

## Implementation of a Group-Based Verification Mechanism for Secure M2M Communications

\* B. Satyanarayana Murthy<sup>1</sup>, Dr. L. Sumalatha<sup>2</sup>

Associate Professor<sup>1</sup>,

BVC Engineering College<sup>1</sup>

Professor of CSE<sup>2</sup>

University College of Engineering<sup>2</sup>,

JNTUK Kakinada<sup>2</sup>

Andhra Pradesh.

**Abstract:** The M2M communication is a technology that can use both reliable and unreliable communication mechanism. We propose an efficient and group based strict verification mechanism for machine-to-machine (M2M) networks. The smart objects in a M2M networks are able to gather and enrich a wide variety of information from a resource constrained environments. And are also interacting with the components in a unconstrained environment without human involvement. The proposed scheme is used to allow any group of smart objects in an M2M environment authenticates mutually by sharing a common secret element (key) for exchanging information in a protected manner. The verification method purely based on mutual agreement among the smart objects/M2M nodes in an environment and there is no involvement of any service provider. The authentication process is coordinated among the smart objects and the gateway with the supervision of the service provider. The proposed mechanism requires the smart objects can obtain a secret session key generated by the service provider and group identity. Using this information, any smart object can authenticate with the gateway and with other objects in the network at home location as well as foreign location. The scheme uses only secret keys and there is no involvement of public keys. Hence it is suitable for resource constrained devices. The proposed scheme is also verified by using SPIN logic, a widely used verification tool.

**Index terms :** Group based authentication, M2M networks, secret key cryptosystem, key exchange, mutual authentication.

### I. INTRODUCTION

With the huge scarcity of communication trends, the rising M2M systems are going to interconnect most of the constrained devices in the internet world [1]. The consistent smart devices are enthusiastic to tale their locations and situations and are capable of barter information amid each other robotically with no direct people's involvement. Mainly three chief categories of the machinery to make three layers in connected things [2]. One category of the mechanism is a collection of connected devices to outline an ecological layer. Another category is the smart device that can sketch a examine layer. Finally, the organizer form the control tier. The chief task of the ecological tier in a connected world is to accumulate and pass on the ecological data over the inter-tier network without human involvement. The purpose of the ecological tier in a connected world would be implemented by Machine-to-Machine (M2M) communication or Machine-Type-Communication (MTC), where things together with sensors smart exchange data to everyone by using equally wireless and wired modes of communication. A M2M messaging mechanism includes the following hidden components: 1) An M2M constrained local network with connecting gateways, 2) A messaging group component plus connecting mediums and 3) An

appliance services field having of the last part holders and applications mandatory in the connected world [3].

An M2M message system of a connected world contains a hardly any flaw that shows the M2M unprotected [4]. Mainly, in an M2M message scheme, the main messaging intermediate is the radio, that is simply unsecure. Next, the smart objects, which are in general useless, have partial functioning in expressions of both transmission and calculation capacity in the M2M message environment. Hence, they are simply eavesdropped and composite protection mechanisms may not be possibly utilized to guard them. Finally, the interconnected mode of a M2M communication system combines both wired and wireless medium for the data transmission to the hub network with variety of protection mechanisms, which raises a protocol break among diverse messaging mechanism and might be a probable hazard to the M2M messaging system. The on top of specified features of the M2M messaging system has missing the scope for various wicked unethical activities to damage the entire environment. Hence to discover the possible ways to efficiently guard the M2M messaging process.

An efficient verification idea has been planned in [5] in order to clean fake information of any M2M messaging system. The system is intended to stop the node defeating threats; they may not be identified because it occurs if a device is gone to sleep mode. The scheme is incorporated for accommodating adjacent filtering mechanism depends on network routers. in the scheme, if a compromise M2M device passed fake information to a network gateway, the bogus information can be clean if any one protected adjacent node involving in the coverage. Though, the mechanism has not shown in order to secure the scheme from attacks.

A new mechanism adopted for a radio mechanized verification and confirmation of the M2M connected devices networks has been defined in [6] by means of the offered verification property of a wireless machinist. They expand the typical Generic Bootstrapping Architecture (GBA) adapted in the 3GPP stipulation to employ their clarification. By the result, the manager node authorizes itself to the wireless operator and obtains key material. The distributed key matter is after that used to protect the rest of transmission among the synchronizing nodes and the M2M host.

An easy structural drawing of the M2M examination has been projected in [7] to hold up an submission in a infirmary with the thought of the movement of hospital personals. A competent safety system with active authentication based on identity has been proposed in the present architecture. The projected idea uses pair wise key pre-distribution to set up a key between the mobile node and a sensor node. Then the device utilizes a go-ahead ID-Based authentication and collision-resistant hash function, to authorize the basis of the flare signal earlier than sensor nodes forward their together data to the mobile node. The safety study proposed that the planned system might endure the imitation defeats because the practice by the vibrant ID. However, the device has a fault to without difficulty reveal the IDs of the

sensors nodes and the mobile nodes. Motivated to progress the safety working in the M2M transmission by means of a great deal more vigorous authentication mechanism, in the proposal, a time - variant-cipher verification among mobile nodes and the M2M service provider (MSP) and a reciprocated verification among the mobile nodes and sensor devices with small cost have been considered and officially confirmed. Our hand-outs completed in this paper can be combined as mentioned. (1) A time variant cipher algorithm has been projected to jointly validate mobile nodes and the MSP. (2) A time variant key creation device which uses an original key material and a kernel to produce a one time key with less computation. Further, the height of protection can be familiar by altering the occurrence of early key resources updating. (3) A simple cipher mechanism has been deployed to protect the information communicated among the communicating entities.

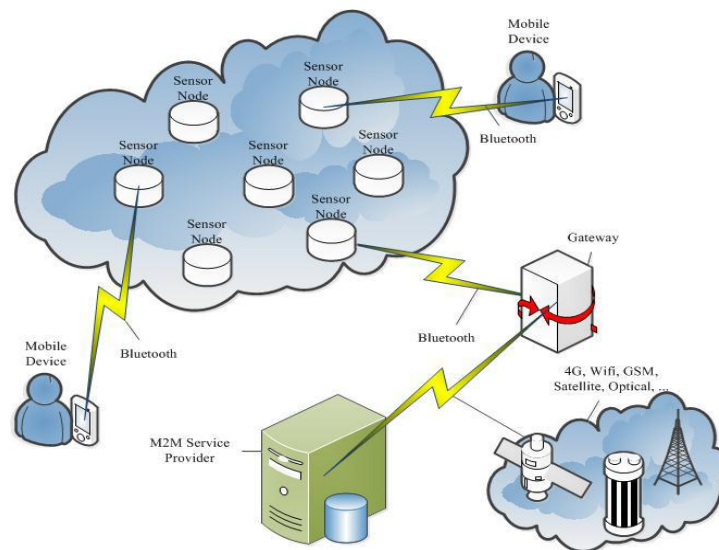


Fig. 1 M2M System Model

Cyber-physical systems (CPS) are intentionally prearranged substantial systems which are included, synchronized, proscribed and monitored in the computing environment. Propagation of IoT is accountable for the materialization of IoT environment so that the in sequence from various associated perspective can be controlled and coordinated among geographical areas along with calculation dimensions. The IoT made a basis for CPS. For extensive distance far-off constrained nodes, M2M is careful a gifted surrounded move toward for IoT. The globe have been completed slighter by IoT, though, a break still forms among our substantial globe and the connected globe. In the close to future, this gap will disappear and all objects in the connected world will be linked with the network.

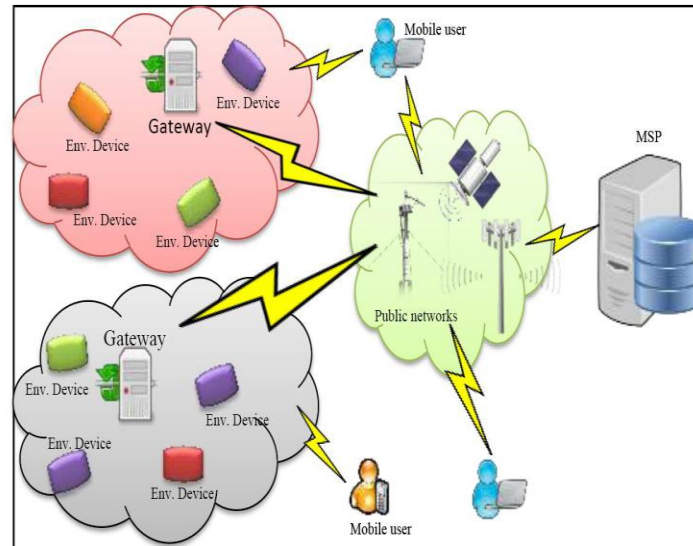


Fig. 2 M2M networks cyber physical systems

Based on [10], CPS combined of different major mechanisms. (i) Ecological layer, a collection of connected devices. (ii) The examiner layer contains a collection of actuators. (iii) Controllers layer. Data is composed obtained sensors from surroundings. This data is forwarded to the scattered connected devices in the internet world for dispensation. Once data is processed, the connected devices use the actuators to raise the operational commands. Similar actions and advice creation are started by the actuators to entail on the substantial scheme. With these steps, CPS is capable to achieve self-consciousness, auto-configuration and decisions [11]. M2M messaging is the method to execute the purpose of the ecological layers of CPS. In M2M, nodes and other devices converse with each one using transmission medium. The message scheme of an M2M comprises of different layers those are linked mutually [12], [8]. The Figure 1 contains, (i) Connecting devices, denoting M2M area layer to. (ii) Message association layer. (iii) application specific users . Because, remote nodes are more often than not found distant in unavailable or prohibited regions, also probable that the sensors nodes could be hazard by physical attacks and reproduced. For example, the application software may be tainted by exact destructive codes, which might vary or create future lively data. Also, the sensor nodes might carry out byzantine disruptiveness following to life form defeated. Thus, the data sent by far-off detecting sensor nodes must be confirmed. Otherwise, far-off users on the other plane would get modified data and therefore respond incorrectly. The M2M distant/ecological devices are organized and restricted with the help of M2M Service Provider (MSP). This thing also performs muster of various elements and manages setup/system of the scheme parameters. In M2M, as the scheme mostly interacts with machinery, the verification schemes are certainly dissimilar from predictable verification. Many presented verification

schemes assume that the devices to be authenticated are humans. Hence, password dependent verification and methods are not appropriate and incompetent in the framework of M2M verification.

## II. RELATED WORK

Li and Xiong projected an encryption mechanism to afford safe communication among the connected devices in a constrained environment allowing for the over-the-air communication network as a fraction of the connected devices [13]. The privacy-preserving aggregation method provides one to figure above the ciphered data without the decipher key, to be confined, each smart meter protects the usage data and only the provider can view their aggregation with the related key, but others can't view it without the key held by each smart meter. The capable mechanisms contain homomorphism encryption [14], [15] and secret sharing [16]. Newly, a fundamental ring architecture and hierarchy structure are planned to conceal a sole meter's custom data and compilation time in [17] and [18], in that order, in which the electric utilization in sequence of a assured area is sent to the power organization center as a substitute of the custom data of a single smart meter. To gather the necessities of communication latency and huge amount of messages, a secure message transmission framework for smart grid was projected in [19], where the session keys are communal among smart meters with the Diffie-Hellman (DH) key agreement protocol [20]. In [21], a key organization system is anticipated using symmetric key and elliptic curve public key mechanism to oppose the man-in-the-middle attack and the replay attack. To observe the power generated by smart grid more perfectly in the real world scenario, an genuine communication scheme was proposed in [22] to attain active attack discovery and message origin authentication. The authentication scheme assures that each one of the smart meter's data is obtained timely and securely transmitted to the management center. Still, the storage complexity in the above scheme cannot be disused. To be more appropriately, we suppose that every 12 minutes a smart connected meter gathers the consumed electricity information, i.e., each day 120 reports require to be sent to the grid by the connected smart meter. For secret transmission of all the reports, the present scheme intended that the connected smart meter build a 7-level Merkle hash tree (MHT) [23] with 128 at most leaf nodes, and is used to authenticate the origin of the message with the corresponding authentication path information (API). The only 120 APIs are to be added with the encrypted form of 120 power usage reports, all the 128 APIs are kept in the connected smart meter as well as the outstanding 32 APIs for the critical necessitate. Since each API includes of 7 outputs of a 128-bit secure hash function, the storage space charge of a grid connected smart meter in a day is 14 KB. Further, if the grid connected smart meter gathers the consumed data every 5 minutes to get real time consumption of electricity; the storage complexity of a smart meter in a day is 72 KB. The grid connected smart meters own limited storage space resources, such as the 8 KB RAM and 120 KB Flash memory set in [22], it is intolerable to put so a great deal storage resource on the APIs. Furthermore, the scheme cannot reach the two way authenticated communication since the hash of API is one-way.

So many other origin authentication schemes like [24],[25] have been published for various types of applications. The scheme proposed in [26] is a proposal to clean out unwanted information in the M2M communication system. This scheme is more efficient and also uses limited bandwidth. Even though, the scheme offers protection against passive defeats which are untraceable because, the negotiation happens while the nodes obtain idle mode, the method does not state the shield of the scheme defeats similar to imitation, replay defeats, etc. In [27], using presented verification mechanism in constrained environments; a new mechanism has been projected for verification in connected devices. The scheme development really enhances the presented mechanism design of general bootstrapping, available in the 3G project stipulation. The manager node obtains the desirable encryption/decryption keys by identifying themselves to the connected devices service provider. The rest of data transmission among the M2M host and the synchronizing node is done by utilizing the pre-shared secret keys. The scheme also does not address the weakness to dissimilar defeats in the M2M transmission. Another novel scheme for healthcare management systems for M2M networks has been addressed in [28]. The approach deals with the medical applications in which the stakeholders are moving. Where, they suggested authentication scheme based on identity. The approach uses a pre-key sharing among the sensor devices and the mobile nodes. However, analysis shows that the mechanism is unable to resistant to denial of service attacks and re transmissions. Another disadvantage is the simple exposé of the identities communicating entities. The approach proposed in [2] did not address at designing a specific scheme. They suggested an official design in an effort to build a general structure for the study of the protection and verification schemes for connected devices. Four simple schemes were projected to undertake dissimilar attacks. However, the structure does not include the particulars of any exact verification mechanism, any precise function and the matching defeats. The work proposed in [29] was mainly focused on resistance to intermediate attacks. The protocol also guards the data protection of other devices and entities which are not part of the matter of the communication. The scheme proposed in [1], depends on ciphering model, collective with key swap mechanisms and identity based key exchange mechanism. The method is capable to endure the majority of the famous attacks; however, the system requires the objective sensors node and mobile nodes to execute compute costly cryptographic parameters. It needs a sensor node to achieve numerous bilinear coupling actions by elliptic curve ciphers in adding up to various point multiplications and power operations. These calculation necessities are not enough for devices with very partial resources. The planned mechanism does not depend on any public key infrastructure. The projected method can perform verification and authentications in a constrained environment with the ciphering and deciphering techniques. These calculations are tremendously simple when compared to other cryptosystems.

### III PROPOSED SCHEME

As described in Fig. 2, there are four major entities in the projected mechanism as mentioned: (i) Machine-to-Machine service provider (*MSP*), it is used to register the entities and performs initial housekeeping operations. (ii) Physical connected nodes (iii) Connected devices (mobile devices), which have restricted resources and are able to communicate with other devices or sensor nodes. (iv) Communication framework (Gateways), which offers the authentication mechanism among mobile devices or sensor nodes. There should be at least one of such framework in every M2M network. Some of the sensor nodes are directly communicate with the gateway, and the others can connect via a mobile device or other sensor node. Here the assumption is the *MSP* is a trusted entity and it provides all the confidential parameters required to offer authentication. Moreover, the mobile nodes and sensors can move from its home location to foreign location anytime and can communicate with other mobile nodes or sensor nodes.

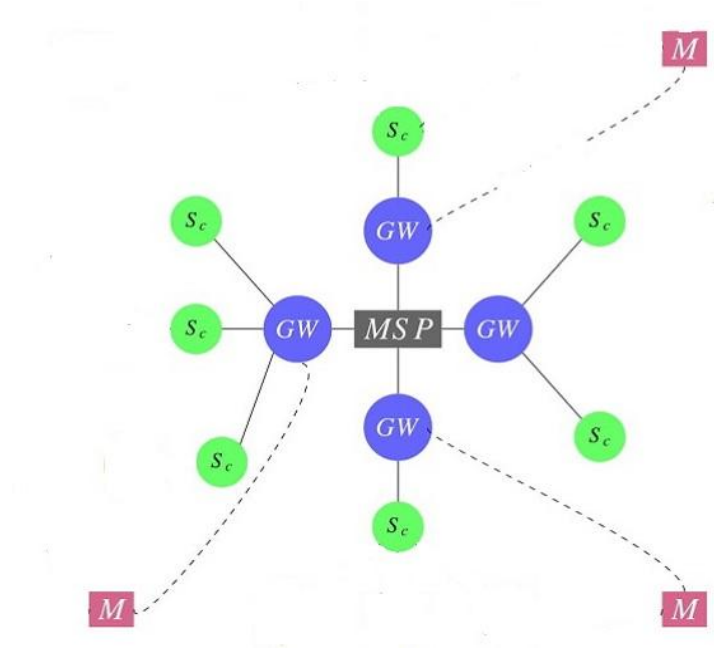


Fig. 3 M2M Architecture for the proposed scheme.

In the proposed mechanism, a mobile node can approach a *MSP* to get his identity and the master secret key for further communication with the other mobile users or sensor nodes in constrained environments. After successful registration with *MSP*, the mobile node can move from location to other location randomly in the M2M communication networks and using the obtained base security key it is capable to verify itself among gateways with the supervision by the *MSP*. Once a mobile node verifies with the foreign location gateway, it can mutually authenticates any other sensor nodes or a group of mobile nodes registered with the same gateway in the network. The sensor nodes no need to attach with the gateway

while authentication process. And also, the sensor nodes may authenticate mutually at any time and are able to transfer messages. The group of sensor nodes and mobile devices can authenticate at a time with each other without connecting to any communication gateway. At any point after successful registration and initial parameter setting, there is no need of MSP.

The following are the basic phases in proposed model for authentication of devices in a M2M communication networks.

- Phase I: In this phase, a mobile node can authenticate with any of the communication gateway using the master secret key obtained from MSP.
- Phase II: After phase I, a mobile node can authenticate with one or a group of mobile nodes or sensor node mutually using the second phase.
- Phase III: Any sensor can mutually authenticate with other sensor node or a group of nodes asynchronously in the last phase.

The proposed mechanism maintains the structure shows in Figure 3. In the proposed scheme two major components namely, the MSP and a group of gateways working by the supervision of MSP. In addition, every connected gateway is interconnects a collection of sensor nodes and mobile nodes. At any time any mobile node is capable of authenticate itself with other mobile nodes. Also, a group of mobile nodes can authenticate themselves in order to communicate with each other. Similarly, any two or more sensors can authenticate themselves in order to exchange information.

#### A. SETUP PHASE

a) In the scheme, the *MSP* acquires the combination of keys, namely private and public keys ( $MSP_{pk}$ ,  $MSP_{sk}$ ) especially used for authentication purpose. It is also known as digital signatures. The public key of *MSP* will be stored at every gateway node (*G*) in the constrained environment network.

b) The *MSP* can also produce a pair wise keys for every gateway node (*G*) namely, ( $G_{pk}$ ,  $G_{sk}$ ). The public key of gateway is stored at *MSP* and the secret key will be stored at the corresponding gateway. The public key of a gateway is used only for registration purpose and during authentication process these are not used.

c) For every *G*, the *MSP* allocates a distinct identity known as  $ID_G$ .

d) In the constrained network environment, each *G* and a sensor node contains a shared master secret key. Hence, each of the sensor node(*S*) distributes a unique random master secret key  $G_{msk}$  for *G*. Both *G* and *S* knows each of their identities to each other in network domain.

## B. GROUP OF USERS REGISTRATION USING A PROTECTED MEDIUM

The mobile node obtains a his unique identity  $ID_M$  along with the secret text (password),  $P_M$  using a protected channel. Immediately, the MSP is looking unique identities and also verifies the identity of gateway,  $ID_G$  for which the user is belongs and authorized.

The registration process contains the following stages:

1. *Mobile Node(M) → MSP*: A temporal sequence,  $N_R$  chosen by M and find out  $H(P_M) \oplus N_R$ . After computing this, it sends  $(ID_M, H(P_M) \oplus N_R)$  to *MSP*.
  2. *MSP → M*: The mobile node selects a master key,  $M_k$  and calculates  $K = H(H(P_M) \oplus N_R) \oplus M_k$ . After that, keep this value in the memory (mart card) of *M*. *MSP* keep  $\{ID_M, M_k\}$  along with his and forward the smart card  $K$  to *M*.
  3. *M*: Once the mobile node obtains  $K$ , *M* can use the smartcard and feed  $ID_M, P_M$  &  $N_R$ . Smartcard calculates  $L = K \oplus M_k$ . *M* removes  $K$  and keep  $L$  in the smartcard.
  4. *MSP → G*: Computes  $G_k = H(ID_G, M_k)$ ,  $E_{Gpk}(G_k, ID_M)$ , signed with  $MSP_{sk}$
  5. *G*: Validates *MSP* authenticity with the help of  $MSP_{pk}$ . Decipher with  $G_{sk}$ . Stores the tuple  $\langle ID_M, G_k \rangle$
- The *MSP* preserves the IDs of each and every device in the constrained environment and the sensor nodes  $M_k$  in a secret catalog. The device *M* retains the pair  $\langle ID_G, M_k \rangle$  in the database. The *G* keeps  $\langle ID_M, k(M) \rangle$  for every entity *M*.

## C. DEVICE (M) AUTHENTICATION WITH GATEWAY

The device *M* is authenticated by gate way *G*, constructs a secret session key used in order to transfer information. The authentication phase between a device or a group of devices contains the following steps:

1. *Device (M) → G*: The device node(M), chooses a time variant nonce (random number),  $M_R$ . And, forwards the pair,  $(G, ID_M, M_R)$  as broadcast message.
2. *G → M*: Checks that  $ID_M$  is available or not, if available then obtains equivalent  $G_k$ . Then, generates a random number  $G_r$ . Calculates  $E_{Gk}(M_R, G_r)$ , sends the tuple  $\langle ID_G, M_k, E_{Gk}(M_R, G_r) \rangle$
3. *Device (M) → G*: First, get the main key  $M_k = L \oplus H(P_M)$  also with the help of  $M_k$ , the obtained  $ID_G$ , nearby calculates  $G_k = H(ID_G, M_k)$ . Using  $G_k$ , decrypts for  $M_R, G_r$ . Checks  $M_R$  using the established value. Discards otherwise,  $M_R$  not satisfied. Else, select  $S_k$ , a secret session key. Finally, calculates the secret key cipher  $E_{Gk}(G_r, S_k)$  and sends  $\langle ID_M, ID_G, E_{Gk}(G_r, S_k) \rangle$
4. *G*: Using  $G_k$ , decrypts for  $G_r, S_k$ . Checks  $G_r$ . Discards,  $G_r$  if not valid, otherwise, allow  $S_k$  to be used as session key.

## D. MOBILE-SENSOR AUTHENTICATION

The gateway, *G* distributes a secret key *with* each of the mobile devices or sensor nodes in a constrained networking environment. The mobile node knows the identities of each *G*, and the sensor nodes may not

be in touch with the gateways while authentication. Because, the sensor nodes may move from home location to foreign location. The following are the common steps to perform authentication between mobile devices and sensor nodes.

1. Mobile  $\rightarrow$  Sensor : Mobile node forwards a pair along with the unique identity ,  $ID_m$ , and the unique identity of the corresponding destined sensor,  $ID_s$
2. Sensor  $\rightarrow$  Mobile : After receiving the message in above step, S sends reply along the information ciphered by using the pre shared key  $G_{msk}$  and forwarded to M, and it holds the individuality of M,  $ID_m$  distinctiveness of S, random nonce  $S_r$  generated by sensor S.
3. Mobile  $\rightarrow$  Gateway : Mobile sends the cipher it received from Sensor to the Gateway.  
 $\langle ID_m, ID_g, ID_s, M_r, E_{G_{msk}}(ID_m, ID_s, S_r) \rangle$ .
4. Gateway  $\rightarrow$  Mobile:  $\langle ID_m, ID_g, E_{G_k}(M_r, K_{sm}, ID_s, E_{G_{msk}}(ID_m, S_r)) \rangle$ . The G, constructs tunneled encryption. The external cipher sent to Mobile with the random,  $M_r$  to authorize any *Gateway* to *Mobile* and a fresh secret session key  $K_{sm}$  between M and S, selected by *Gateway*. The nested cipher will be sent to S containing the random  $S_r$  to authorize G, S and the similar secret session key among Mobile and Sensor.
5. Mobile  $\rightarrow$  Sensor: *Mobile* deciphers the exterior part, checks the random  $M_r$ , if it is valid then keeps  $K_{sm}$  to be used as secret session key. Then sends the nested cipher without modification to Sensor. Sensor deciphers, checks the random  $S_r$  and keep  $K_{sm}$  as the secret session key by the same mobile node.  $\langle ID_m, ID_s, E_{G_k}(K_{sm}, ID_m, S_r) \rangle$ .

#### IV. SECURITY ANALYSIS

Finally, we examine the hardness of the projected mechanism. The analysis is depends up on the fundamental protection needs, comfortable conversation on battle to common defeats.

Mutual Authentication between *Mobile* and *Gateway* is implemented by obtaining a secret session key, which is used for both ciphering and deciphering. And also two random numbers generated for both mobile and gateway, a secret master key is used. An M2M service provider also generates a master key to gateway. Both mobile and gateway agreed upon a common secret key and authenticated. And the connected device, S previously distributes a session secret key. Once Mobile node desires a secure association to a Sensor, Sensor send back along with the cipher. This encryption can be the random nonce  $rs$  forwarded by *Gateway* and that can demonstrated later on by *Sensor*. *Gateway* sends the cipher to both *Mobile* and *Sensor* along with the random numbers for confirmation.

The M2M network scheme over the revise is a dispersed scheme containing of different categories of entities: connected entities, mobile nodes and the service provider. To show the rational accuracy of the verification mechanism in the constrained networks, we use SPIN.

The Fig. 4 depicts the procedure of verification between Mobile node and Sensor node using a Gateway.

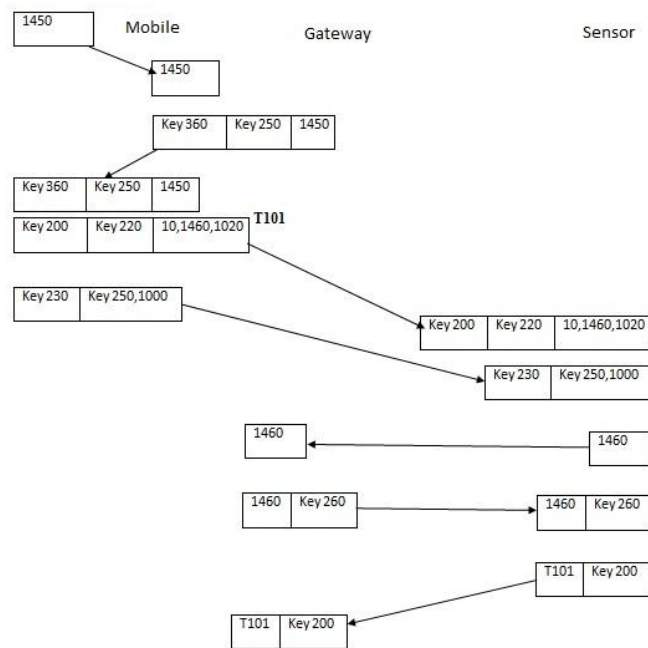


Fig. 4. Authentication in M2M systems.

Where the identity of sensor node is 1450 and it is sent to the Gateway. Based on the identity, Gateway returns the secret key of sensor to mobile signed by the gateway (key 360). Once the mobile node receives this, it can verify the signature of gateway and confirms that the key is belongs to sensor node. After this, mobile node generates a master secret key(key 200), a shared public-key/private-key pair(key 220). These are sent to the sensor node. It can verify the signature of the gateway, and request for mobile node key to decrypt the secret key. Once it got the key of mobile node, decrypts the shared secret key.

## V. RESULTS

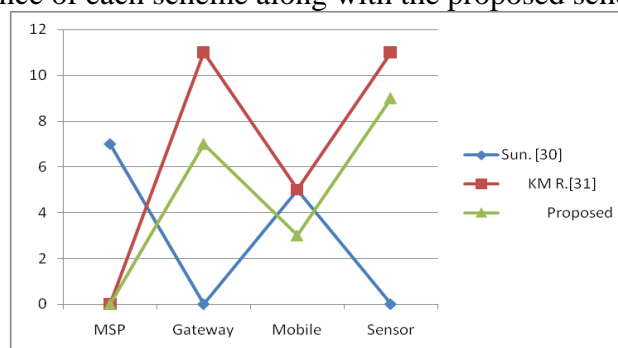
In this part, we evaluate the planned method to other freshly projected mechanisms. The following are the notations and the cost of other cryptographic hash functions costs used in the result analysis.

Symbol	Description	Cost
$C_k$	Cost of hash function	$C_k$
$C_e$	Cost of exponentiation	$500 C_k$
$C_m$	Cost of scalar multiplication	$62.5 C_k$
$C_p$	Cost of pairing	$1250 C_k$
$C_e$	Cost symmetric cryptosystem.	$C_k$

Based on the data provided above, we compare the computation cost of recently proposed schemes. We compare the Sun et al. scheme [30] and KM RENUKA [31]. The comparison is projected in the following table.

Entity	Sun. [30]	KM R.[31]	Proposed
MSP	$5C_k + 2C_e = 7C_h$	Not Involved	Not Involved.
Gateway	Not Involved	$11 C_h$	$7C_h$
Mobile	$4C_k + C_e = 5C_h$	$5C_h$	$3C_h$
Sensor	Not Considered	$11C_h$	$9C_h$
Total	$12 C_h$	$27 C_h$	$19 C_h$

The mobile node and sensor nodes authenticates with each other and also a group of mobile nodes with one another. But, the MSP is not involved in the authentication phase. The following graph represents the performance of each scheme along with the proposed scheme.



The gateway requires  $7C_h$  and the mobile node requires  $3C_h$ . Similarly, the sensor node takes only  $9C_h$ . However, the proposed scheme can perform better in group based authentication.

## VI. CONCLUSION

The M2M is most widely used technology used to decrease the break among the physical mechanism and connected devices. Authentication is a challenging task and it must be resistant to various types of attacks in the networking environment. The proposed scheme is established in such a way that it generates a

session key and the same is used to exchange the data in a secure manner. The proposed scheme removes the burden on devices which are communicating in a network and it is handed over to gateways. The M2M service provider generates a master secret key and it is given to the devices. So that any device can authenticate anywhere in the networking environment while it is roaming with any gateway. Using this master secret key, any mobile device can also authenticate any other sensor node in the network. In addition to that a group of mobile nodes and sensors can authenticate itself in the proposed scheme.

The projected method is fairly little at calculation and storage value as it needs little computations of hash functions and secret key cipher/decipher. Hence, the projected method is insubstantial and appropriate for devices with constrained resources. The proposed scheme is also analyzed using SPIN logic. We have proved the planned method is resistant to dissimilar possible adversarial attacks. Based on the analysis, the projected method is efficient and appropriate for M2M networks with devices contain limited resources.

## VI. REFERENCES

- [1] L. Sha, S. Gopalakrishnan, X. Liu, and Q. Wang, "Cyber-physical systems: a new frontier," *Proceedings of IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing (SUTU)*, June 2008, pp. 1-9.
- [2] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: towards survivable cyber-physical systems," *Proceedings of IEEE 28th International Conference on Distributed Computing Systems*, June 2008, pp. 495-500.
- [3] Min Chen, Jiafu Wan, and Fang Li, "Machine-to-machine communications: architectures, standards, and applications," *KSII Transactions on Internet and Information Systems*, Vol. 6, No. 2, February 2012, pp. 480-497.
- [4] Chen Hongsong, Fu Zhongchuan, and Zhang Dongyan, "Security and trust research in M2M system," *Proceedings of IEEE International Conference on Vehicular Electronics and Safety (ICVES)*, July 2011, pp. 286-290.
- [5] Rongxing Lu, Xu Li, Xiaohui Liang, Xuemin Shen, and Xiaodong Lin, "GRS: the green, reliability, and security of emerging machine to machine communications," *IEEE Communications Magazine*, Vol. 49, No. 4, April 2011, pp. 28-35.
- [6] Sachin Agarwal, Christoph Peylo, Ravishankar Borgaonkar, and Jean-Pierre Seifert, "Operator-based over-the-air M2M wireless sensor network security," *Proceedings of the 14th International Conference on Intelligence in Next Generation Networks (ICIN)*, October 2010, pp. 1-5.

- [7] Tien-Dung Nguyen, Aymen Al-Saffar, and Eui-Nam Huh, "A dynamic ID-based authentication scheme," *Proceedings of the Sixth International Conference on Networked Computing and Advanced Information Management (NCM)*, August 2010, pp. 248-253.
- [8] S. Chen, M. Ma, and Z. Luo, "An authentication scheme with identity-based cryptography for M2M security in cyber-physical systems," *Secur. Commun. Netw.*, vol. 9, no. 10, pp. 1146-1157, 2016.
- [9] W. Ren, L. Yu, L. Ma, and Y. Ren, "How to authenticate a device? Formal authentication models for M2M communications defending against ghost compromising attack," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 2, 2013, Art. no. 679450.
- [10] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proc. 28th Int. Conf. Distrib. Comput. Syst. Workshops*, Jun. 2008, pp. 495-500.
- [11] Y. Zhang, W. Duan, and F. Wang, "Architecture and real-time characteristics analysis of the cyber-physical system," in *Proc. IEEE 3rd Int. Conf. Commun. Softw. Netw.*, May 2011, pp. 317-320.
- [12] M. Chen, J. Wan, and F. Li, "Machine-to-machine communications: Architectures, standards and applications," *KSII Trans. Internet*.
- [13] F. Li and P. Xiong, "Practical secure communication for integrating wireless sensor networks into the Internet of Things," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3677-3684, Oct. 2013.
- [14] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1621-1631, Sep. 2012.
- [15] H. Li, X. Lin, H. Yang, X. Liang, R. Lu, and X. Shen, "EPPDR: An efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 8, pp. 2053-2064, Aug. 2014.
- [16] W. Jia, H. Zhu, Z. Cao, X. Dong, and C. Xiao, "Human-factor-aware privacy-preserving aggregation in smart grid," *IEEE Syst. J.*, vol. 8, no. 2, pp. 598-607, Jun. 2014.
- [17] M. Badra and S. Zeadally, "Design and performance analysis of a virtual ring architecture for smart grid privacy," *IEEE Trans. Parallel Distrib. Syst.*, vol. 9, no. 2, pp. 321-329, Feb. 2014.
- [18] Z. Lu and Y. Wen, "Distributed algorithm for tree-structured data aggregation service placement in smart grid," *IEEE Syst. J.*, vol. 8, no. 2, pp. 553-561, Jun. 2014.
- [19] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 675-685, Dec. 2011.
- [20] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644-654, Nov. 1976.
- [21] D. Wu and C. Zhou, "Fault-tolerant and scalable key management for smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 375-381, Jun. 2011.

- [22] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, "An efficient Merkle tree-based authentication scheme for smart grid," *IEEE Syst. J.*, vol. 8, no. 2, pp. 655–663, Jun. 2014.
- [23] R. C. Merkle, "Protocols for public key cryptosystems," in *Proc. IEEE Symp. Secur. Privacy*, Apr. 1980, pp. 122–134.
- [24] Q. Jiang, J. Ma, C. Yang, X. Ma, J. Shen, and S. A. Chaudhry, "Efficient end-to-end authentication protocol for wearable health monitoring systems," *Comput. Elect. Eng.*, vol. 63, pp. 182–195, Oct. 2017.
- [25] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, "An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 76, pp. 37–48, Dec. 2016.
- [26] Q. Jiang, Y. Qian, J. Ma, X. Ma, Q. Cheng, and F. Wei, "User centric three-factor authentication protocol for cloud-assisted wearable devices," *Int. J. Commun. Syst.*, vol. 32, no. 6, 2019, Art. no. e3900. doi: 10.1002/dac.3900.
- [27] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "GRS: The green, reliability, and security of emerging machine to machine communications," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 28–35, Apr. 2011.
- [28] T.-D. Nguyen, A. Al-Saffar, and E.-N. Huh, "A dynamic id-based authentication scheme," in *Proc. 6th Int. Conf. Netw. Comput. Adv. Inf. Manage. (NCM)*, Aug. 2010, pp. 248–253.
- [29] J.-M. Kim, H.-Y. Jeong, and B.-H. Hong, "A study of privacy problem solving using device and user authentication for M2M environments," *Secur. Commun. Netw.*, vol. 7, no. 10, pp. 1528–1535, 2014.
- [30] X. Sun, S. Men, C. Zhao, and Z. Zhou, "A security authentication scheme in machine-to-machine home network service," *Secur. Commun. Netw.*, vol. 8, no. 16, pp. 2678–2686, 2015.
- [31] KM RENUKA, SARU KUMARI, DONGNING ZHAO, AND LI LI, "Design of a Secure Password-Based Authentication Scheme for M2M Networks in IoT Enabled Cyber-Physical Systems", *SPECIAL SECTION ON SECURITY AND PRIVACY FOR CLOUD AND IOT*, Vol 7., 2019, pp. 51014-51027.