te-Kwei Wang , Fan-Ren Chang , "Network Time Protocol Based Time-Varying Encryption System for Smart Grid Meter " , Parallel and Distributed Processing with Applications Workshops (ISPAW), 2011 Ninth IEEE International Symposium on , 26-28 May 2011
[8] Md Kausar Alam, Sharmila Banu K , "An Approach Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds" , International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013.
[9] Xu Li, Inria Lille, "Securing Smart Grid: Cyber Attacks, Countermeasures, and Challenges" , IEEE Communications Magazine ,August 2012.
[10] Chee-Wooi Ten, Junho Hong , "Anomaly Detection for Cybersecurity of the Substations " , Smart Grid, IEEE Transactions on (Volume:2 , Issue: 4), Dec. 2011.
[11] Pin-Yu Chen, Shin-Ming Cheng, "Smart Attacks in Smart Grid Communication Networks", IEEE Communications Magazine , August 2012



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY