Research article Available online www.ijsrr.org ISSN: 2279–0543

International Journal of Scientific Research and Reviews

Survey of Internet of Everything with Trusted Security

E. Padma

Research Scholar, Department of CSESCSVMV (Deemed to be University), Enathur
Email: mailtopadma@kanchiuniv.ac.in

ABSTRACT*:*

In the area of Internet of Everything the foundation of "Internet of Things" can be carried over by the network intelligence which allows convergence, orchestration and visibility across disparate systems. The authentication can be done with the sensors and the devices which are connected with the various systems. The main objective of the proposed system is to contribute the attestation for the interconnected system. The concept of Internet of Everything emerged as a natural development of the IoT movement. IoE encompasses the wider concept of connectivity from the perspective of modern connectivity. The security feature enhances the interconnected system with authentication. Each interconnected devices must be authenticated before it connect with sensor. The system will be highly protected with three way authentication scheme. One way authentication can be carried over with protection of registered system with high protected security technique. As a case of Internet of Everything all the sensor devices which are connected with the registered system will be given more secure feature with random number generation. The number will be sent with encrypted key value. The proposed system will maintain the authorized user to access the information from the interconnected sensor devices.

KEYWORDS: Internet of Everything, Attestation, Authentication, Sensors, Security, Encryption

***Corresponding author:**

E. Padma

Research Scholar, Department of CSESCSVMV

(Deemed to be University),

Enathur

Email: mailtopadma@kanchiuniv.ac.in

1. INTRODUCTION

The Internet of Everything (IoE) is a broad term that refers to devices and consumer products connected to the Internet and outfitted with expanded digital features. It is a philosophy in which technology's future is comprised of many different types of appliances, devices and items are connected to the global **Internet**. The “Internet of Everything” builds on the foundation of the “Internet of Things” by adding network intelligence that allows convergence, orchestration and visibility across disparate systems. The concept of Internet of Everything emerged as a natural development of the IoT movement. IoE encompasses the wider concept of connectivity from the perspective of modern connectivity technology use-cases**.** IoE comprises of four key elements including all sorts of connections imaginable as People, Things, Data and Process. People expand the feature with connected end nodes across the internet to share information and activities. Examples include social networks, health and fitness sensors, among others. Things consist of Physical sensors, devices, actuators and other items generating data or receiving information from other sources. Examples include smart thermostats and gadgets. Data comprise of Raw data analyzed and processed into useful information to enable intelligent decisions and control mechanisms. The security feature enhances the interconnected system with authentication. Each interconnected devices must be authenticated before it connect with sensor. The system will be highly protected with three way authentication scheme. One way authentication can be carried over with protection of registered system with high protected security technique. As a case of Internet of Everything all the sensor devices which are connected with the registered system will be given more secure feature with random number generation. The number will be sent with encrypted key value. The proposed system will maintain the authorized user to access the information from the interconnected sensor devices. Examples include temperature logs converted into an average number of high-temperature hours per day to evaluate room cooling requirements. Process Leverage connectivity among data, things and people to add value. Examples include the use of smart fitness devices and social networks to advertise relevant healthcare offerings to prospective customers. IoE establishes an end-to-end ecosystem of connectivity including technologies, processes and concepts employed across all connectivity use-cases. Any further classifications – such as Internet of Humans, Internet of Digital, Industrial Internet of Things, communication technologies and the Internet itself will eventually constitute a subset of IoE.

2. PROPOSED METHODOLOGY

In Proposed system, the authentication can be dealt with registered machine in the network area. The machine once got registered, it will be identified for the uniqueness with its MAC Address. Each user will be given separate username and password. The authentication can be done with the sensors and the devices which are connected with the various systems. The main objective of the proposed system is to contribute the attestation for the interconnected system. The concept of Internet of Everything emerged as a natural development of the IoT movement. IoE encompasses the wider concept of connectivity from the perspective of modern connectivity. The security feature enhances the interconnected system with authentication. Each interconnected devices must be authenticated before it connect with sensor. The system will be highly protected with three way authentication scheme. One way authentication can be carried over with protection of registered system with high protected security technique. As a case of Internet of Everything all the sensor devices which are connected with the registered system will be given more secure feature with random number generation. The number will be sent with encrypted key value. The proposed system will maintain the authorized user to access the information from the interconnected sensor devices. Internet of Everything will connect the authorized user with sensor device. Each user will be given identity with high security password. The sensor device stores the information in the encrypted key format. The encryption will be extracted for decrypted using Data Encryption Standard Algorithm. If the user without registering in the network wants to access the information, he will use the secondary machine, in order to identify the unregistered user's entry he will be sent with an OTP as second way authentication. To access the encrypted information from the cloud the user will be sent with 12 digit random number to his mail id which will be an additional identity for the trusted user. The system got protected with full secure enhancement feature to avoid Dos Attack. In the proposed system, the information is in the cloud server with the encrypted format using Advance Encryption Standard Algorithm. Man in the middle attack causes no vulnerability to the proposed system, as the attacker want to communicate as a normal user also he will not be allowed to access the system. The proposed system has been protected with 12 digit random number for the valid user. Information is transferred from one end to other end using simulation environment.

3. LITERATURE REVIEW

[1] IoE is based on the idea that in the future, internet connections will not be restricted to laptop or desktop computers and a handful of tablets, as in previous decades. Instead, machines will generally become smarter by having more access to data and expanded networking opportunities. Actual IoE applications range from digital sensor tools/interfaces used for remote appliances to smarter and

more well-connected mobile devices, industrial machine learning systems and other types of distributed hardware that have recently become more intelligent and automated. IoE features fall under two main categories: Input which allows analog or external data to be put into a piece of hardware. Output allows a piece of hardware to be put back into the internet. The IoE term is driving much discussion about IT's future. For example, organizations like Cisco use the term in its branding to refer to the potential of modern and future technology.

[2] The “Internet of Everything” builds on the foundation of the “Internet of Things” by adding network intelligence that allows convergence, orchestration and visibility across previously disparate systems. Luke Simmons provides an ample real life example explaining internet of everything vs. internet of things on cloudrail.com. He quotes-“The Internet of Everything connects up all of these separate concepts into one cohesive whole. It’s not just about allowing devices to talk to each other; it’s about allowing everything to talk about each other. In some ways, you can see the Internet of Things as the equivalent of a rail road line, including the tracks and the connections, whereas the Internet of Everything is all of that, and the trains, ticket machines, staff, customers, weather conditions, etc.” IoE is somewhat synonym to IoT but not the same. The website defines Internet of Everything as “a broad term that refers to devices and consumer products connected to the Internet and outfitted with expanded digital features. It is a philosophy in which technology’s future is comprised of many different types of appliances, devices and items connected to the global Internet.”

[3] The Internet of Everything (IoE) is the essential prerequisite for the creation of virtual communities and ecosystems of institutions, communities and smart objects. IoE is built on the connections among people, processes, data and things. IoE are explicitly linked to global higher education (HE) and betterment to economic development, new research and innovation. Significant numbers of learning activities are moving to individualized proliferation of ebooks, e-readers, etextbooks, elearning and e-everything where transition to "hybrid" classes that combine online learning components with less-frequent on-campus, in-person class learning becomes more and more the norm. Through mass adoption of IoE is expected to witness a shift in expert resources use in HE that allows more people to gain access to education, regardless of their learning background. IoE adaptation in HE and the ubiquitous connectedness will transform the pedagogy towards one that empowers a new generation of digital citizens who understand the technologies that underpin IoE, but the impact of widespread adoption, and the right application of the information need yet to be understood. This article endeavours to discuss the evolving challenges of IoE adaptation in the HE including (1) access to right content and information and availability of materials on any device, at any time, (2) customization of curriculum to enable high/active engagement, interaction and attendance, and (3) to reduce the skills mismatch between what the labour force can do and what

employers need as indicators of success for IoE adoption in HE. To transform information into processes and products is necessary to gain from the sharing and use of knowledge. We analyze how an Internet of Everything that filter, select and distinguish relevant information to tailored student need enhances performance.

[4] Sensors are used in everyday objects such as touch-sensitive elevator buttons (tactile sensor) and lamps which dim or brighten by touching the base, besides innumerable applications of which most people are never aware. The use of sensor have expanded beyond the traditional fields of temperature, pressure or flow measurement, for example into MARG sensors. Moreover, analog sensors such as potentiometers and force-sensing resistors are still widely used. Applications include manufacturing and machinery, airplanes and aerospace, cars, medicine, robotics and many other aspects of our day-to-day life. A sensor's sensitivity indicates how much the sensor's output changes when the input quantity being measured changes. For instance, if the mercury in a thermometer moves 1 cm when the temperature changes by 1 °C, the sensitivity is 1 cm/°C (it is basically the slope Dy/Dx assuming a linear characteristic). Some sensors can also affect what they measure; for instance, a room temperature thermometer inserted into a hot cup of liquid cools the liquid while the liquid heats the thermometer. Sensors are usually designed to have a small effect on what is measured; making the sensor smaller often improves this and may introduce other advantages.

4. APPLICATIONS OF IOE

IoE is enabling organizations to engage with their customers in whole new ways and to create new business models. IoE is all about making new connections possible: interactions among people, and between people and devices. It’s also about the ability of devices to communicate with each other, with applications, and with digital services, and then empowering those technologies to take action based on these communications. Transform the process of building awareness and encouraging purchases, by bringing together data from various sources, including sensors that pick up signals to help anticipate customer needs. Target these customers in real time based on history, location, and activity. Apps move from performing cross-brand product comparisons to enabling customers to determine where to find items based on criteria they set, including best price, product ratings, and the most convenient retail location to shop. Connected vending machines, digital signage, and other surfaces will recognize customers and deliver customized content at the point of need. Items will be ordered on — and delivered to — a customer’s mobile phone, wherever it is located.

4.1 Properties of IOE

- Unique addressable object

- Unique location within a network
- Information-processing by machines surpasses humans as networks join up
- Complex interoperability of networks will require intelligent analytics, security and management
- Time and location takes on new meaning as real-time ambient intelligence becomes the norm

4.2 Sensors in IOE

Sensor technology and adoption have evolved to the point of having too many sensors with the internet of everything, with elements of sensors for data collection, big data analytics, sophisticated mobile and web applications, integrated with operational elements of customized delivery services. Sensors range from throw-away, single-use models to MEMs and RFID solutions. They can be apps on mobile phones to gadgets that are wearable or not to sensors attached to and even inside our bodies. Integrate the sensor hardware and reports so that it is integrated with applications and analytics. Create sensors that collect only the relevant data for specific purposes, short-term and long-term. Manage the sensor development project so that each individual sensor solution is cost effective and also customized to the needs of the user.

4.3 Responsibilities of Sensors

Retail: Beyond knowing what you purchased, stores will monitor your eye gaze, knowing what you glanced at… what you picked up and considered, and put back on the shelf. Dynamic pricing will entice you to pick it up again. **City Traffic:** Cars looking for parking cause 40% of traffic in city centers. Parking sensors will tell your car where to find an open spot. **Lighting:** Streetlights and house lights will only turn on when you're nearby. **Transportation:** Self-driving cars and IoE will make ALL traffic a thing of the past. **Healthcare:** You will be the CEO of your own health. Wearables will be tracking your vitals constantly, allowing you and others to make better health decisions.**Invisibles:** The next big thing is sensor-based technology that you can't see, whether they are in jewelry, attached to the skin like a bandage, or perhaps even embedded under the skin or inside the body. In Future, 30% of wearable will be ***"unobtrusive to the naked eye,"*** according to market researcher Gartner. The Internet of Everything will become the nervous system of the human economy.

5. CONCLUSION

The proposed system concludes with the security feature for interconnected devices. The authorization has been carried over for the authenticated and registered system. The attestation key has been generated for each individual user. The user will be identified with MAC Address of the machine. The primary machine will check for the user identity. The secondary machine will be identified with interconnected network system. The authenticity for the secondary machine will be done with One Time Password as a security enhancement feature. The authentication way has been carried over with Data Encrypted Algorithm. The web layer and access layer had been verified for the user authenticity.

6. REFERENCES

WEB REFERENCE

1. https://www.techopedia.com/definition/30121/internet-of-everything-ioe
2. https://internetofthingswiki.com/internet-of-everything-explained/690/
3. https://en.wikipedia.org/wiki/Sensor
4. http://Fountain Blue’s Blog Marketing Leadership in an Age of Personalization February 17 2018.
5. https://blog.hubspot.com/marketing/internet-of-things-examples
6. https://en.wikipedia.org/wiki/Network_simulation.
7. https://searchsecurity.techtarget.com/definition/botnet.
8. https://www.nortonsecurityonline.com/security-center/bots.html.

JOURNAL ARTICLE

1. I. Bandara, F. Ioras , “The Evolving Challenges Of Internet Of Everything: Enhancing Student Performance And Employability In Higher Education 10th annual International Technology, Education and Development Conference DOI: 10.21125/inted.2016.1158
2. Timothy W. Smith Architect, “Internet of Everything (IoE) Mobility”, A Survey Paper January 15, 2014.
3. Sarah Wheeler, “IoE vs. IoT vs. M2M: What’s the Difference and Does It Matter?” A Survey Paper January 2016; 20.
4. Dave Evans, “The Internet of Everything and How It Will Change the World, 21st Century Tech - A Look at our future” Cisco IBSG April, 2015; 20