SMARTIE: A SECURITY SOLUTION FOR A SMART CITY USING INTERNET OF THINGS - ARCHITECTURE REFERENCE MODEL

Ashwin V. Didolkar[1], Fazeel I.Z. Zama[2]

[1] *Student, M.Tech. Final semester, Department of Computer Science and Engineering, Wainganga College of Engineering and Management, Nagpur, Maharashtra, India*
[2] *Head of the Dept., Department of Computer Science and Engineering Wainganga College of Engineering and Management, Nagpur, Maharashtra, India*

ABSTRACT

If the fact is considered 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. In the vision of the Internet of Things; IoT-Architecture wants to promote, a high level of interoperability that needs to be reached at the communication level as well as at the service and the information level, going across different platforms, but established on a common grounding. The designers of any distributed network system require the ability to study the system operations under a variety of scenarios before actually implementing them. Similarly, designers of a distributed transaction processing system need to study the performance of the system under a variety of load models as well as its time and response to failure conditions. Thus, the Internet of Things – Architecture Reference Model creates many opportunities for more direct integration and interaction; resulting in improved accuracy, efficiency and economical benefit.

This is what is the main crux behind this project while it is an attempt made at constructing a simulation model using Network Simulator version:2 simulating use of heavy cryptographic algorithm protocol enhancing the security to another level and thus achieving privacy preservation and coordination among devices with a mobile ad hoc network i.e. MANET which is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly using AODV i.e. Ad hoc on demand Distance Vector as the routing protocol which establishes a route to a destination only on demand. This is thus an earnest and a sincere attempt using new techniques for enhancing and upgrading what the base paper SMARTIE may or may not perceive at all.

Keyword: - *SMARTIE, MAES, NS2, MANET, AODV, Heterogeneous devices and data sources, etc….*

1. INTRODUCTION

Urbanization is not just merely a modern phenomenon, but a rapid and historic transformation of human social roots i.e. a gradual increase in the shift in the proportion of human population from a rural to an urban area based on a range of relevant disciplines that bring about enormous changes to human physical, social, economic and environmental circumstances i.e. right from the first settlements of hunter gatherers to the settlements founded on bloodlines, intimate relationships and communal behavior to the settlements with unknown, distant bloodlines, unfamiliar relationships and competitive behavior. This usually happens across a political boundary where according to 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. not enough work or jobs, city life) 4. Cultural (e.g. marriage, religious freedom, education). This started the need for smarter communication after which how everything started to change rapidly has been explained very precisely. The Internet of Things term was coined by Kevin Ashton executive director of Auto-ID Center which was opened to be a

research-oriented successor to the MIT Auto-ID Center, found by Kevin Ashton, David Brock and Sanjay Sarma, in the year 1999.The reference number should be shown in square bracket During 2003-2004, the term was mentioned in main-stream publications like The Guardian, Scientific American and the Boston Globe. Projects like Cooltown, Internet0 and the Disappearing Computer initiative seek to implement some of the ideas and the Internet of Things term started to appear in book titles for the first time. In 2005, the IoT hit another level when the UN'S International Telecommunications Union ITU published its first report on the topic. In 2008, the recognition by the EU and the first European IO conference was held. According to Cisco Internet Business Solutions Group IBSG, the Internet of Things was born in between 2008 and 2009 at simply the point in time when more things or objects were connected to the Internet than people. 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. 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.

While realizing a smart city, there is a close to real or virtual environment. This environment consists of discrete scenarios of any network of smart objects. These smart objects i.e. human beings, animals, machines, etc. make themselves recognizable and they obtain intelligence thus forming unique identifications are then embedded with many electronic circuits, computer softwares, actuators, sensors, etc. which brings to the fact that they can communicate information about themselves. They can access information that has been aggregated by other things or they can be components of complex services enabling collection and exchange of data either by sensing or by controlling them remotely across the networking infrastructure. Thus, this is the Internet of Things.

A Reference Architecture (RA) can be visualized as the "Matrix" that eventually gives birth ideally to all concrete architectures. For establishing such a Matrix, based on a strong and exhaustive analysis of the State of the Art, we need to envisage the superset of all possible functionalities, mechanisms and protocols that can be used for building such concrete architecture and to show how interconnections could take place between selected ones. Thus, the Architecture Reference Model; ARM is the combination of the Reference Model and the Reference Architecture, the set of models, guidelines, best practices, views and perspectives that can be used for building fully interoperable concrete IoT architectures and systems. data is information. A data set is homogeneous if it is made up of things (i.e. people, cells or traits) that are similar to each other. They relate to the validity of the often convenient assumption that the statistical properties of any one part of an overall dataset are the same as any other part. For example, a data set made up of 20-year-old college students enrolled in Physics 101 is a homogeneous sample. The opposite of homogeneous is heterogeneous data. A heterogeneous data is the data from any number of sources that are unlimited but largely unknown and in many discrete formats. In a similar way, a heterogeneous network is a network connecting computers and other devices or people by using different driver system softwares – drivers, operating systems, etc. that also use different protocols or algorithms. Analogously, a heterogeneous hardware system may consist of multiple functionality on a single hardware with embedded softwares. But, the deployment and the implementation part, is a very costly and time consuming and enormous task that may involve a considerable amount of human population. Hence, the designers of any distributed network system require the ability to study the system operations under a variety of scenarios before actually implementing them. Similarly, designers of a distributed transaction processing system need to study the performance of the system under a variety of load models as well as its time and response to failure conditions.

2. OBJECTIVES

The main aim of this project is to provide a very strong solution system for the secured sharing of trusted data, for any number of secured communication taking place amid any number of heterogeneous devices and data sources using new and improved encryption and decryption technologies as derived from the already established existing technologies and from the ever changing Internet of Things – Architecture Reference Model. This allows to focus on the specific goals that are to be attained and realized using this project as under: -

2.1. Requirements and Architecture:

- Deliver by providing a common framework supporting data sharing across applications, with a secured and trusted platform for not just identifying but also securing any privacy requirements may be very personal, business or even legal.

- Then deriving the technical requirements and setting secure policy parameters for such a data storage and retrieval, processing and even sharing thus, emphasizing on reusability.

2.2. Analysis and Design:

- Develop new technologies using the already established existing technologies and the ever changing Internet of Things – Architecture Reference Model.
- It may be noted that here any of the weakest links determine the security and hence trustworthiness must already be accomplished.
- Adapt to the security policies and mechanisms based on the requirements at runtime on demand only.
- Thus, achieve encryption and decryption of data using heavy cryptographic protocols and processing for offering only trustworthy data and its secure communication between the devices using the platform.

2.3 Developed components:

- Firstly, to achieve a proper and optimal use of such a colossal kind of trusted data visualize quickly before deployment or implementation in real time, using simulation saving cost and time and space.
- Secondly, to protect and then secure such a massive amount of trusted data use heavy cryptographic protocols while avoiding unpredictable varying overhead.

2.4 Advantages:

This project has been planned and designed in such a way so as to meet the specific demands of any number of communication for any amount of data.

1. For individuals or even group of people practicing big businesses, this project may prove to be much profitable and tremendously helpful in terms of the costs involved in the data exchanges.
E.g.: - Different Local Area Networks connecting any number of PC i.e. Personal Computer nodes having different operating system softwares or protocols or hardware.

2. For individuals or even group of people engaged in administrative matters, this project may turn out to be a boon by saving the much needed time for the deployment and implementation and other works if there are chances of involvement of any category of authority for matters of importance.
E.g.: - In times of any kind of war, communication in between army, navy or the air force of one nation may require communication only from some specific information source nodes for some specific time.

3. The project's security policies and mechanisms across domains will be based on the requirements at runtime.
E.g.: - In times of crisis in the widely populated areas of cities, this project may help manage any emergency vehicles through the traffic according to the secured communication done at that particular moment, to find the better path towards their destinations i.e. the accidents that may happen anywhere, anytime.

4. Even when there is poor coordination among all the network infrastructure services from any communication sources to their destinations, the project will work even if approximately large amount of time may be consumed to achieve some task if required.
E.g.: - In such situations when in between any sources and any destinations, if any nodes moves or may temporarily loose connectivity or it may happen that a part of the network is taken off the already defined position for some maintenance still, finding an alternative path this project will successfully achieve communication anyhow like the situation when one power grid of a particular area of a city fails but others may still stand and communication may even happen normally if at all with some time or space constraints.

2.5 Disadvantages:

Even if this project proposes to work on the predefined specific lines of actions, it may not always adapt successfully to the ever changing Internet of Things – Architecture Reference Model.

The most challenging disadvantage of this project is going to be its increasing complexity as its frequency of use will increase.
(E.g.): - The communication regarding some natural disasters forecast from many nodes of damaged areas to nodes in other areas.

Again, when in some situations when there may be poor coordination among the communicating heterogeneous devices and data sources, if the alternative routing path also fails, the system may also fail.
(E.g.): - The failures in the Railways reservation system might be the best examples for such emergency circumstances.

It is a known fact that things never remain the same i.e. change is inevitable after some work experience over some time, likewise it is asserted that constant efforts will be taken in the proper direction for increasing the efficiency and accuracy of this project without any variations to its already maintained quality. The vision of SMARTIE (Secure and sMARter ciTIEs data management) [1] is to create a distributed framework for IoT-based applications storing, sharing and processing large volumes of heterogeneous information. Recent advances in wireless communications and pervasive computing are driving the constant development of the so called Internet of Things (IoT) [2], providing ubiquity and intelligence to our surrounding environment. in order to obtain end-to-end connectivity between constrained devices and any entity connected to the Internet [3][4]. These adjustments are based on header compression and encapsulation mechanisms. Moreover, the CoRE WG was specifically founded to define an application layer protocol for resource constrained devices. As a result, the Constrained Application Protocol (CoAP) [5] was designed. However, current security and access control solutions were not designed with these aspects in mind and they are not able to meet the needs of these incipient ecosystems regarding scalability, interoperability, lightness and end-to-end security.

These mechanisms are integrated and extended with other standard security technologies in order to support smart objects during its life cycle. Furthermore, such mechanisms are framed within a security framework which is compliant with the Architectural Reference Model (ARM), recently presented by the EU FP7 IoT-A initiative 1. The proposed framework is intended to provide a holistic security approach to be leveraged by IoT devices throughout their life cycle. Additionally, a set of evaluation results was analyzed and discussed to demonstrate the suitability of the proposed mechanisms. Mandal et al. [6] worked on performance evaluation of cryptographic algorithms: DES and AES. These algorithms take significant amount of computing resources such as simulation time, memory usage and level of encryption are of major concern. In AES, avalanche effect is high as compared with the DES which is used in the financial applications. The more research can be done in the field of image and provide more security to the system. Urbanization, pollution – air, water, soil, etc., health – human and animal in general the basic needs, the quality of life and sustainability i.e. the constantly changing environmental balance has tremendously affected the daily lives of humans and animals thereby prompting to constantly search for the best solutions to a better life.

Privacy Preservation-

In today's world, there are innumerable number of heterogeneous devices that are capable of discovering and reporting the locations that they are at but, a considerable number of users using these devices may shy away from doing so in the fear of being tracked or profiled by any of their service providers.This problem may even be even more evident when the service provider wishes to outsource the spatial services to the cloud.

To resolve this problem, a very simple but unique solution may be required as under-

- Firstly, any node that wishes to communicate is assigned a unique identification token number or key.
- Secondly, that key is XORed with the resultant key of the Advanced Encryption Standard Algorithm generated key, thus making it more robust and secure.

This way, communication is thus secured from external threats. Poor coordination among all the network infrastructure features and services from a communication source to its destinations- The whole world is increasingly connecting today; coming closer day by day.

- There may be situations where the users of the heterogeneous devices may travel.
- They may temporarily lose connectivity and more often even worse problems pertaining to poor latency and bandwidth may arise.
- There may be even many situations when just temporarily a part of the whole network may be taken off for some maintenance.

This type of problem may be resolved –

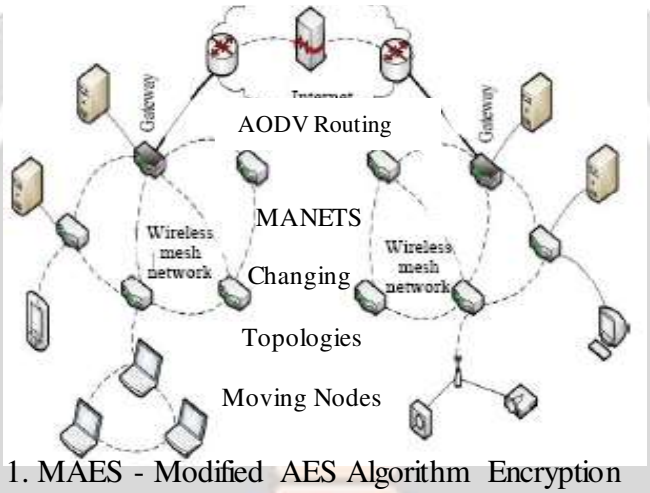
- Just by assigning a different node that is ready to communicate in the network such that it comes within the path of the ongoing communication that has failed.
- This way an alternative path is generated after the source node goes out of the communication boundary of the existing network infrastructure paving the for the new node.

Thus, these two points together form many major problems for the smarter network security solution for any Smart city.

SYSTEM ARCHITECTURE MODULES:

- A GRID OF SMART MOVING NODES
- SMART COMMUNICATION AND ROUTING PROTOCOL - AODV
- SMART SECURITY USING HEAVY ENCRYPTION AND DECRYPTION ALGORITHM – MAES
- SMARTER NETWORK SECURITY AND PRIVACY PRESERVATION

SMARTIE IOT - ARM SILUMATED SYSTEM



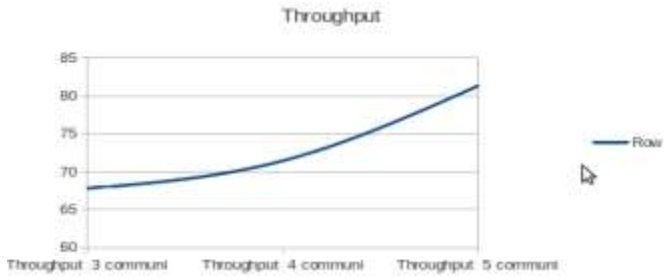
1. MAES - Modified AES Algorithm Encryption
2. Privacy Preservation

Figure: 5.5 SMARTIE System Architecture

5. CONCLUSION AND FUTURE WORK

The simulation and the resultant graphical output representations for communication in between the various nodes of the network, show why this idea may be of much help for the network security of a Smart city. In this thesis for the project titled "SMARTIE: A SECURITY SOLUTION FOR A SMART CITY USING INTERNET OF THINGS - ARCHITECTURE REFERENCE MODEL" as envisioned, a city data platform that allows data processing and sharing while protecting the security and privacy, it seems that implementing heavy cryptographic protocols onto a Cloud may give SMARTIE the required boost, robustness and stability that it wanted to realize in reality without any additional performance overhead but only using specific new enhanced and modified techniques. As the final comparison results came out on the Graph Analysis module which were as under:

Throughput Line Graph:



These graphs are based on the following actual value averages mentioned in the table for Throughput values, as under:

Time	Throughput 3 commu.	Throughput 4 communi	Throughput 5 communi
1	100	100	100
1.00124	45.283019	45.283019	45.283019
1.00556	45.283019	45.283019	100
1.0073	100	100	100
1.0088	100	100	45.283019
1.00921	100	100	100
1.01061	45.283019	100	100
1.01195	100	45.283019	100
1.01311	100	45.283019	45.283019
1.01366	45.283019	100	45.283019
1.01467	45.283019	45.283019	100
1.01469	45.283019	100	45.283019
1.01656	100	45.283019	45.283019
1.0172	45.283019	100	100
total	1016.981133	1071.698114	1071.698114
final	67.798742	71.44654093	71.44654093

Table: 1. Throughput values.

This Project's Network Security architecture features concretely adapt in and completely follow the Internet of Things-Architecture Reference Model. Thus privacy preservation is successfully realized using simulation results. The future work regarding such a result is to implement this work in the applications on the cloud.

6. REFERENCES

[1]. SMARTIE Project: Secure IoT Data Management for Smart Cities By Jens-Matthias Bohli, Antonio Skarmeta, M.Victoria Moreno, Dan García, Peter Langendbrfer- 2015.

[2]. L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Elsevier Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.

[3]. N. Kushalnagar, G. Montenegro, and C. Schumacher, "Ipv6 over low power wireless personal area networks (6lowpans): overview, assumptions, problem statement, and goals," RFC4919, August, vol. 10, 2007.

[4]. A. J. Jara, M. A. Zamora, and A. Skarmeta, "Glowbal ip: An adaptive and transparent ipv6 integration in the internet of things," Mobile Information Systems, vol. 8, no. 3, pp. 177–197, 2012. Jose L. Hernandez, Antonio J. Jara, Leandro Marinc and Antonio F. Skarmeta G6meza. DCapBAC: Embedding Authorization logic into Smart Things through ECC optimizations. International Journal of Computer Mathematics, 1-22, 2014.

[5]. Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (coap)," IETF RFC 7252, vol. 10, June 2014.

[6]. A.K. Mandal, C. Parakash, A. Tiwari, Performance evaluation of cryptographic algorithms: DES and AES, in: IEEE Students' Conference on Electrical, Electron- ics and Computer Science, 2012, pp. 1–5.