A Secure and Smarter Solution to the Network Security for a Smart City Using SMARTIE

Ashwin V. Didolkar,
Department of Computer Science and Engineering,
Wainganga College of Engineering and Management,
Nagpur, Maharashtra, India

Fazeel I. Z. Zama,
Department of Computer Science and Engineering,
Wainganga College of Engineering and Management,
Nagpur, Maharashtra, India

***Abstract*:-** Today, adopting the practice of using very fast and vast computer networks, hosting remote servers on the Internet for the real time, secure data gathering, storage, access control and retrieval of data involving heterogeneous network devices and data sources i.e. Cloud Computing has empowered and can unite citizens of the world narrowing it down to a network of physical objects or things embedded with electronics, software, sensors, and network connectivity, enabling these to collect and exchange data i.e. Internet of Things[1], thus, leading to a network centric real time data paradigm, the simple and secured components, modules, protocol application and operation along with the structures that will be developed and integrated into this project architecture, overcoming many anomalies and obstacles that SMARTIE[1] may or may not perceive as per the current prerequisites for the Smarter Network Security solutions to be implemented for any Smart City.

Keywords*:-*SMARTIE, Modified A.E.S. Algorithm, D.D.O.S Attacks.

*****

1. Introduction

Urbanization is not merely a modern phenomenon, but a historic and a rapid transformation of human social roots on a global scale as defined by the gradual increase in the proportion of people living in urban areas. Migration (human) is the movement of people from one place in the world to another for the purpose of taking up permanent or semi-permanent residence, usually across a political boundary where many types of push and pull factors may influence people

in their movements (sometimes at the same time), including: 1. Environmental (e.g., climate, natural disasters) 2. Political (e.g., war) 3. Economic (e.g., work) and 4. Cultural (e.g., religious freedom, education). By compiling into one system all the key data and applications that are now siloed away, cities create a foundation for rolling out new services for citizens and employees. Gathering and sharing urgent, useful information, and layering on new technologies, such as activators, sensors,

analytics and mobile applications, which can help make their communities safer and more livable which gives the government departments and agencies the data necessary to get citizens the services they need.

Taking into account the situations as mentioned above, then adopting the practice of using a network of remote servers hosted on the Internet to store, manage, process and secure the data, rather than a local server or a personal computer is called as Cloud Computing. The three of the main benefits of cloud computing include: 1. Self-service provisioning: End users can spin up computing resources for almost any type of workload on-demand. 2. Elasticity: Companies can scale up and then scale down products and services again as per demands. 3. Pay per use: Computing resources are measured at a granular level, allowing users to pay only for the resources and workloads they use.

This project thus revolves around real time data paradigm to create and provide simple, secured and smarter data gathering, storage, access control and retrieval, adapting to the current scenarios and situations, for the Smarter Network Security solutions, prevalent in the context of a developing nation like India, to be implemented for any Smart City.

2. Related Work

Several methods and techniques have already been proposed and developed in literature but may provide superfluous features and structures or lack in something or other feature without thinking of adjustment based on the conditions and scenarios of India. If we also consider the fact that IoT related technologies come with a high level of heterogeneity, with specific protocols developed with specific applications in mind, it is no surprise that the IoT landscape nowadays appears as highly fragmented. Many IoT enabled solutions exist with recognized benefits in terms of business and social impact, however they form what we could call a set of Intranets of Things, not an Internet of Things! Considering this, the literature comprises a plethora of contributions which strengthen in particular the features and the structures, the ones that are being proposed. These may be elucidated as under:-

2.1 PrivLoc[2]:

PrivLoc by Jens-Matthias Bohli Dan Dobre, Ghassan O. Karame and Wenting Li, 2014;
Location based services are progressively utilized as a part of our every day exercises. In current services, clients

however need to surrender their area security with a specific end goal to get the administration. The part gives two principle interfaces; 1. Subscribe (fencedArea)- Monitor a range, scramble territory ask for, and forward it to a standard spatial database. 2. Report (development): Notification-Used by followed gadgets, they report about their last development, again scramble the area and forward to database, if the development enters subscribed territory, tell to the supporter. Quite, PrivLoc empowers a proficient and protection saving crossing point of development vectors with any polygon of enthusiasm, utilizing usefulness from existing Geofencing administrations or spatial databases. The security and protection procurements of PrivLoc are broke down and the execution of our plan by method for usage are assess where the outcomes demonstrate that the execution overhead presented by PrivLoc can be generally endured in reasonable organization settings.

2.2 shortECC[3]:

The shortECC is a lightweight security methodology in light of change of elliptic bends cryptography. The decrease of the length of the security parameters impacts the security level additionally spares the vitality required for calculation and correspondence. The shortECC methodology is intended for securing the trading of short payloads (e.g., 32-bit long, however not restricted to) inside of the remote sensor system. This methodology is relevant in situations where the remote sensor hubs are partnered to a shut gathering and the individuals from this shut gathering trust one another where it is conceivable to get to and to leave the trusted gathering. For the computerized signature, an adjusted rendition of standard Elliptic Curves Digital Signature Algorithm is utilized. It doesn't utilize a hash capacity, in light of the fact that the negligible length of yield of the standard cryptographic hash capacity is 160 piece, which is too vast. The mark calculation is a 1-to-1signature without reference section. The message is marked with the underwriter's private key and encoded with the beneficiary's open key. This plan can be reached out to a 1-to-n signature if the beneficiaries in the gathering share a gathering key pair. For the confirmation, the beneficiary uses its private key (or the gathering key) to unscramble the message and the underwriter's open key to check the mark. The primality testing is done utilizing the lightweight deterministic primality test–Deterministic Miller Rabin Test. In the same paper the creators demonstrate that the era or confirmation of an advanced mark utilizing the ECC P160 bend requires no less than one request of greatness more vitality than sending it over the radio for the TmoteSky hub Hardware stage outfitted with MSP430F1611 microcontroller and cc2420 tranceiver from Texas Instrument.

2.3 DCapBAC[3]:

Distributed Capability Based Access Control proposes an answer for settle on Access Control choices already, giving an approval token to a client who is requesting a specific administration or usefulness offered by a thing. This token is marked by a stage which should be trusted by both sides. The approval token is sent alongside a solicitation to the thing that confirms the legitimacy of the solicitation and the approval token, conveying the asked for information, if effective. This depends vigorously on Public Key Cryptography as any token will be appointed to a stage's open key just. this gives a simple approach to approve them, once they can convey the token themselves and use it while it is substantial.

2.4 lwsCoAP[4]:

The Constrained Application Protocol (CoAP) is a committed exchange convention for use with compelled IoT hubs and obliged systems (i.e. low-control, lossy). Obliged hubs regularly have low-controlled CPUs, for example, 8-bit microcontrollers with little measures of ROM and RAM, while compelled systems, for example, IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) frequently have high parcel mistake rates and a normal throughput of 10s of Kbit/s. CoAP is a light-weight application convention taking into account UDP that backings multicast demands, changing and REST web administrations between the end-focuses, and is seen as a future convention for IoT. CoAP is still work in advancement of the IETF CoRE Working Group which utilizes the "coap" and "coaps" URI plans for distinguishing CoAP assets and giving a method for finding the asset. Assets are composed progressively and administered by a potential CoAP inception server listening for CoAP asks for ("coap") or DTLS-secured CoAP asks for ("coaps") on a given UDP port. That is the reason, a possibility for immediate and basic HTTP asks for over HTTP ports for assets will be arranged through the framework as required, maintaining a strategic distance from any all the more moderate Hardware and high bundle blunder rates.

2.5 Secure RD[5]:

There are numerous cases in the IoT frameworks where direct disclosure of assets and administrations is not down to earth because of unmoving and/or dozing hubs scatter systems or systems where multicast movement is wasteful. In this way, it is required to utilize a middle of the road framework that stores all data of IoT items, assets and administrations together with all important information including capacity, connections, geo-area and so on. Utilizing such a framework, lookups can be performed and fitting IoT asset can be found and in this way utilized. The RD segment depends on the protected stockpiling and client confirmation parts keeping in mind the end goal to empower secure access to the dynamic data about every single accessible asset in the framework at a given time. The assets are enlisted in the RD utilizing particular message as a part of XML organization utilizing HTTP POST. This message contains meta-information about the asset and/or administration, abilities, area and other significant information. Ensuing hunt and revelation is performed utilizing XML message sent utilizing HTTP GET containing fitting channels, showing coveted administrations or assets. Here, the RD usefulness is actualized in JAVA innovation in mix with a MySQL database and scrambled information for determined stockpiling of information. Exchanges are executed in put away methodology. The RD articles are gone through JAVA DAO (Data Access Object) class to put away methodology for information administration.

2.6 DDOS Attacks[6]:

Opeyemi A. Osanaiye has observed that Distributed Denial of Service attack has been identified as the biggest threat to service availability in Cloud Computing which prevents legitimate Cloud users from accessing pool of resources provided by Cloud providers by flooding and consuming network banwidth to exhaust servers and computing resources. IP ridiculing, otherwise called IP address falsification or a host document capture, is a commandeering system in which a wafer takes on the appearance of a trusted host to disguise his personality, parody a Web webpage, seize programs, or access a system. Mock IP Packet location systems;

1.Hop-Count sifting (HCF)[7] is a strategy proposed by J. Cheng, H. Wang and K.G. used to channel using so as to flood movement amid a DDOS assault the Time-to-Live (TTL) estimation of the source parcel header where the bounce number worth is contrasted and the valueobtained from the built IP2HC mapping table. Bundles will be acknowledged if qualities match while a bungle will be termed satirize and dismisses. The significant downside of this method is that all the OS designers don't have the same introductory TTL esteem; henceforth confuse can happen effortlessly.

2. Way unique finger impression strategy called ANTID Anti-DDoS[8] proposed by F.Y. Lee and S. Sheih, recognizes and channels parodied bundles in DDoS assault where every parcel has an installed special way unique finger impression which distinguishes the highway an IP bundle crosses from source to destination by recognizing diverse IP ways taken by distinctive IP parcels. The server has a guide for each of the customer and maps the customers IP locations to the relating way unique finger impression.

3. Follow course is a typical system device that is broadly utilized for deciding the way at which a bundle navigated, is utilized to recognize a ridiculed parcel will advise the quantity of bounces to the genuine wellspring of the bundle. Among the significant disservices of this strategy is that it is moderate and if the genuine source is ensured by a firewall, the examining parcel will give back the quantity of jumps to the firewall which won't mirror the bounce check of the genuine source.

4. TCP intuitive system was proposed because of TCP being an association situated convention that guarantees dependable conveyance of bundles by sending ACK messages for each conveyed parcel in the middle of source and destination. Correspondence between both sides empowers location of mock parcels as its source won't react to any test from the objective in the event that it doesn't exist.

The creator then proposes another technique for OS fingerprinting which is the observing of an approaching bundle to decide the OS the source is running on. OS fingerprinting can either be dynamic and inactive. Dynamic fingerprinting includes sending an exceptionally made test parcel towards the genuine source while uninvolved gets the header highlights from approaching packets.(E.g.)(Active) NMAP AND SinFP while (Passive)POF and OSF.

3. Proposed Work

Protection and the IoT: Navigating Policy Issues - Opening Remarks of FTC Chairwoman Edith Ramirez[9], "Today, I might want to concentrate on three key difficulties that, in my perspective, the IoT stances to shopper security: (1) universal information gathering; (2) the potential for sudden employments of customer information that could have unfavorable results; and (3) elevated security dangers. These dangers to protection and security undermine buyer trust. Also, that trust is as critical to the boundless shopper appropriation of new IoT items and administrations as a system association is to the usefulness of an IoT gadget. I accept there are three key steps that organizations ought to take to upgrade shopper protection and security and subsequently construct customer trust in IoT gadgets: (1) embracing "security by configuration"; (2) taking part in information minimization; and (3) expanding straightforwardness and giving purchasers notification and decision for sudden information employments. I trust these strides will be vital to effective IoT plans of action and to the assurance of customer data." This venture needs to accomplish nevertheless objective as expected in both of the base papers consolidated.

The following are the better, simple features that can make this project as a benchmarking step in the implementation of the network security solutions for a Smart City:-

3.1 Privacy Preserving mechanism -
U. I. D.:

A user identification (UID) is a unique positive integer acting as a unique key randomly generated and then assigned by the system to each user. But UID known to everyone but the best possible way it must be assigned to each user must be the single motto i.e only for some meaning and a reason. Each user is identified to the system by its UID and user names are generally used only as an interface for humans. Only, this is to be done after the user has successfully registered herself/ himself on the proposed system application graphics user interface to become a smart user.

3.2 Encryption using Modified AES Algorithm[10]:

It is an essential viewpoint to shield the classified sight and sound information from unapproved access. Interactive media substance can be content, sound, still pictures, liveliness and video. Such substance are ensured by interactive media security strategy. This is accomplished by procedures that depend on cryptography. Utilizing customary encryption calculation will make encryption troublesome for substantial volume of sight and sound information. For the encryption of any sight and sound information we need such calculations that require less calculation on account of expansive size of information. Symmetric-key calculations are less computationally genuine than any Asymmetric key calculations. Commonly, symmetric key calculations are thousands times sooner than those of the unbalanced calculations. So the better suitable

strategy to scramble the mixed media information is to encode it with symmetric key encryption calculations. As an outcome of equipment execution AES is quick symmetric piece calculation. This technique is known as innocent methodology. Applying the gullible methodology on huge measure of information takes vast calculation and makes the encryption speed moderate because of assortment of limitations. The essential expect to alter AES is to give less calculation and better security for information. The change AES calculation adjuststo give better encryption speed.

In Modified-AES the encryption and unscrambling procedures take after to that of AES. The piece length and the key length are indicated by detail: three key length options 128, 192, or 256 bits and square length of 128bits. For instance, expect the key length of 128bits which is most regularly implemented.The calculation is separated into four operational pieces where we watch the information at either bytes or bit levels and the calculation is intended to treat any blend of information and is adaptable for key size of 128 bits. These four operational squares speak to one roundof Modified-AES.

There are 10 rounds for full encryption. The four distinct stages that we use for Modified-AES Algorithm are: 1. Substitution bytes 2. ShiftRows 3. Change and 4. AddRoundKey. To conquer the issue of high count and computational overhead, skirt the Mix segment step and include the changes along these lines lessening the estimation piece of calculation for enhancing the encryption execution. The other three points must remain unbothered as they seem to be. Substitution Bytes, ShiftRows and AddRoundKey stay unaffected as it is in theAES. A solitary 128bit square is the info to the encryption and unscrambling calculation. This piece is a 4x4 square framework of comprising of bytes which is replicated into a state exhibit. The state exhibit is changed at every phase of encryption and unscrambling. Likewise, the 128bit key is additionally portrayed into a square framework which is communicated into a variety of key calendar expressions of 4 bytes each. The aggregate key calendar words for 10 rounds are 44 words; each round key being like one state. Here the essential capacity is Permutation which is utilized rather than Mixcolumn.

Stage is broadly utilized as a part of cryptographic calculations. Stage operations areinteresting and critical from both cryptographic and design perspectives. In the stage table every passage demonstrates a particular position of a numbered data bit comprising of 64 bits in the yield.

In the stage table every passage demonstrates a particular position of a numbered inputbit comprising of 64 bits in the yield. While perusing the table from left to right and after that start to finish, watch that the 58th piece of the 64-bit square is in first position,the 50th is in second position et cetera. In rendition of security examination and test comes about our proposed encryption plan is quick and then again it gives great security and includes less overhead the information, this today is the prerequisite of the greater part of the interactive media applications.

Along these lines Modified AES calculation is superior to anything AES calculation. Hypothetical examination and test aftereffects of the accomplishment makes it extremely suitable for high rate and essentially, less overhead on the information. For all these pay it is suitable for any huge scale content andimage exchange.

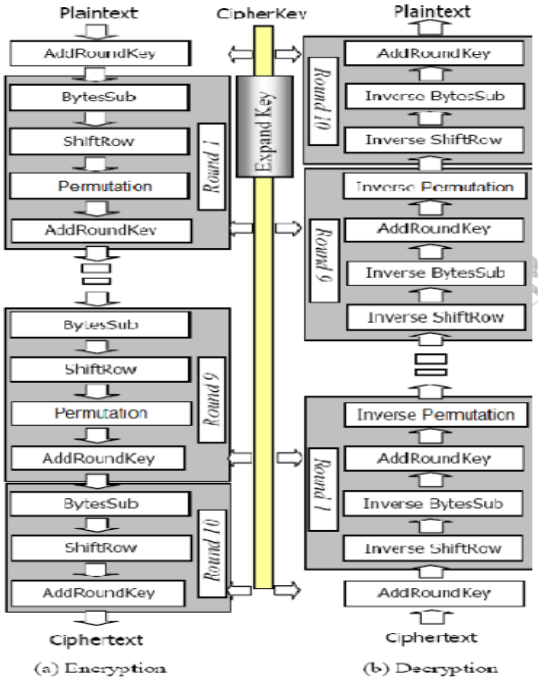

Figure: 1. Modified Advance Encryption Standards

To test the algorithm different sizes of text and image files are taken and the calculated time of both the Modified-AES with Advanced Encryption Standard are compared. Table shows the comparison results performed on different sizes of text files using Modified-AES and the AES algorithm.

In the version of security analysis and experimental results our proposed encryption scheme is fast and on the other hand provides good security and adds very less overhead on the data, this today is the requirement of most of the multimedia applications.

3.3 Load Balancing:

Burden adjusting in distributed computing gives a productive answer for different issues dwelling in

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Table: 1. Permutation table -Modified Advance Encryption Standards

File size	AES	Modified-AES
10kb	00:00:01:9624000	00:00:00:7332000
20kb	00:00:05:9436000	00:00:01:3884000
30kb	00:00:09:2040000	00:00:02:4180000
40kb	00:00:12:0276000	00:00:03:8064000
50kb	00:00:16:7232000	00:00:06:0998000
60kb	00:00:20:2488000	00:00:08:8296000
70kb	00:00:25:3812000	00:00:10:6080000
80kb	00:00:30:0786000	00:00:14:1180000
90kb	00:00:36:0098000	00:00:17.113200

Table: 2. Comparison of encryption between AES and Modified AES Algorithms

distributed computing environment set-up and use. Burden adjusting must consider two noteworthy assignments, one is the asset provisioning or asset portion and other is errand planning in disseminated environment. Proficient provisioning of assets and booking of assets and also errands will guarantee: a. Assets are effortlessly accessible on interest. b. Assets are proficiently used under state of high/low load. c. Vitality is spared in the event of low load (i.e. at the point when use of cloud assets is beneath sure edge). d. Expense of utilizing assets is lessened. Distributed computing can have either static or element environment based upon how engineer arranges the cloud requested by the cloud supplier. In static environment the cloud supplier introduces homogeneous assets that are not adaptable. The cloud requires former learning of hubs limit, preparing force, memory, execution and insights of client necessities. These client necessities are not subjected to any change at run-time.(E.g.):Round Robin calculation and voracious with Round Robin calculation. In element environment the cloud supplier introduces heterogeneous assets. The assets are adaptable in element environment. Any cloud can't depend on the earlier learning while it considers run-time insights. The necessities of the clients are allowed adaptability (i.e. they may change at run-time). A heap adjusting system in element environment designates the asset with slightest weight to an assignment and considers hub capacities. In view of the weight and capacities of the hub, undertaking is appointed to a hub.

Subsequently, giving numerous servers implies when in time of any circumstance if any enrolled client asks for a server for any administrations, the one server that is the nearest to the client is to be chosen by the framework to just give those administrations to that specific enlisted client.

3.4 Log monitoring mechanism:

Focal Logging and Monitoring permits to merge the million log sources in one spot and conceivably perform light connection over all the different log sources. Log observing are a sort of programming that screen log documents. Servers, application, system and security gadgets produce log documents. Blunders, issues, and more data is always logged and put something aside for examination. To recognize issues naturally, framework chairmen and operations set up screens on the created logs. The log screens filter the log records and hunt down known content examples and principles that demonstrate on imperative occasions. Once an occasion is recognized, the observing framework will send caution, either to a man or to another programming/equipment framework.

Likewise, User Activity Monitoring (UAM) is the observing and recording of client activities. UAM catches client activities, including the utilization of uses, windows opened, framework orders executed, check boxes clicked, content entered/altered, URLs went to and about each other on-screen occasion to secure information by guaranteeing that representatives and temporary workers are staying inside of their alloted assignments, and representing no danger to the association.

Hence Log management (LM) contains a way to deal with managing substantial volumes of PC created log messages (otherwise called review records, review trails, occasion logs, and so on.). LM must cover:

- centralized aggregation
- log collection
- long-term retention
- log rotation
- log analysis (in real-time and in bulk after storage)
- log search and reporting.

Worries about security, framework and system operations, (for example, framework or system organization) and administrative consistencies drive the Log Management.

Cloud base had turned out to be more than normal with the associations flourishing to venture into a limit less world. Moving to the general population cloud base had constantly spellbound a sympathy toward security of the applications and the information facilitated on the cloud. Aside from information security, there are various difficulties like system crime scene investigation, investigating, deficiency checking, and consistence. To beat these difficulties, IT security experts need to screen and examine the log information produced by their cloud framework progressively. Logs being the advanced foot shaped impressions of everything that happens to your application, frameworks, and information facilitated on mists, give exact system security insight data that guarantees information security.

In this way a straightforward and savvy Log checking instrument for every single client action and information exchange and upgrade inside the framework that is being created, has been executed in this task.

3.5 Access Control and Granting mechanism:

First, the direct authorization to the mobile user clients that have registered successfully for this project takes place. Then the mobile user clients' demand for some service or another may be achieved by just monitoring the Media

Access Control type Hardware address of devices. Along with this, the Unique Identification key generated by the system for the users then decides the access granting policy mechanism in this project.

3.6 Data Communication and Transmission mechanism:

Data communication transmission refers to the movement of data in form of bits between two or more digital devices using a transmission medium. This is achieved in this project by receiving direct Hyper Text Tranfer Protocol requests from the clients, which is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web. Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text. This is done along side eliminating the need of a special proxy server, which will save the time complexity significantly.

4. Conclusion

This Project's Network Security architecture features concretely adapt in and follow the Internet of Things-Architechture Reference Model. Following are some of the crucial and strategic findings that come afore as all the features of the existing and the proposed work are studied and examined:

1. It can be sensed that IoT is on the cusp of a new technological revolution. Some observers have argued that precisely because IoT is in its early stages, all must wait to see how it evolves before addressing privacy and security issues. But it is believed that all have an important opportunity to ensure that new technologies with the potential to provide enormous benefits develop in a way that also protects consumer information. Companies are investing billions of currency in this growing industry; they should also make appropriate investments in privacy and security.

2. New technologies for information retrieval, processing and security guided by access control policies must always be a welcome change since it must be noted that the weakest link determines the security. Thus, security for information source (sensor devices, smart phones) is as crucial and essential as secure communication between devices and platform using heavy cryptographic protocols.

3. This project thus lets anyone implement the complex methods by using the simple schemes specified above thereby also considering the circumstances that come afore in the developing part of the world like in India, apart from the developed one paving a directed path for some very poor part of the world,to be stepped into and make progress.

4. Any City must be a reflection of human ambitions, an embodiment of human creativity, society-governance and the capacity to innovate and continue revenue generation.

References

[1] Jens-Matthias Bohli, Antonio Skarmeta, M.Victoria Moreno, Dan García, Peter Langendbrfer- SMARTIE: Secure IoT Data Management for Smart Cities, International Conference on Recent Advances in Internet of Things (RioT), Singapore, 978-1-4799-8325-4/15/$31.00 ©2015 IEEE, 7-9 April 2015.

[2] Jens-Matthias Bohli, Dan Dobre, Ghassan O. Karame, Wenting Li- PrivLoc: Preventing Location Tracking in Geofencing Services Proceedings of the 7th International Conference on Trust and Trustworthy Computing - Volume 8564-P- 143-160, Springer-Verlag New York, Inc. New York, NY, USA ©2014 ISBN: 978-3-319-08592-0.

[3] Jose L. Hernandez, Antonio J. Jara, Leandro Marinc and Antonio F. Skarmeta Gómeza- DCapBAC: embedding authorization logic into smart things through ECC optimizations, International Journal of Computer Mathematics, ISSN: 0020-7160, DOI:10.1080/00207160.2014.915316.

[4] Krimmling, J. ; IHP, Frankfurt (Oder), Germany ; Peter, S.- Integration and Evaluation of Intrusion Detection for CoAP in Smart City Applications, Conference on Communications and Network Security (CNS), 2014 IEEE, 29-31 Oct. 2014, P-73 – 78. INSPEC Accession Number: 14838002.

[5] Editor: Boris Pokric, DunavNET, Work-package leader: Peter Langendörfer, IHP, Dissemination level: (Confidentiality) PU, Suggested readers: Consortium/Experts/other reader groups, FP7-SMARTCITIES-2013 Project number: 609062 http://www.smartie-project.eu/-SMARTIE Deliverable D3.1 Components for secure information gathering and storage, □ 2014 Participants in project SMARTIE, P-15-17.

[6] Opeyemi.A. Osanaiye- Short Paper: IP Spoofing Detection for Preventing DDoS Attack in Cloud Computing, 2015 18th International Conference on Intelligence in Next Generation Networks, 978-1-4799-1866-9/15/$31.00 ©2015 IEEE 2015 P-139 to 141.

[7] J. Cheng, H. Wang and K.G, "Hop-count filtering: an effective defense against spoofed DDoS traffic," In Proceedings of the 10th ACM conference on Computer and communications security, USA, pp.30-41. October 2003.

[8] F. Y. Lee and S. Shieh, "Defending against spoofed DDoS attacks with path fingerprint," Computers & Security, 24(7), pp.571-586, 2005.

[9] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 21-22 (2012). FTC Chairwoman Edith Ramirez Privacy and the IoT: Navigating Policy Issues International Consumer Electronics Show Las Vegas, Nevada January 6, 2015. Opening Remarks.

[10] Vandana c. koradia, Modification In Advanced Encryption Standard Journal Of Information, Knowledge And Research In Computer Engineering, ISSN: 0975 – 6760| NOV 12 TO OCT 13 | VOLUME – 02, ISSUE – 02, P-356-358.