An Efficient Framework for a Secured Internet of Things Architecture

Adigun Maria F[1], Orunsolu Abdul A[2], Sodiya Adesina S[3] and Babalola Yetunde E[4]

[1]Department of Computer Science, Babcock University, Illisan Remo, Ogun State (mariaadigun@gmail.com)
[2]Department of Computer Science, Moshood Abiola Polytechnic, Ojere, Abeokuta, Ogun State (orunsolu.abdul@mapoly.edu.ng)
[3]Department of Computer Science, Federal University of Agriculture, Abeokuta, Ogun State (sodiyaas@funaab.edu.ng)
[4]Department of Computer Science, Federal University of Agriculture, Abeokuta, Ogun State (babalolayetty@yahoo.com)

Abstract— *The Internet technology is currently achieving a new height of "smartness" with the proliferation of Internet of Things revolution. Sensors of different grades have been deployed to emphasize the reality of smart world. However, this new impressive technology is now being challenged by myriads of problems ranging from non-standardization of its architecture, communication protocol compatibility to security issues. In this paper, we report an efficient framework for a secured IoT architecture which provides a security modification of the current architecture. The framework introduces an additional layer called IoT cloud into the current system to provide pragmatic communication using a lightweight encryption system based on the concept of Password Authentication Key Exchange Protocol. The communication flow of the lightweight encryption was analyzed and discussed.*

Keywords—electronic communication; IoT; Password Authentication; Protocol; Security

I. INTRODUCTION

Internet technology has become a dominant factor in the advancement of human civilization. This technology has brought about tremendous transformation that had earned the world a new appellation called "global village". In this way, information is transverse and shared with millions around the world within a second. Nearly every human sector has a feel of internet in one way or the other. New terms emerge every day with significant touch on the ways in which humans carry out their activities. For instance, e-commerce has made buying and selling an automatic thing across border and boundaries. Today, the trending technology is going toward ubiquitous computing which has been popularized with the concept of "Internet of Things (IoT)" [1].

IoT refers to an interconnected network of electronically embedded object/devices and other smart objects with sensors and actuators having a unique framework for information sharing. These devices can do everything ranging from smart home, virtual power plants to intelligent transportation. The goal of IoT is to create a smart environment where an individual will have a touch of their surrounding with internet availability. One current challenge of IoT is that it does not stick to any specific protocol but is open to any state of the art protocol available as at the moment [2]. This is a major problem from the fact that the internet technology has been continuously plagued with myriads of attacks. In addition, current internet tailored protocols such as IPv4, IPv6, DNS, DNSSEC, BGPSEC etc. have one challenge or the other in their adoption of the concept of IoT. In addition, the "smartness" of IoT cannot be separated from the advancement of other technologies in terms of security and performance improvement. For instance, machine learning algorithms can improve real-time decision making which is central to the IoT technologies. This can be extended to the use of audio and video recognition in the design of IoT. The use of lightweight encryption algorithm can improve security of sensors and mobile devices on the IoT ecosystem. Hence, the applications of some current technologies promise a smarter future for IoT. This implies that the possibilities associated with IoT are endless with what they can do for individuals, government and businesses. These possibilities are going to be challenged by the advancement of supporting communication protocols, available intelligent algorithms, encryption methods and security protocols.

In this work, we investigate a framework for a secured IoT architecture by addressing cybersecurity challenges from the development and implementation of various security protocols and AI. In order to achieve this, there is need to examine open issues in the current IoT architecture and limitations of common security protocols. In this way, security requirements for various stages of IoT architecture can be defined more efficiently. The rest of the paper is organized as follows: Section 2 contains literature review and in section 3, we discuss the framework of our proposed IoT-based architecture. In section 4, we present some relevant discuss and the work is concluded in section 5.

II. RELATED WORK

The literature review for this paper is divided into two sections. In the first section, the issues on development and progress of some internet protocols are discussed. In the second section, the implementation of IoT and some main security concerns is discussed.

A. The State of Current Internet Protocols

With such a high percentage of IoT devices, there is need for proper security measures for safeguarding the technology and the network it connects to. One of such security protocols that has been introduced is IPv6. Others are DNSSEC, BGPSec etc. What is the impact of these protocols on the future of IoT?

Heer et al. [3] examined how existing IP security protocols and architecture can be deployed. The work discussed the applicability and limitations of existing IP protocol in the context of IoT. The authors concluded by providing requirement for IP-based security solutions and highlight specific technical limitations to standard IP security protocols. For instance, IPv6 is the most recent version of Internet Protocol (IP), a 128-bits addressing system, that provides an identification and location system for computers on networks and routes traffic across the internet. This IP technology was developed to address the problem of address exhaustion in earlier version and to accommodate the emerging technology of IoT. Thus, the IPv6 have been significant to provide more addresses and accommodate more components and networks into the world of smart things. The new protocol provides technology for device mobility, security, use of multicast, hierarchical address, allocation and stateless address auto-configuration, which are essential to the functionality of IoT devices. The introduction of IPv6 as fundamental building blocks of IoT applications promises to bring a number of basic advantages including:

i. A homogenous protocol ecosystem that allows simple integration with Internet hosts
ii. Simplified development of very different applications
iii. A unified interface for applications, removing the need for application-level proxies.

Such features occasioned by IPv6 technology greatly simplify the deployment of the envisioned scenarios from building automation to production environment to personal area networks, in which an IoT environment is made up. Nowadays, there exists a multitude of version for IPv6 protocols due to the resource-constrained networks of smart things. For instance, we have Proxy mobile IPv6 (PMIPv6) and IPv6 based Low-power Wireless Personal Area Networks (6LoWPAN). PMIPv6 was developed to handle extreme mobility but consideration is not made for efficient route optimization in its default design. On the other hand, the 6LoWPAN was developed to make devices with resource constraints be included in the digital world of IoT. However, the 6LoWPAN is affected by a number of vulnerabilities such as rank attack, where a malicious node violates the rank rule in routing protocol for low power and lossy networks.

The Domain Name System Security Extension (DNSSEC) is a suite of Internet Engineering Task Force (IETF) specification for securing certain kinds of information provided by the DNS as used on IP networks. It is an authentication protocol that protects DNS information from common attacks such as session hijacking, sniffing etc. To implement DNSSEC, several new DNS record types are added to provide for the required authentication. Such records include Resource Record Signature, delegation signer etc. These records provide a strong incentive to secure DNS on which the operation of internet is fundamentally based upon. The use of DNSSEC will provide a secured exchange of data between the device and the internet. DNSSEC ensures security against a MitM attacker who is able to eavesdrop and modify traffic: however, to provide security it requires adoption by both end-points of DNS transaction and significant deployment and maintenance efforts. Although, DNSSEC was proposed in 1997, it is still not widely supported and deployed. Apart from low level of deployment, DNSSEC has some potential subtleties and vulnerabilities such as impairment of DNS functionality due to DNSSEC validation, interoperability problems due to DNSSEC enabled DNS responses and traditional DNS responses, voluminous DNS queries for launching reflection amplification DDoS attack, bootstrap problem and absence of security confidentiality.

The Border Gateway Protocol Security is an extension of Border Gateway Protocol that provides improved security for routing. The motivation for developing BGPSEC is that BGP does not include mechanisms that allow an Autonomous System to verify the legitimacy and authenticity of BGP route advertisements. This protocol extends the Resource Public Key Infrastructure by adding an additional type of certificate called BGPSEC router certificate that binds an AS number to a public signature verification key. The goal of BGPSEC is to use signatures to protect the AS Path attribute of BGP update messages so that a BGP speaker can assess the validity of the AS Path in update messages that it receives. Since BGPSec is a global protocol running across organization and national borders, it lacks a single centralized authority that can mandate its deployment. Hence, the deployment of this protocol becomes a coordination game among thousands of independently operated networks

B. IoT implementation and its security concerns

The Internet of Things is an emerging global internet-based information architecture facilitating the exchange of goods and services in global supply chain network. It involves a number of communication patterns such as Human to Human, Human to Things, Things to Things etc. which indicates the highly heterogenous nature of IoT. The successful implementation of the IoT involves consideration of a huge number of aspects such as the technology used for communication, various communication protocols which form the backbone of the IoT, standards to be used for communication, hardware and embedded devices used to build the hardware, the software, operating system that is compatible with hardware and the protocols being used (Fig. 1).

Suo et al. [4] provided one of the earliest work to investigate the security of IoT. Their work discussed key research issues to facilitate the emerging domain of IoT with emphasis on encryption mechanism, communication security, protection of sensor data and cryptographic algorithms. Weber [5] investigated the security and privacy challenges of the IoT. The authors identified that there should be measures that would make IoT architecture resilient to attacks apart from adequate legal framework by an international legislator to address salient issues of specific needs. In a more current literature, Diego et al. [6] provided a thorough survey that relates to the privacy and security challenges of the IoT. Their work addressed the intrinsic vulnerabilities as well as the security loopholes of the various layers of IoT architecture from the principles of data confidentiality, integrity and availability. Similarly, Adat et al. [1] examined the history, background and security analysis of IoT architecture. The authors further provided the taxonomy of security challenges in IoT environment and the available defense mechanisms. In our work, we critically considered some suggestions of this work in the design of our proposed approach.

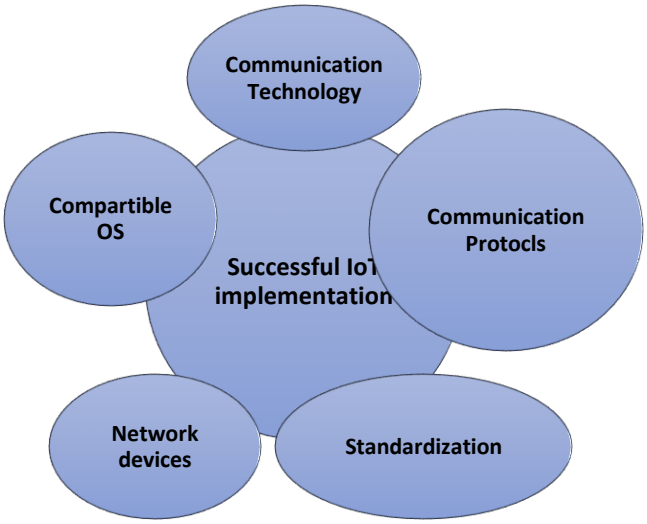

FIGURE 1. PARAMETERS FOR SUCCESSFUL IOT IMPLEMENTATION

The IoT requires architectural solutions that can manage various heterogenous states/devices in order to work effectively, efficiently and securely. However, there is no unified view of the IoT framework. For example, Farooq et al. [7] identified the security goals of confidentiality, Integrity and Availability as important in the construction of secured IoT ecosystems. Their work provided hints on various security algorithms for the perception layer, the network layer and the application/middleware layer (Fig. 2). In a more recent work, Hossain et al. [8] considered the research gap in the IoT ecosystem and provided a systematic analysis of security issues of IoT-based systems. In concluding their work, the authors highlighted a set of open problems and provided a detailed description of each suggestion. Various engineering bodies have issued a number of technology-specific standards on security and guidelines. For instance, IEEE posited a standard for architectural framework for the IoT where secure information exchange is considered. Based on a number of issues with the present IoT system, there is a need for a security-based framework where the weakness of human factor must be addressed. The IoT devices demand a number of security requirement in order to be considered as secure. These requirements include the followings:

i. secure authentication of devices/users,
ii. secure transmission of data,
iii. secure bootstrapping,
iv. security of IoT generated data and
v. secure access to data by authorized persons (availability)

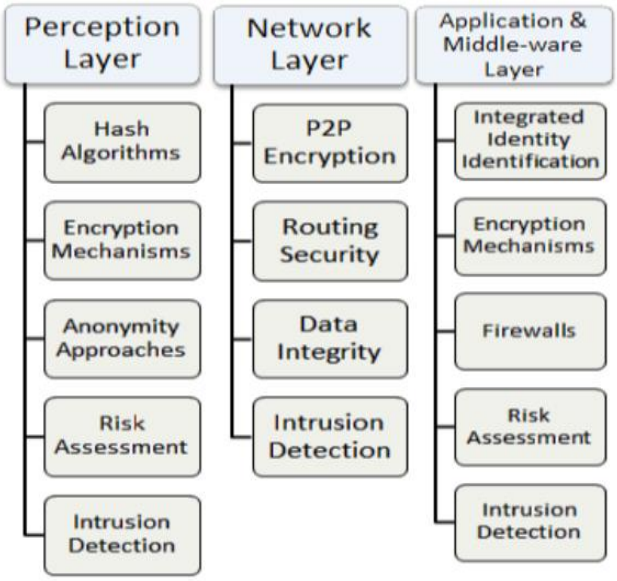

FIGURE 2. SECURITY ARCHITECTURE OF IOT (FAROOQ ET AL. [7])

III. THE PROPOSED FRAMEWORK

Although, the architecture of IoT is not standardized as different international organizations are still working on the project, the most common and basic architecture in existing literature consists of four layers (Fig. 3). However, our proposed framework is based on a modified version of the existing architecture with the inclusion of IoT cloud which is responsible for the management of security using lightweight Password Authentication Key Exchange protocol (Fig 4). This modified architecture addresses key areas in IoT systems such as Communication security, Protection of sensor data and cryptographic algorithms for data confidentiality and integrity.

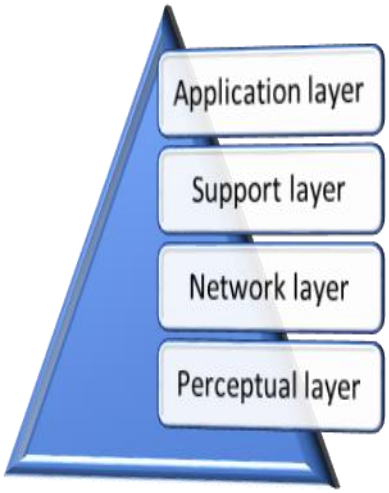

FIGURE 3. THE BASIC IOT ARCHITECTURE

A. *Components of the Proposed Framework for Secured IoT*

The proposed framework for secured IoT consists of the perceptual layer, the network layer, the support layer, the application layer and the IoT cloud, which provides the orchestration for managing all the other components through various security definitions in a lightweight Password Authenticated Key Exchange (PAKE) algorithm. In addition, the security requirement for each component is discussed.

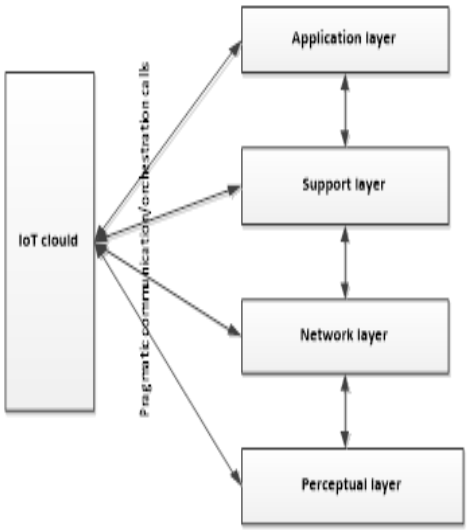

FIGURE 4. THE PROPOSED FRAMEWORK FOR SECURED IOT ARCHITECTURE

The first layer of the architecture is referred to as the perceptual layer, which collects different kinds of information using several sensing technologies. This layer hosts a number of physical devices ranging from RFID reader, Bluetooth devices, GPS to different grades of sensors that capture and convert physical world information into digital signals. As a result, the perpetual layer is the most concentrated points on the IoT architecture and forms the larger IoT environment. This implies that the security of perpetual layer has great implication on IoT architecture apart from the fact it is the source point of data. Thus, we defined the following security goals for the perceptual layer:

a. Authentication of devices to connection points
b. Confidentiality of transmitted data
c. Accuracy of data transmission

The network layer is next to the perceptual layer in that it serves as transmission medium for data capture through sensor devices. This transmission is often facilitated by Internet technology. Some security challenges in this area include:

i. Network congestions
ii. Distributed Denial of Service attack (DDoS)
iii. Data sniffing

The support layer is where intelligent operations are performed on the transmitted data. This layer is often concentrated and populated with large volume of data collected and transmitted through the network layer from the perceptual layer. Thus, the support layer requires high

computational power to process such large volume of data. Security considerations for this layer include:

i. How to ensure multi-party authentication among processes
ii. Intelligent processing of large volume of data
iii. Identification of malicious or suspicious information

The application layer is the topmost layer which concerns the end user. It consists of personalized services, user interface, environment monitoring services etc. which communicates directly with the end user and defined the acceptance of the IoT in practical applications (Adat et al. [1]). Security concerns for this layer include:

i. Data privacy and leakage
ii. Control of access
iii. Key management and authentication of services.

The last layer is the IoT cloud which is the main contribution of our research findings to the IoT architecture. The IoT cloud defined various services through which security can be guarantee in other layers of the architecture. This is based on the concept of PAKE using lightweight encryption algorithms of ECC and ElGamal (Orunsolu et al. [9]). This is necessary because most devices and sensors in the IoT environment are small devices with constraints over resources such as memory, external storage, memory cards etc. The logic behind the introduction of PAKE is that since all devices on a network either simple network or complex network like IoT requires communication where acknowledge/handshake plays a key role (Fig. 5), the use of PAKE is adopted to strengthen such communication while ensuring the lightness in terms of communication costs, memory overheads etc.

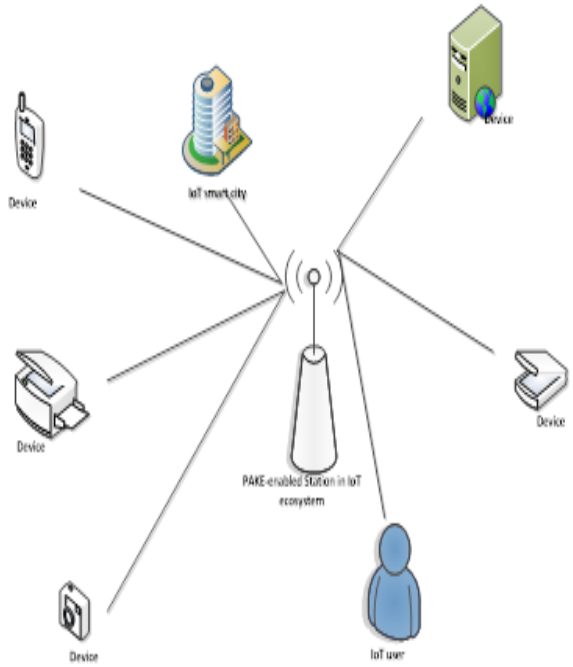

FIGURE 5. THE PROPOSED FRAMEWORK FOR SECURED IOT ARCHITECTURE

Each device within the PAKE-enabled station is equipped with a lightweight encryption algorithm that provide a secure path before communication can be established. The system works by starting with a numerical value p where $p > 3$ is a prime such that $a, b \in Fq$ satisfy that the discriminant delta = $4a3+27b2 \neq 0$, which defines the elliptic curve with singularity. The curve is of a simple form:

$y2= x3 + ax + b$ with $a, b \in Fq$ or F2m.

The Elliptic Curve E(Fq) over Fq consists of a set of points together with a point at infinity. These points form an abelian group (E (Fq), +) with 0 as a group identity. This concept of group is very essential to ensure that every communication within the IoT architecture is decipherable among different layers of the system while unauthorized entities cannot achieve the same task. That is, every communication can be related to encryption key where their inverses exist. For some group, $G \in Zp$, suppose $a, b \in G$. Then solving for an integer x such that $ax = b$ is called the discrete logarithm problem which formed the basis of conventional ELGAMAL cryptosystems. The DLP in Zp is replaced by elliptic curve field, Fq, to form the Elliptic curve ELGAMAL cryptosystem and is considered intractable if prime q has at least 160 digits and q - 1 has at least one large prime factor. These criteria for q are safeguards against the known attack on EC-ELGAMAL.

B. Elliptic Curve-Elgamal algorithm-based PAKE for IoT cloud

In this scheme, an EC-ELGAMAL approach is adopted for a PAKE based on the difficulty of Elliptic Curve Discrete Logarithm Problem. The EC-ELGAMAL is a very useful protocol for randomly generated curves and points because the order of the curve, the factors of that number or the order of the base point is not necessary. Given an elliptic curve E defined over a finite field Fq, P∈ E is point of order n and G is the generator point on the curve. A point Q = kP where k ϵ [1, n-1] defines the scalar multiplication which forms the basis of EC-based cryptographic approach. The secret key for password decryption is an integer r ϵ Fq while the public key for password encryption is computed as c = mG. We define a deterministic mapping function dmap () that take distributed password, p = a + b + c+…= m, to curve point M ϵ Fq such that it obeys the additive homomorphic property of EC-ELGAMAL protocol:

dmap (a + b + c +...) =dmap (a) + dmap (b) + dmap (c)+… where M demonstrates how many times m associates with G

.i.e. M = mG. The reverse mapping function rdmap () is the decryption function that extracts the password m from a given point mG.

One important operation for this mapping is the addition over elliptic curve that is only possible with the points on the curve.
If we define the opposite (encryption) point of

P = (x1, y1) to be $^{-}$P= (x1, -y1) and

Q= (x2. y2) with Q≠-P,

then (P+Q) = (x3, y3) can be calculated as:

$$x3=\lambda 2-x1-x2$$

$$y3= \lambda(x1-x3) - y1$$

$$\lambda = (y2-y1) / (x2-x1) \text{ if } x1\neq x2 \text{ i.e. adding}$$

$$\lambda= (3x12+A) / 2y1 \text{ if } x2=x1 \text{ i.e. doubling}$$

Since the preceding formulae has great impact on the performance optimization of the EC-ELGAMAL based approach, we choose the Double and Add algorithms for the above computation. The optimization of the basic Double and Add algorithm using addition-subtraction method is used for this implementation as described in algorithm 1. Addition-subtraction method has the advantage of reducing the complexity of scalar multiplication by reducing the required number of addition operations.

Algorithm 1: Double and Add Point Scalar Multiplication with subtraction

input: P ∈ E(GF(q)), k = Σ i=0nk−1 ki2i
output: Q = [k]P ∈ E(GF(q))

```
Begin
  Initialize: Q=P;
    for i ← nk − 2 to 0 do
        Q = 2Q //Point Doubling;
       if ki = 1then
      Q = Q + P //Point Addition;
     if ki = -1then
   Q = Q - P //Point Subtraction;
  end
 end
end
```

The proposed protocol applies ECDLP to the PAKE protocol to enhance the safety level and to simply the computational and communication load. The process flow of user authentication is described in Figure 6.
Prior to commencement of the protocol, the two entities say, IoT cloud, A and other layers, B must agree upon the password, Pw. Then, A and B share and divide the previously known password communicated in a secure way by the chopping function define below into x and y

$$P = f(x, y) = b$$

where f is a cipher algorithm that act on x, y which is equivalent to Boolean variable b equal 1 (true) if the flow is incorruptible.

A select an elliptic curve Ep (a, b) defined on Zp and picks a random point e1 over the elliptic curve of order n. In addition, A chooses a random integer r as his private key and computes the public key, C1 as:
C1 = r * e1

The username of entity A and C1 are sent to B. Entity B chooses his private key, d and computes his own public key using any selected points on the curve as:
C1b = d* e2

Upon receiving the request, B examines the sender's credentials and uses the public key of A to encrypt his own y portion of the password Pw as:

Y*= C2 = y+ d*C1

Thereafter, B sent the encrypted Y* and C1b to A. A decrypt Y* according to the computation below:

y= C2 – (r* C1b)

The proof of y as generated by user A is:
y + r * e2 - (d * r * e1) = y + r * d * e1 – r * d * e1 = y + 0 = y
where y, C1, C2, e1, e2 are all points on the curve while 0 is the zero point which serves as the identity of the elliptic curve additive group operation.

If no attack has modified the value of Y*, it follows that Y=Y* as already known by A from B. A repeat the same process encrypting his x portion of the password with the public key of B so that B confirms that X=X* as already known by B.

Consequently, A and B authenticated each other and generates a session key upon successful authentication for confidential exchanges of data in the IoT environment.

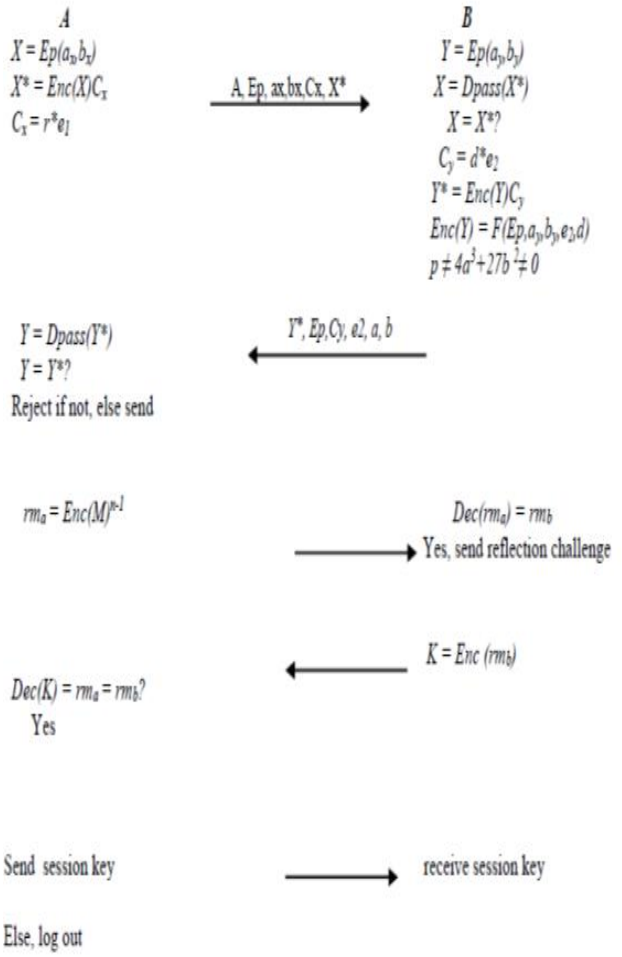

FIGURE 6. SECURED INFORMATION IN IOT CLOUD USING PAKE

The notion of reflection message is proposed in this analysis to thwart unauthorized entity corruption. The reflection message, rm, is introduced into authentication flow to tackle entity corruption and compensate for forgetfulness on the parts of genuine access points. The superscript n-1 on the reflection message denotes that it is related to the topic discussion of the most recent previous secret communication. It is a message whose disclosure can affect the parties in the communication severely. Thus, parties in natural sense guard such information from a third party. A doubting partner may require this message from the other party to prevent corruption.

The hybrid classifier is optimized using machine learning algorithms consisting of Naïve Bayes and Support Vector Machine.

IV. SECURITY ANALYSIS OF THE PROPOSED PAKE ALGORITHM

The security of the proposed PAKE algorithm is discussed from the concept of message confidentiality and integrity. Although message availability is also a key requirement of a secured communication, we intentionally omitted its discussion because IoT framework should be more concerned with confidentiality and integrity.

A. Message confidentiality

Message Confidentiality means that it is computationally infeasible whether online or online for an adversary to gain any partial information on the content of EC-ELGAMAL message. In our protocol, if the adversary intercepts the password message and searches the message to obtain r. However, to find r, the attacker needs to solve the equation C1=r*e1 in which he must find the multiplier that creates C1 starting from e1. This is the elliptic curve discrete algorithm. Equally, the adversary cannot know accurately guess the private key in one run (since the approach permit only one run of the private key), he cannot compute the session keys due to the difficulty of the elliptic curve discrete logarithm problem. In addition, the security mask provides by C1 cannot be partitioned in decrypting the message because the adversary had to inverts i.e. C1-1 = (r*d*e1)-1 and multiplies with the result of C2 to remove the mask. The secret knowledge of d increases the computation hardness of this attack.

B. Message Integrity

Message integrity preserves the message from unauthorized modification, deletion and destruction. Suppose the adversary can know d, then he can use P= C2-(d*C1) to find the point P related to the plaintext password message. Because e2=d*e1, this is the same type of problem. Adversary knows the value of e1 and e2; he needs to find the multiplier of d.

V. CONCLUSION

In the last few years, this emerging domain for the IoT has been attracting the significant interest and will continue for the years to come. In spite of rapid evolution, we are still facing new difficulties and severe challenges. The problem of security and standardization of IoT protocol will dominate research issue in current literature and beyond. The customization of current generation of internet protocol for suitability in IoT environment in term of security, speed, efficient result utilization etc. will create huge research potential in academics and industries.

REFERENCES

[1]. Adat V and Gupta B. 2017, Security of internet of Things: issues, challenges, taxonomy and architecture. Springer Journal of Telecommunication System

[2]. Odelu,V.,Das,A.K., Khan,M.K., Choo, K. K. R. and Jo,M. 2017. Expressive CP-ABE scheme for mobile devices in IoT satisfying constant-size Keys and ciphertexts. IEEE Access, 5, 3273–3283

[3]. Heer T., Oscar G, Rene H., Sye L., Sandeep K. and Klaus W. 2015, Security Challenge in the IP-based Internet of Things. Springer Journal of Wireless Personal Communication.

[4]. Suo H., Wan J., Zou C., Liu J. and China G. 2012. Security in the Internet of Things: A Review. 2012 International Conference on Computer Science and Electronics Engineering.

[5]. Weber R .2010. Internet of Things – New security and privacy challenges. Computer law and Security Review. Vol. 26 pp. 23-30

[6]. Diego M, Ioannis P and Yang B. 2017. Internet of Things: Survey on Security and Privacy

[7]. Farooq M., Waseem M., Khairi A. and Mazhar S. 2015. A Critical Analysis on the Security Concerns of Internet of Things (IoT). International Journal of Computer Applications. Vol 3. No.7

[8]. Hossain M., Hassan R and Skjellum A. 2017. Securing the Internet of Things: A meta-study of Challenges, Approaches and Open Problems. IEEE International Conference on Distributed Computing Systems Workshops

[9]. Orunsolu A, Sodiya A, Folorunso O and Agboola A. 2017. Distributed Password Authentication Key Exchange Protocol using Hybrid Approach. Serial Anale Informatica.