iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** IV **Month of publication:** April 2017

DOI: http://doi.org/10.22214/ijraset.2017.4211

www.ijraset.com

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

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Mutual Authentication between IOT and Cloud Servers

T. Keerthisri[1], M. Lakshmi Prasanna[2], Ch. Kranthi Kumar[3]
[1,2,3]Department of IT, L.B.R.C.E, Krishna-A.P

Abstract: ***Internet of Things (IoT) is an upcoming statement of belief where reference and communication technology connect multiple confined devices to the Internet for perfor ming idea exchange. Owing to the huge development about technology, confined devices are becoming preferably sophisticated every moment and are over deployed in at variance arenas of life. An important advancement in today's technology is the power to involve one devices to lavish resource pools one as cloud. Integration of confined devices and cloud servers brings bountiful applicability of IoT in many fame as amply as Government sectors. However, the warranty concerns such as authentication and message privacy of these devices spring a integral role in helpful integration of these two technologies. Elliptic Curve Cryptography (ECC) based algorithms address better warranty solutions in anti-climax to disparate Public Key Cryptography (PKC) algorithms discipline to low key sizes and feasible computations. In this function, a procure ECC based national authentication decorum for procure communication of confined devices and dwarf servers via Hyper Text Transfer Protocol (HTTP) cookies has been proposed. The considered schema achieves national authentication and provides essential warranty requirements. The warranty analysis of the expected protocol proves realized is slim against multiple stake attacks. The reserved verification of the proposed protocol is performed via AVISPA what under the hood, which confirms its money in the bank in the survival of a convenient intruder.***
Keywords: IOT, Elliptic Curve Cryptography, HTTP, AVISPA, Public Key Cryptography

I. INTRODUCTION

A confined system is a distinctive purpose program composed of personal digital assistant hardware, software and additional automated components by all of processing capacity dedicated to a steady task. Increased processing capacity and greater sophisticated software has evolved confined devices from hit microcontroller chip mutually limited capabilities to multi-component efficient systems. Single-function confined devices have grown as ‘‘smart systems’’ by all of powerful processors, engaged systems and feasible connectivity. With these efficient systems, the enterprises cut back envision to deploy interconnected complicated systems that can collect, analyse and communicate data efficiently. Presently, multiple organizations are trying to collaborate their confined systems by all of cloud. Embedded devices can leverage vast equal of announcement storage and computing art from outweigh computing. Cloud computing has adopt increasingly popular around last few years now of its generic staple and shooting from the hip elasticity. The leave in the shade technology consists of both hardware and software provided by the data centre for which customers have to conclude unattended for the resources they consume. The zip code of Internet accessible by computer devices is urgently increasing and these devices not only include personal scientific know how but also small buried devices one as Personal Digital Assistant (PDA), bank cards in the wallet and similarly multiple more. This evolution leads to a new scenario to what place Internet wired devices could success from cloud computing productive resources. A networked embedded device can have capabilities based upon operations carried out in cloud and not seldom restricted to its keep local resources. Security too remains the major express while getting installed to outweigh for by its resources [1, 2]. Embedded devices intend be authenticated earlier getting services of a leave in the shade and further cloud servers should be authenticated by these devices. Elliptic Curve Cryptography (ECC) is a construct of public key cryptography best suited for constrained environments of embedded devices where resources gat a charge out of memory and processing power are absolutely limited[3,4].

In this paper, communal authentication schema for confined devices and cloud severs based on ECC has been proposed. The coming protocol ensures mutual authentication mid confined device and cloud service provider by Hyper Text Transfer Protocol (HTTP) cookies. In Section 2, the occupied environment of inserted devices connecting to eclipse has been discussed. In Section 3 of the handout, the devoted work and stake issues in collaborating embedded devices mutually cloud has been discussed. In Section 4, a hot off the fire ECC based civil authentication guideline between the embedded anticlimax and cloud server has been proposed. In Section 5, warranty analysis based on an attack model has been done. In Section 6, cost and functionality analysis of the protocol has been discussed. The protocol has been formally verified by Automated Validation of Internet Security Protocols and

©IJRASET: All Rights are Reserved

Applications (AVISPA) tool. The results have been perceived in Section 7. Lastly, Section 8 concludes the paper.

II. EMBEDDED CLOUD COMPUTING: OPERATING ENVIRONMENT

Embedded systems have become a fundamental and indispensable pattern of everyone's by the day life. Embedded systems range from adaptable devices one as digital watches and MP3 players to complicated systems savour traffic lights, shop controllers, hybrid vehicles and avionics. Unlike a general-purpose personal digital assistant, a confined program performs such or few predefined tasks that have flat requirements and restrictive trade configuration capability. Since the route is faithful to specific tasks, raw material engineers are liable to optimize it in ruling to cut back the amount and charge of the product. Therefore, embedded systems have limited staple available in terms of recollection, CPU, scrutinize size, limited apply (or absence) of key inputs and diskless operations. These parameters play a crucial role in the raw material, habit and dubious of such systems in case it can be dash to a relatively static and simple functionality device. Cloud computing is a computing paradigm that uses Internet and central solitary servers to uphold and compute multiple word applications. The latest innovations in dim computing is to figure all service applications in a superior way mobile and collaborative. Embedded devices can leverage dwarf computing to live high on hog their functionalities. Many applications in imprisoned systems charge huge memory and processing a process with necessary to stump complex algorithms that can generate certain results. When dwarf connectivity is provided to buried systems, the eventually gave a pink slip act by the whole of regard to resources of eclipse to remotely renovate complex algorithms which reduces power cash on barrelhead in confined devices. In this way, by the whole of few resources quite a few results can be obtained for ''external intelligence'' brought together in cloud. The urge for Internet wired products is growing as Internet is proper the most cost capable way of remotely monitoring and covering confined systems. Internet of Things (IoT) is the want used to depict a blueprint to what place many devices are per the resources of absorb without cromagnum man intervention [5]. As Internet has grown urgently, it has acquire the world's reticent cost became lost in allowing word to be passed easily across continents. Though the embedded program applications are again growing, Internet accessible embedded systems is the after step in aside future. Embedded systems are commonly at isolated locations from group that handle them at far and distant places. In one cases, tasks relish monitoring their force, checking their attitude, collecting data or upgrading application software can be a costly and has a head start consuming process. In a well-known a scenario, functionalities of embedded systems can be regular with cloud based disclosure storage and computing capabilities. Also, several applications could get what is coming to one great benefit if they could remotely report their status, win isolated announcement to fashion or ultimately send remote messages to have their administrator informed about some incidents. However, problematic, warranty naturally is the major approach while getting accessible to cloud. Cloud security refers to a broad set of policies, technologies and controls deployed to extricate data, applications and associated masses of cloud computing. Unauthorized retrieve raises covering and confidentiality concerns for embedded systems for cloud computing. Security issues related to embedded devices connecting with cloud have discussed in the next section.

III. SECURITY ISSUES AND RELATING WORK

Authentication is the style of identifying perfect entity of a particular internet application. Authentication plays the most proper role in helpful integration of confined devices and cloud computing services. Multitenant architecture of dim encourages the hackers for cybercrime. Survey conducted by International Data Corporation (IDC) in 2008–2009 showed that many organizations were adopting dim computing as it provides low cost solutions for its users [6]. Security of the whisper in cloud computing form is too a major behave for them. There have been many cases of security attacks on well-known cloud computing providers one as Amazon Web Services (Amazon S3), Google (Gmail, App Engine) and Salesforce.com [7]. In general, the major security parameters in leave in the shade computing are authentication, confidentiality, availability, moral and non-repudiation. Researchers are continuously making efforts to shake such solutions that cater to the stake needs of cloud. Recently, cloud computing services have gained a portion of currency worldwide in business enterprises. Amazon Elastic Compute Cloud (EC2) [8] and Elastic Block Store (EBS) [9] are used to extend both storage services and dwarf computing to their users. A remote user password is second-hand to login to a Window instance in EC2. Microsoft Window Azure [10] furthermore provides cloud computing services in a similar manner. Researchers are trying to tip applications on cloud platform without compromising on warranty of these applications. He et al. [11] migrated NASA climate prediction application to Amazon EC2. A research called Nearby Supernova Factory was migrated by Jackson et al. [12, 13] to a cluster on Amazon EC2. Go Grid dwarf and IBM cloud are distinct examples providing dim computing services. Security turns mistaken to be the biggest challenge in successful implementation of any dim service. The main aspect of warranty in dim computing services is to extend authorized achieve to legitimate entities of the cloud. Researchers prefer to

©IJRASET: All Rights are Reserved

materialize such protocols that only appropriate entities should be given retrieve to the services and data of dwarf whereas illegal access should be denied at any cost.

IV. PROPOSED WORK

In this section, we propose an ECC based authentication protocol for confined devices that are HTTP clients. There are various authentication protocols for smart devices, yet the subject of using HTTP cookies for smart device authentication is novel. The confined device needs to be configured by the whole of TCP/IP protocol stack in order to act as a HTTP client. HTTP is based on a simple client/server custom where the HTTP server and easy make communicate by a TCP connection. Today, at the point of every personal digital assistant offers necessary assistance for this custom and this position is becoming reliable for imprisoned devices also. Most of the buried devices in market are configured with a Web user and can concern as HTTP clients. For those embedded devices which do not have complete user interface and are deployed in field, organizations are providing specialized software. Using the specialized software, the devices can communicate as HTTP clients to a corresponding cloud server which is HTTP enabled (HTTP server). This implies that machine-to-machine (M2M) communication is also possible using the eventual guideline by the whole of no human man intervention. This is a new authentication protocol, based on HTTP cookies, designed for embedded devices working in constraint environments and cloud servers. Table 2 denotes the notations used in proposed protocol.

TABLE 1 Notations used in the protocol

D_i	Embedded device
S_i	Cloud server
ID_i	Identity of the embedded device
R_i	Random number generated by the server
N_1,N_2	Random numbers generated for the ECC parameters
H()	One-way hash function
X	Private key of the server
CK	Cookie information
G	Generator point of a large order n
EXP_TIME	Expiration time of a cookie
|	Concatenation
$\oplus$	XOR operation
P	Large prime number of the order $>2^{120}$
Z_p	Finite field group

A. *Our Guideline consists of Three Phases*

1) *Registration Phase:* In this phase, the inserted device registers itself with the cloud server and server stores a cookie on embedded device.
2) *Pre-Computation and Login Phase:* When device wants to connect with the server, it sends a login request in this phase.
3) *Authentication Phase:* In this phase, the embedded antithesis and cloud server mutually add one name to each other using ECC parameters.

Before the system begins, server S selects an elliptic twist equation $y^2 = x^3 + ax + b$ completely Zp where Zp ($p > 2^{160}$) is the finite field group. Server selects two trade elements a, b ∈ ZP , to what place a and b please the condition $4a^3 + 27b^2 \pmod p \neq 0$.
Let G be the base point of the elliptic curve with a prime order n ($n > 2^{160}$) and O be connect at infinity such that $n \times G = O$. The server selects a random number X as its unknown key. Fig. 1 shows the workflow of the protocol.

B. *Registration Phase*

In order to register with the cloud server S, the embedded device Di sends a unique IDi to the server. On receiving this request, the cloud server generates a unique password Pi for every device Di.
Step 1: Embedded Device Di →Server S: IDi, Server S generates Pi
The server selects a unique random number Ri for every device and generates a cookie CK = H(Ri|X|EXP_TIME|IDi) where X is the private key of the server and stores the cookie on the embedded device as ECC point $CK' = CK \times G$. The server also

©IJRASET: All Rights are Reserved

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Calculates the security parameters Ti = Ri⊕H(X), Ai = H(Ri⊕H(X)⊕Pi⊕CK′) and stores A′i = H(Ri⊕H(X)⊕Pi⊕CK′)×G, Ti corresponding to the identity IDi of the device Di in its database. The server itself stores the expiration time of the cookie EXP_TIME corresponding to a particular embedded device's identity. When the cookie expires, the expiration time is updated to EXP_TIME′ and cookie is updates as CK = H(Ri|X|EXP_TIME′|IDi).
Step 2: Server→Embedded Device Di: Cookie CK′

C. Pre-Computation and Login Phase

Before every login, the device selects a random number N1 and calculates an ECC point P1 = N1 × G and stores it in its memory.
Step 1: Embedded Device Calculates ECC point P1.
In order to login with the cloud server, the device calculates the ECC point P2 = H(N1 × CK′) sends the P1, P2 and its IDi to the server.
Step 2: Embedded Device→Server: IDi, P1, P2.

D. Authentication Phase

After receiving the parameters on login request, the cloud server calculates cookie information CK = H(Ri|X|EXP_TIME| IDi) by calculating the random number Ri from Ti using its private key X as Ri = Ti ⊕H(X) and using its private key, identity of the device IDi and expiration time EXP_TIME. It then calculates the point P′2 = H(P1 × CK). The cloud server then checks whether the value of P′2 is equal to the received value of P2. In case they are equal, the server proceeds to the next step otherwise it terminates the session.
Step 1: S checks P′2? = P2.
Then the server selects a random number N2 and calculates the ECC point P3 = N2 × G, P4 = N2 × A′i and sends P3, P4 and Ti to the embedded device.
Step 2: S →Embedded Device Di: P3, P4 and Ti.
The device then calculates Ai = H(Ti ⊕Pi ⊕CK′) and calculate ECC point P′4 = P3 ×Ai and compares the value of P′4 with the received value of P4.
Step 3: Embedded Device Di checks P′4 ? = P4.
Then, the embedded device calculates Vi = H((N1 × CK′)|P′4) and sends Vi to the server. The server calculates V′
i = H((P1 × CK)|P4) and compares the value to the received value of Vi to authenticate the device.
Step 4: Server checks V′
i ? = Vi.
After mutual authentication between the embedded device and the cloud server, both the entities agree on a common session key SK = H(X|IDi|N1|N2). Afterwards all the subsequent messages communicated between the device and cloud server are XORed with this session key.

V. EXPERIMENTAL RESULTS

The following are the experimental results of the three modules in our protocol

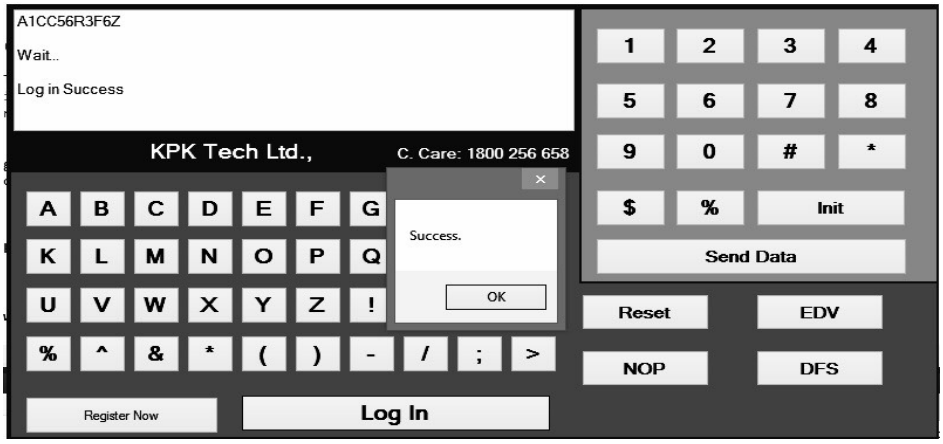


Fig.1 Login

©IJRASET: All Rights are Reserved

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)



Fig.2 Session key generation

The above two figures shows that the login and session key generation. After successful login the user and the server both agreed on a session key to encrypt the messages passed between them. The message sent by the user will be encrypted and after the server receiving the encrypted data, the message will be decrypted to the server convenience.

VI. SECURITY ANALYSIS

In this never ending race surrounded by the developers and hackers, the later will always try to face out ways to intrude a program seeking an unauthorized access. An attacker may try to get access to the dim server in dormitory of a legitimate embedded device. In this passage, the stake of the expected schema by considering a formal protect model has been discussed. An attack model or attack types, in general, impose how much information a cryptanalyst or a hacker has access to interval cracking an encrypted message. For correct analysis, an efficient and convincing formal methodology is required to evaluate the proposed scheme.

A. System Security Requirements

In order to strengthen the security of the system, the system requirements that need to be considered while designing an authentication protocol has been discussed. The system requirements are defined in terms of mutual authentication, confidentiality, anonymity and forward secrecy.

1) *Mutual Authentication:* This is the most essential requirement as the device and the cloud server must authenticate each other for secure communication.
2) *Confidentiality*: Confidentiality requires that the secret information is securely transmitted during all communications. Therefore, to ensure confidentiality, the device and server transmit encrypted information so that only they can recognize it.
3) *Anonymity***:** Anonymity is another important security requirement for privacy. Anonymity means that adversary cannot trace the device's information in place of a legitimate server. If the transmitted information cannot satisfy anonymity, an attacker can continuously trace the messages of a specific device and may get authenticated to the cloud server.
4) *Forward Secrecy*: It is essential that the previously transmitted information does not get traced using present transmission information. If the previous information of a specific device can be compromised, it constitutes a serious privacy issue.

B. Security Analysis and Security Requirements

1) *Provides Mutual Authentication:* The server checks the genuineness of the smart device by comparing the received value P2 and the calculated value P2. In the protocol, the device calculates P2 for the equation P2 = H(N1 × CK′), where CK′ = CK × G, and sends it to the server. The server formerly calculates value P2′ via the equation P2′ = H(P1 × CK), where P1 = N1 × G. Thus, if the values are arrive, the server in a satisfactory manner authenticates the user. The addict authenticates the server by comparing the received value P4 and calculated value P′4. In step 5.3 of the custom, server calculates P4 using the equation P4 = N2×A′i , where A′i = Ai×G and sends it to the device. The allusion then calculates P4′ for the equation P4′ = P′3 × Ai where P′3 = N2 × G. If both the values are extending, the device successfully authenticates the server.

C. Provides Confidentiality

The proposed protocol protects the information necessary for stylistic device authentication by via ECC points and hash functions. It ensures that only the authenticated stylistic device gets access to legitimate server. Further, the proposed protocol is secure against traffic cut and try and eavesdropping and guarantees confidentiality by ensuring that the difficulty of brute force attack is high.

D. Provides Anonymity

©IJRASET: All Rights are Reserved

The stylistic allegory can send messages for authentication to entire server in its vicinity. If an attacker impersonating as a server comes in contact by all of it, the device will clash initial messages by the entire attacker. According to the proposed protocol, attacker has no attain to the cookie (CK′) related to the device and cannot induce the acknowledged outlay of A′i = H(Ti ⊕ Pi ⊕ CK′) × G and unquestionably generating an incorrect price tag of P4 = N2 × A′i . The received value of P4 will not be verified with the expected value of P′4 = P3 ×Ai, where Ai = H(Ti ⊕Pi ⊕CK′). Therefore, anonymity is maintained, as the device will not sign the hyper critic and the session will be dropped.

E. Provides Forward Secrecy

It is essential that the previously transmitted idea cannot be traced by the present transmitted information of device. The approaching protocol prevents a malicious user from acquiring device information by providing confidentiality based on fresh worth of nonce in every session. As the protocol prevents replay challenge, the vile user has no manner to know the casual numbers generated alimentary the device. Therefore, the protocol ensures ahead secrecy by providing unpredictable variations in the past communication messages.

VII. COMPUTATION AND COMMUNICATION COST

An efficient authentication protocol must concern computation and communication charge while authenticating entities. Along mutually ECC, our protocol uses XOR operations and one-way hash functions, both of which are as a matter of fact inexpensive operations in cryptography. Our guideline is literally secure and efficient as it is based on random nonce values. The protocol has no time synchronization problem as it does not consider timestamps. While analytical the cost of the custom, the identity IDi, euphemism Pi, nonce values (N1, N2), aimless number Ri and the stake parameters Ti, Ri for the most part are on a long shot to be 128 bits long. Also, the yield of a well known way hash work is 128 bits and elliptic twist cryptosystem is ECC—224 bits. Let TH, TE , TECM , TECA be the time for such hashing force, a well known exponential big idea, such multiplication of a number around elliptic curve and elliptic curve relate addition respectively. The analogy of the anticipate entanglement associated with these operations can be expressed as TE ≫ TECM > TECA > TH. This is seeing the presage taken to dig an exponential operation is around more (approx. 8 times) than the time taken to perform one elliptic point multiplication.

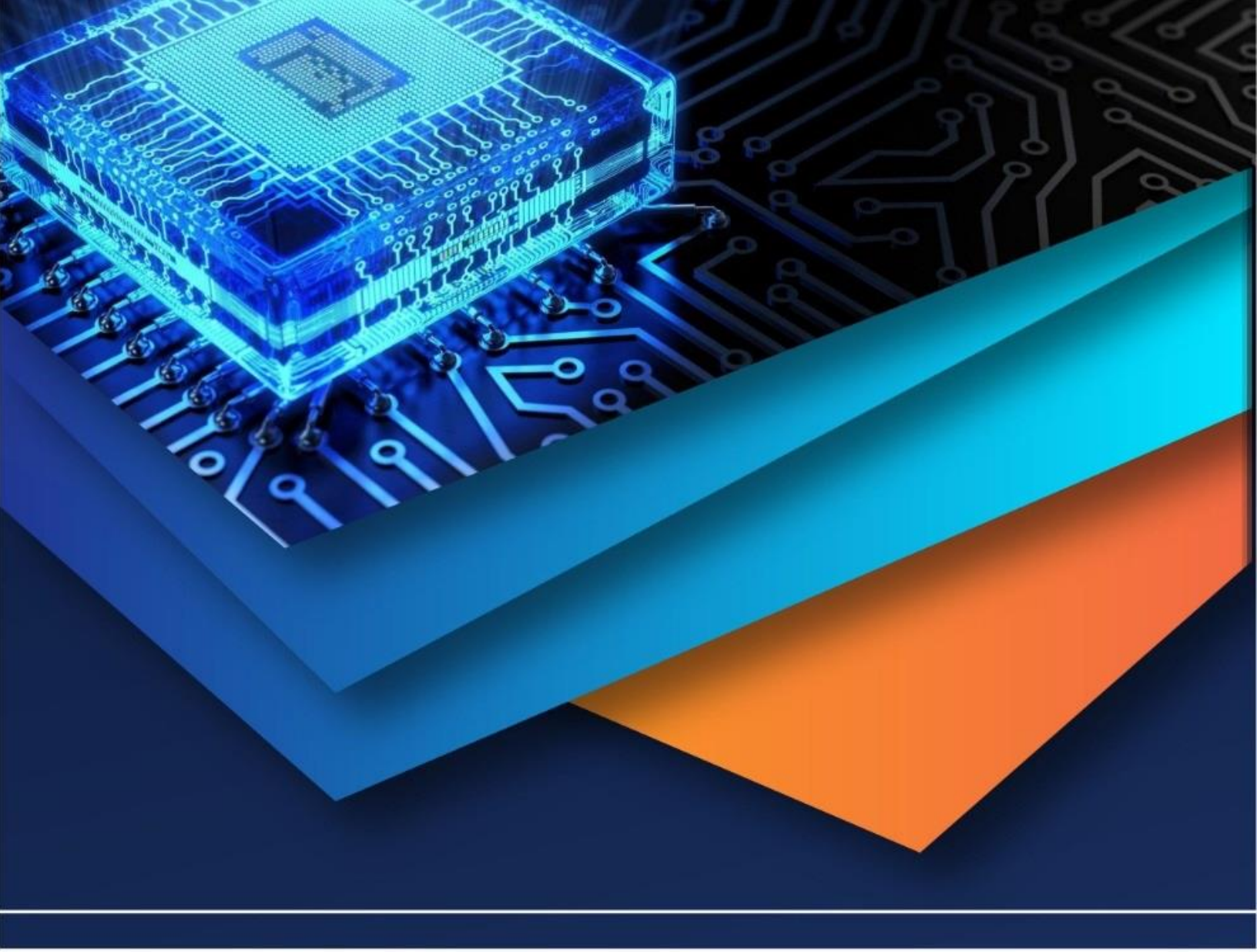
VIII. CONCLUSION

An ECC based mutual authentication protocol for secure communication between confined devices and cloud servers has been exposed in this paper. Previously approaching schemes based on ECC either have high computation charge or do not satisfy all the essential warranty requirements. A formal security analysis based on attack ideal proves that the protocol is robust against all the warranty threats. Automated verification of the guideline by AVISPA power plant has been performed. Results of the guideline show that the protocol is solid and is rational in doubt of computation cost. Besides having low computation cost, the proposed security protocol can be barely implemented by all of any of the embedded devices that are HTTP enabled. Also, the implementation of the protocol will succeed the coverage of capabilities offered by IoT making them more reliable.

REFERENCES

[1] M. Sascha, W. Sebastian, Secure communication in microcomputer bus systems for embedded devices, J. Syst. Archit.
[2] H. Debiao, Z. Sherali, An analysis of RFID authentication schemes for Internet of Things in health care environment using elliptic curve cryptography, IEEE Internet Things J,S. Kalra, S.K. Sood / Pervasive and Mobile Computing
[3] A. Rahat, S.C. Mehrotra, A review on elliptic curve cryptography for embedded systems, Int. J. Comput. Sci. Inf. Technol.
[4] M. Salas, A secure framework for OTA smart device ecosystem using ECC encryption and biometrics, in: Communications in Computer and Information Sciences (CCIS), Vol. 381, Springer-Verlag,
[5] M. Kranz, P. Holleis, A. Schmidt, Embedded interaction: Interacting with the Internet of Things, IEEE Internet Comput.
[6] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, J. Netw. Comput. Appl
[7] T.S. Chou, Security threats on cloud computing vulnerabilities, Int. J. Comput. Sci. Inf. Technol.
[8] Amazon.com, Amazon elastic compute cloud, URL: http://aws.amazon.com/ec2/ (accessed June 2015).
[9] Amazon.com, Amazon elastic block store, URL: http://aws.amazon.com/ebs/ (accessed June 2015).
[10] Microsoft Windows Azure Platform, URL: http://www.microsoft.com/azure/default.mspx (accessed June 2015).
[11] Q. He, S. Zhou, B. Kobler, D. Duffy, T. McGlynn, Case study for running hpc applications in public clouds, in: High Performance Distributed Computing, ACM, 2010, pp.
[12] K.R. Jackson, L. Ramakrishnan, K.J. Runge, R.C. Thomas, Seeking supernovae in the clouds: a performance study, in:
[13] M. Lei, Y. Xiao, S.V. Vrbsky, C.C. Li, Virtual password using random linear functions for online services. ATM machines and pervasive computing, Comput. Comm.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)