International Journal of Engineering, Science and Mathematics (UGC Approved)
Vol. 8 Issue 5, May 2019,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijmra.us, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Secure and Fault-tolerant Advanced Metering Infrastructure

Prof. Meenu Jeemon v n jeemon, Prof. Zol Ramdas Madhukar, Prof. Katyarmal Pooja, Prof. Hugar Niranjan Shivasharanappa, Prof. Rawale Pournima Pradip

Dattakala Shikshan Sanstha "Dattakala Group of Institution" Swami-Chincholi, Daund, Pune,

Maharashtra 413130. India.

***Abstract*—**A smart grid consists of several digital functions that transform the grid into an intelligent system. One of the main components of a smart grid is Advanced Metering Infrastructure (AMI). AMI helps to acquire data from Interface Energy Meters (IEMs) that are geographically dispersed in substations. AMI includes interface energy meter, data hub, IT infrastructure and various communication tools for meter data transmission, such as Power Line Communication Carriers (PLCC), Fiber Optics, Very Small Aperture Terminal (VSAT), GSM/GPRS/3G/4G, etc. The current meter data profile, event profile, load profile and billing profile are used for load and renewable energy forecasting, planning, power outage management, power system planning and efficient power network management. Any failure/error in AMI components will cause data unavailability. The communication between the IEMs and the control center is vulnerable to various communication channel attacks such as meter attack, authentication attacks, Man-In-The-Middle (MITM) attacks, response attacks, etc. High availability, reliability and data integrity of the meter is the need of the hour for effective management of power systems. The proposed solution helps to achieve fault tolerant AMI through highly secure communication between IEMs and control centers while maintaining interoperability..

Keywords— Interface Energy Meters, Advanced Metering Infrastructure, DLMS/COSEM protocol, high availability, communication security

I. INTRODUCTION

The Indian power grid is divided into 5 regional grids for its operation and planning. Initially, the inter-regional grid was planned for the exchange of operations within the regional boundaries. Due to the limited exchange of operations within the inter-regional grid transmission capacity was unable to enhance. To enable the transmission of surplus power among states the regional links were established. In the year 2013 December 31st the regional grids were connected and became the national grid with the aim of 'One Nation – One Grid – One frequency'. Because of the Synchronization of all regional grids, the transmission facilities were available to meet the demand by ensuring the 24x7 supply of electricity. In the last few years, there has been a huge improvement in transmission networks. The strong and highly integrated transmission system has enabled the development of the electricity market
resulting in the momentum of the growth of the power sector [1].

International Journal of Engineering, Science and Mathematics (UGC Approved)
Vol. 8 Issue 5, May 2019,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijmra.us, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Penetration of Renewable energy sources and distributed energy sources to the power grid is growing rapidly which leads manifold increase in intra-state, inter-state and inter- regional and transnational electrical energy transactions [2]. Bulk energy transactions whether from renewable energy sources or conventional sources require efficient scheduling, measurement of energy imports/exports, billing and settlement of energy transactions, which are required to be handled by load dispatch centers. Meter data help for load dispatch centers for efficient scheduling, load/renewable forecasting, energy accounting, outage management, real-time deviation monitoring, billing and settlement of the transactions.

Meter Data Acquisition System (MDAS) [3] is the part of the advanced metering infrastructure (AMI) for automatically collecting meter data from substation interface energy meters and transferring the data to a central database for the power system operations. This technology is mainly used by utility providers for monitoring the real-time and also to predict future consumption or generation based on the received current and historical data. Real-time meter data information helps both the utility providers and customers for better use of electric energy. AMI technology includes meters, data concentrator units, wired and wireless network components like radiofrequency devices, Power-line communication carriers, GSM/GPRS/3G/4G, Optical fiber networks and IT infrastructure at the control center. Fault/error in the AMI system leads to the unavailability of meter data, which in turn leads to cascading effects on power system operations. Communication between meters and control center is also vulnerable to various attacks. High availability, reliability and integrity of meter data is the need of the hour for load dispatch centers for efficient management of the grid. This paper focuses on meter data acquisition from sub-stations Interface energy meters, which is required for load dispatch centers.

The rest of the paper is organized as follows. Section 2 discusses the AMI system and possible faults for data loss. Section 3 discusses meter data communication protocols and their vulnerabilities. Section 4 discusses the secure and fault- tolerant AMI system and Section 5 ends with the conclusion.

II. GENERAL ARCHITECTURE OF AMI SYSTEM

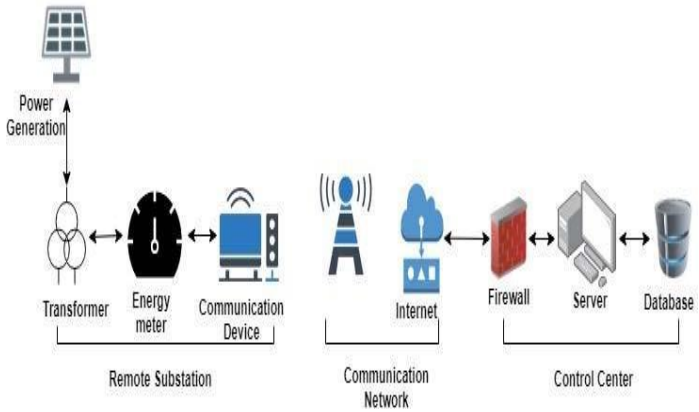

Fig. 1. Architecture diagram of AMI system

The general architecture diagram of the AMI System is shown in Fig.1. Smart energy meter shall support association requirements, various parameters list, advanced security profile, on-demand data services, push data services and firmware upgrade services and features [4][5]. Transformer operated HV/LV consumer meters shall comply with the D-3 category parameter list. Transformer operated Boundary/Bank/Ring/Availability Based Tariff meters shall comply with the D-4 category [4] parameter list. The parameter list contains various profiles like instantaneous profile, block load profile, daily load profile, billing profile, event profile, nameplate profile, and programmable parameters [4].

The Data Concentrator Unit/Communication device is installed at each and every sub-station, which acts as an interface between control centers and sub-station IEMs. Based on the configuration provided by the control center, DCU acquires data and status from IEMs in defined periodic intervals and sends it to control center and similarly receives control commands like time synchronization, connect/disconnect, configuration changes, firmware upgrade, etc. from the control center and executes on IEMs.

DCU collects data from IEMs over Ethernet and sends it to the control center. Various communication mediums used in the AMI system is GSM/GPRS, Power-line carrier communication (PLCC), Optical Fiber Communication (OFC), wired internet, radiofrequency, etc. This acquired data at the head-end system helps in monitoring energy flows in the grid network which helps in energy auditing, monitoring, decision support, customer energy usage, billing, tamper and outage detection, and notifications.

Various faults in AMI systems like communication network failure, DCU failure, and Head-end system failure may lead to loss of real-time meter data. The communication between the meters and the control center is vulnerable to various attacks; those are discussed in section 3. Data loss and communication attacks lead to cascading effects on power system operations. The proposed system helps to increase the high data availability, detect where the failure occurred, and also helps for secure communication between IEMs and control center.

International Journal of Engineering, Science and Mathematics (UGC Approved)
Vol. 8 Issue 5, May 2019,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijmra.us, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

III. METER DATA COMMUNICATION PROTOCOL AND ITS VULNERABILITIES

Both software and hardware have to work in harmony to bring the grid to stability. The power system has classified the meters into Class A, Class B, and Class C meters [4]. Interface Energy Meters are the smart meters that consist of hardware and embedded software. IEM places a crucial role in grid operations. The IEMs are smart electronic devices that record the information at defined intervals based on the standard protocol. Device Language Message Specification (DLMS) standard communications protocol is used in the AMI system.

DLMS/COSEM (Companion Specification for Energy Metering) [5] is an interface model and communication protocol for meter data exchange. The three-step approach (Modeling, Messaging, and Transporting) is followed in this standard. DLMS/COSEM protocol communication between meter (server) and client consists of 3 phases i.e. application association (AA) establishment, data exchange, and AA release. During association establishment, authentication and access right to various objects will be decided between server and client. As per standard No security, Low-Level Security (LLS), and High-Level Security (HLS) are the three different kinds of authentication mechanisms that are available with various authentication levels.

A. DLMS/COSEM –Association

This section discusses the vulnerabilities of TCP variant of DLMS protocol. As per protocol, an association is the first step of meter data communication. Authentication happens during the association connection establishment phase as shown in Fig.2 [5].

1) DLMS – no security authentication: In this profile, the meter doesn't require any authentication for association establishment from the client. Due to this any unauthorized client/attacker can establish an association with the meter and collects the limited meter details like nameplate profile [9][10]. similarly, In monitoring direction, the attacker can perform a reply attack with spoofing of meter IP address and can respond to legitimate meter clients[6].

2) DLMS – Low-level security authentication: In LLS, the server requires the client to authenticate itself by supplying the password known by the server. Here the clients provide the secret password in plain text format to the server during the association establishment. If the password is valid then the server accepts the association connection. Meter data communication can be captured using various network traffic monitoring software and can retrieve the secret password. This secret password can be used by an attacker for association establishment and meter data exchange. In another way, an attacker can gain the password by using a brute force attack. Once the attacker gains access can get all instantaneous profile, block profile, load profile, nameplate profile, billing profile and event profile of meter[6].

In monitoring direction, the client doesn't require any authentication from the meter for association confirmation.Due to this, an attacker can spoof meter IP, perform reply attacks, and can confirm the association establishment.

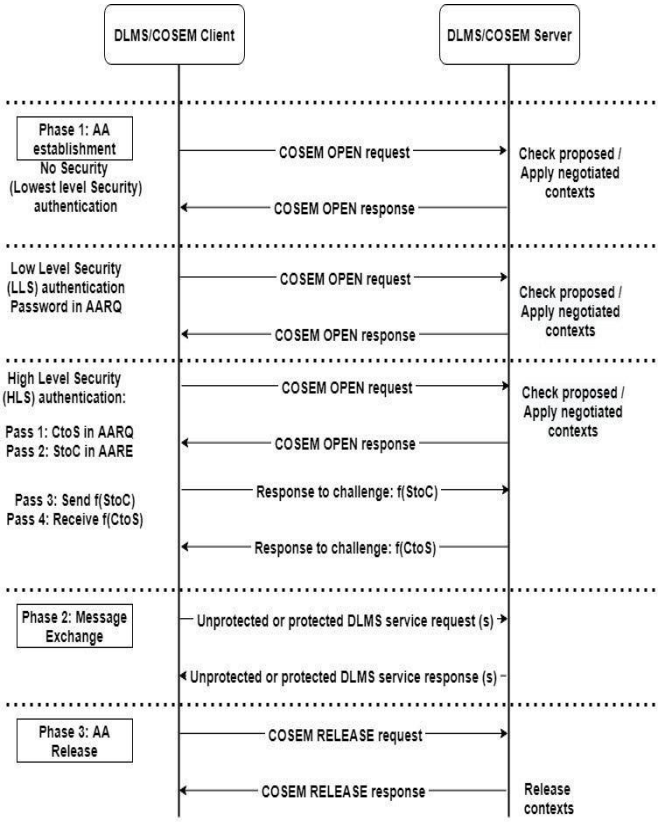

Fig. 2. DLMS/COSEM authentication mechanisms

B. DLMS/COSEM – Data Exchange

Data communication between meter and client is either in plaintext format or ciphertext format. Plain text communication is easy to understand and intercept the meter data by an eavesdropper which leads to a confidential problem. Attacker, who successfully launches a man-in- middle attack with the knowledge of protocol information can modify/tamper the meter data which leads to data integrity problems[11].

IV. SECURE AND FAULT-TOLERANT METER DATA ACQUISITION SYSTEM

The proposed solution helps to achieve a secure and fault- tolerant AMI for load dispatch centers for efficient management of the power system.

A.Fault-tolerant system

In this system, the communication between the control center and the substation is established using wired and wireless dual communication modes. In the wired mode, the use of OFC is recommended for better reliability, in case of unavailability of OFC, wired internet can be used. Wireless communication is GSM/GPRS/4G used in this system. The wired network acts as a

primary mode of communication, and GSM/GPRS acts as a secondary mode of communication. In case of failure of the primary communication the secondary mode of communication overtakes for meter data communication.

The proposed system uses two data concentrator units (DCU) at the substation end for collecting data from multiple interface energy meters and sends it to the head-end system of main and backup control centers. Fig.3 shows the secure and fault-tolerant advanced metering infrastructure. Fig.4 shows the fault-tolerant IT infrastructure of power system operations [2][12]. Fault-tolerant DCU (2 DCUs) works on the principle of the master-slave model. One DCU acts as a master another acts as a slave. Master DCU executes all monitoring and control commands received from the control center, whereas slave DCU executes the only monitoring requests. Both DCUs simultaneously collect data from substation energy meters and sends it control center. When DCU receives time synchronization, firmware update, etc. control commands from the control center, only master DCU performs the control actions on meters, whereas the slave DCU doesn't handle controlling commands. Both DCUs are interconnected over serial/Ethernet for exchanging health signals, watchdog information continuously. Whenever master DCU fails, slave DCU acts as a master and the same information updates to the control center. The internal architecture of fault-tolerant DCU is shown in Fig.5.

In the AMI system, the meter acts as a server and the DCUs acts as a client. In this model, the DCU makes the request to the meter based on the configuration provided from the control center. Both DCUs have the same configuration information. The configuration consists of the details of the meter like meter communication port, communication protocol, protocol version, periodic updating interval, various profile information, etc. The configuration file also includes the security information to access the data and type of data to be accessed like load profiles, instantaneous profiles, or billing profiles. This configuration also contains details of the control center and backup control center communication details for needful data transfer.

At the substation, all the interface energy meters are connected to DCU using the Ethernet switch. In this system, the DCU establishes communication based on the configuration information provided by the control center. Before accessing the data from the meters, DCU establishes a secure connection with the control center to acquire the control configurations which are used to access the data from the meters. The connection established between the DCU and Control center is a secure connection which is achieved by adding the SSL/TLS layer [13][7][8] on top of the TCP/IP connection. After receiving the configuration from the control center the DCU establishes the communication with meter based on the standard communication protocols. After acquiring the data from the meters the DCU stores a copy of data at the local substation system and also sends the data to the control center using the wired and wireless communication modes. The DCU also sends a copy of data to the backupcontrol center to avoid the data unavailability in case of primary control center failures.

International Journal of Engineering, Science and Mathematics (UGC Approved)
Vol. 8 Issue 5, May 2019,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijmra.us, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

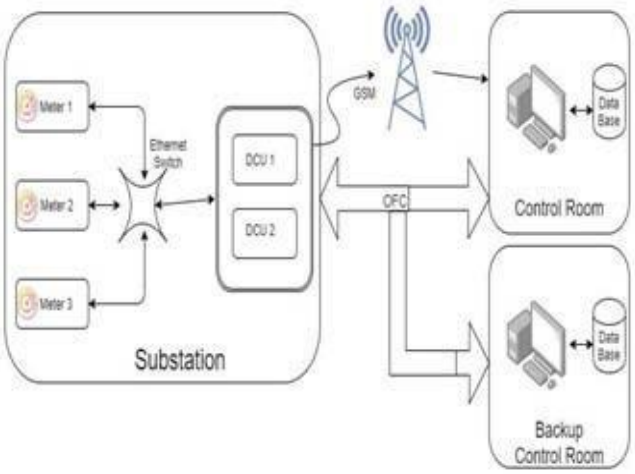

Fig. 3. Secure and Fault-Tolerant AMI

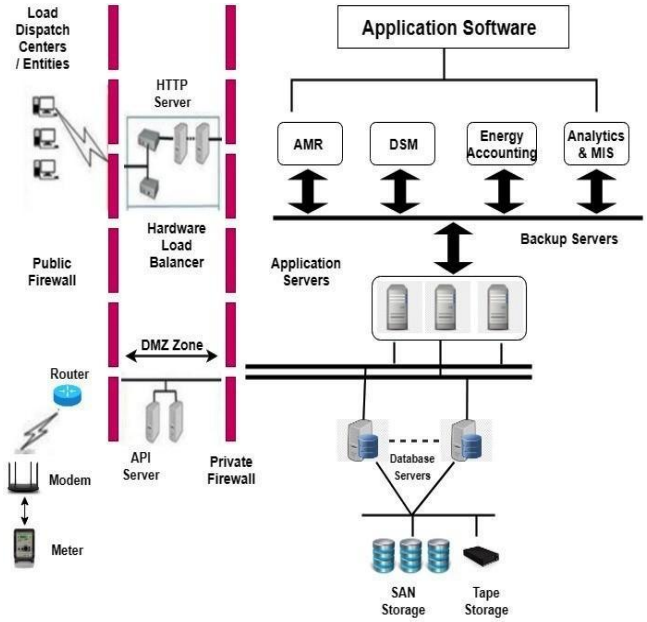

Fig. 4.Fault-tolerant IT Infrastructure Architecture

AMI Health monitoring system at the control center helps the operator regarding the status of the meters, the health of wired and wireless communication modes, and the status of fault-tolerant DCU as shown in Fig.6. The Health monitoring system helps to identify an early diagnosis of problems like is DCU, Communication, IT infrastructure running in fault- tolerant mode, or not. If the system diagnoses any problems, self-healing actions will be performed automatically and the same updates to the operators for further any actions.

International Journal of Engineering, Science and Mathematics (UGC Approved)
Vol. 8 Issue 5, May 2019,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijmra.us, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

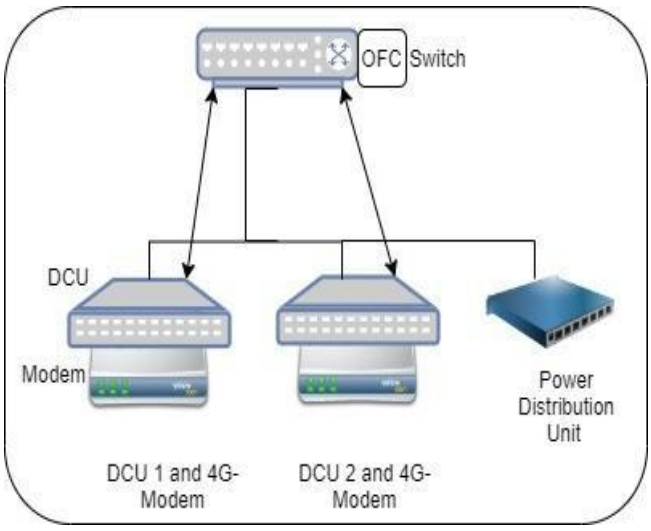

Fig. 5. Internal Architecture of fault-tolerant DCU

B.High Secure communication

Authentication between client and meter happens during application association. To avoid various authenticated issues in No security, LLS authentication mechanisms, it is recommended to use High-level security (HLS) authentication mechanism which is shown in Fig.2 [5] and various processes are shown in Table. I. This HLS mechanism helps in mutual authentication between meter and client using a challenge- response mechanism. After the successful application association between the client and meter, the service request by the client will be processed depending upon the access rights and responses provided to the client. The challenge-response mechanism and data exchange communications are protected based on the security context chosen during the association establishment phase.

DLMS Security suites are shown in Table. II [5]. Security suite id 2 is used for higher security in the AMI system. AES- GSM-256 authenticated encryption is used for cryptographic protection of the information to achieve confidentiality and authentication. This can be combined with the compression technique. Elliptic Curve Digital Signature Algorithm (ECDSA) is used for message integrity. DLMS/COSEM provides a set of keys to be used for the encryption of the data. It also provides the key management procedure i.e. key transfer, key agreement, and key wrapping. The security setup class provides various methodologies that must be followed by the client in achieving key management; it also provides the certificate management methodologies which the client must follow in import, export, deletion, creation of the digital certificates. The public key infrastructure (PKI) in the green book [5] discusses the certification authorities (CA), sub certification authorities (Sub-CA), and the end entities. Table.III is illustrated with various experiments conducted on the proposed AMI system and events/results obtained and Fig.6 shows the event monitoring system at the control center.TABLE I. AUTHENTICATION PROCESS IN HLS

International Journal of Engineering, Science and Mathematics (UGC Approved)
Vol. 8 Issue 5, May 2019,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijmra.us, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Authentication Mechanism	**Pass 1: C->S**	**Pass 2: S->C**	**Pass 3: C->S f(StoC)**	**Pass 4: S->C f(CtoS)**
	AARQ	AARE	XX.request Reply to HLS Authentication	XX.response Reply to HLS authentication
Mechanism Id (2) HLS	CtoS: Random String 8-64 octets	random String 8-64 octets	Man. Spec.	Man. Spec.
Mechanism Id (3) HLS			**MD5** (StoC || HLS || Secret)	**MD5** (CtoS || HLS || Secret)
Mechanism Id (4) HLS			**SHA-1** (StoC || HLS || Secret)	**SHA-1** (CtoS || HLS || Secret)
Mechanism Id (5) HLS	CtoS: Random string 8-64 octets Optionally: System-Title-C in calling-AP-title	StoC: dom string 8-64 octets Optionally: System-Title-S in responding-AP-title	SC || IC || **GMAC** (SC || AK || StoC)	SC || IC || **GMAC** (SC || AK || CtoS)
Mechanism Id (6) HLS			**SHA-256** (HLS Secret || System Title-C || System Title- S || StoC || CtoS)	**SHA-256** (HLS Secret || System Title-S || System Title-C || CtoS || StoC)
Mechanism Id (7) HLS ECDSA	CtoS: dom string 32-64 octets Optionally: System-Title-C in calling-AP-title, Cert-Sign-Client in calling AE-qualifier	StoC: Random string 32-64 octets Optionally: System-Title-S in responding-AP-title, Cert-Sign-Server responding AE-qualifier	**ECDSA** (System Title-C || System Title-S || StoC || CtoS)	**ECDSA** (System Title-S || System Title-C || CtoS || StoC)

International Journal of Engineering, Science and Mathematics (UGC Approved)
Vol. 8 Issue 5, May 2019,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijmra.us, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

TABLE II. DLMS/COSEM SECURITY SUITES

Security Suite Id	Security Suite Name	Authenticated encryption	Digital Signature	Key Agreement	Hash	Key Transport	Compression
0	AES-GCM-128	AES-GCM-128	-	-	-	AES-128 key wrap	-
1	ECDH-ECDSA-AES-GCM-128-SHA-256	AES-GCM-128	ECDSA with P-256	ECDH with P-256	SHA-256	AES-128 key wrap	V.44
2	ECDH-ECDSA-AES-GCM-256-SHA-384	AES-GCM-256	ECDSA with P-384	ECDH with P-384	SHA-384	AES-256 key wrap	V.44

Event Category	DCU Name	Meter Name	Date Time
Connection closed from meter	DCU_1	METER_1	2020-08-11 21:35:31
Data not received from meter	DCU_1	METER_1	2020-08-11 21:25:38
Data not received from meter	DCU_1	METER_2	2020-08-11 21:25:36
Connection closed from meter	DCU_1	METER_2	2020-08-11 21:25:35
Primary Control Center Failed to Receive the Data	DCU_1	METER_2	2020-08-11 20:23:56
Primary Control Center Failed to Receive the Data	DCU_1	METER_2	2020-08-11 18:41:34
High Level Security Pass 3 fail - unauthorised client	DCU_1	METER_2	2020-08-11 18:37:04
connection failed due to wrong AARQ association	DCU_1	METER_2	2020-08-11 18:35:04
HLS Level 7 ECDSA Request	DCU_1	METER_2	2020-08-11 18:29:04
HLS Level 2 Request	DCU_1	METER_2	2020-08-11 18:29:04

Fig.6: AMI Event monitoring systemTABLE III. SIMULATED EXPERIMENTS ON AMI SYSTEM

V. CONCLUSION

AMI is one of the important and key components of a smart grid. The Meter data plays a key role in scheduling, renewable, and load forecasting, outage management, deviation settlement, billing, and various other operations related to the efficient management of the grid. This meter data helps in efficient accounting of electrical energy injected/drawn by each stakeholder and helps to improve discipline in the grid system. The proposed fault-tolerant and secured meter data acquisition system addresses high availability problems by using fault- tolerant DCU, redundant communication networks, fault- tolerant IT infrastructure, and AMI health monitoring system. High secure communication achieved in AMI through challenge-response mechanisms, authenticated encryption, digital signatures, and key management as per DLMS/COSEM security suite identification number 2.

REFERENCES

[1] https://www.powertoday.in/News.aspx?nId=iiqS5/Em1nMxwSV1Z+tY ow==

[2] Forum of Regulators - Report on Scheduling, Accounting, Metering and Settlement of Transactions in Electricity (SAMAST)
Dated: 15th July 2016
http://www.forumofregulators.gov.in/Data/WhatsNew/SAMAST.pdf

[3] Dodla, Sidhartha, LagineniMahendra, KattaJaganmohan, RK Senthil Kumar, and B. S. Bindhumadhava. "Wireless Real-time Meter Data Acquisition System." In TENCON 2019-2019 IEEE Region 10 Conference (TENCON), pp. 997-1002. IEEE, 2019.

[4] IS 15959 Part-1, Part-2 and Part-3: DATA EXCHANGE FOR ELECTRICITY METER READING, TARIFF, AND LOAD CONTROL — COMPANION SPECIFICATION

[5] Companion Specification for Energy Metering "DLMS/COSEM Architecture and Protocols – Green Book Edition 8.1"

[6] SidharthaDodla, LagineniMahendra, KattaJaganmohan, R.K.Senthil Kumar, B.S.Bindhumadhava "Secured Automatic Meter Reading for Implementation of SAMAST framework in India" ISUW2020- 6th international conference and Exhibition on smart grids and smart cities- preprint

[7] IEC 62351-5 security standard

[8] IEC 62351-3 security standard

[9] Luring, N., Szameitat, D., Hoffmann, S., and Bumiller, G., 2018, February. Analysis of security features in DLMS/COSEM: Vulnerabilities and countermeasures. In 2018 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT) (pp. 1-5). IEEE.