# Security Framework for SWS Using IoT

[1]Dr. P Bindhu Madhavi, [2]Rahul B, [3]Rintumol M Thomas
[1] Professor & Head, Department of Information & Science Engineering,AMCEC,Bengaluru
[2,3] Assistant Professor, Department of Information & Science Engineering,AMCEC,Bengaluru

***Abstract-*** *The Internet of Things (IoT) will associate not just PCs and cell phones, however it will likewise interconnect keen structures, homes, and urban communities. The IoT exploit the most recent correspondence innovations with a specific end goal to give ideal and solid administrations to Smart Cities (SC). The foundation of SC is the Critical Infrastructures, for example, the city's water framework. In SC, the water framework profits by the improvement of mechanization and correspondence advancements to make keen situations which are more proficient in the utilization of the accessible assets; we call it Smart Water System (SWS). In this paper we exhibit a multilayer engineering to coordinate the SWS to the IoT, making it accessible from wherever whenever. Nonetheless, with the presentation of IoT we will encounter stupendous difficulties to secure and ensure its propelled data benefits because of the huge increment of the assault surface, unpredictability, heterogeneity, and number of interconnected assets. We additionally present an IoT Framework for SWSs to construct dependable and secure applications and administrations. The structure empowers designers to consider security issues by any stretch of the imagination IoT layers and coordinate security calculations with the capacities what's more, administrations offered in each layer as opposed to thinking about security in a specially appointed and after idea way. Indicating how this structure can be utilized to grow profoundly secure and dependable SWS administrations and how to apply our Anomaly Behavior Analysis approach to secure and ensure these administrations against any kind of assaults.*

***Keywords***- Internet of things, Smart City, Smart Water, Anomaly Behavior Analysis.

## I. INTRODUCTION

EVOLUTION in versatile and unavoidable figuring, social arrange advances, and the exponential development in Web applications and administrations will prompt the advancement of the up and coming age of (Internet of Things, IoT) that are inescapable, omnipresent, and touch all parts of our life [1]. It is normal that the quantity of IoT gadgets will achieve more than 50 billion gadgets by 2020 [2]. Be that as it may, the reconciliation of physical and digital frameworks and in addition the human practices what's more, co-operations (e.g., makers, purchasers, and aggressors) will drastically build the helplessness and the assault surface of associated framework biological systems [3].

In this paper, we center around one developing IoT benefit related with Smart Water Systems (SWS) that will have real security issues. For instance, present day brilliant foundations, (for example, the SWS) are controlled by complex disseminated frameworks involving huge measure of heterogeneous hubs with rich availability gave by inside systems furthermore, Internet. With the exponential increment in frameworks insight and network, security and protection have turn into the primary worries for brilliant frameworks [3]. Scientists have demonstrated that Smart Infrastructures (SI) can be assaulted from an assortment of interfaces including physical access for example, USB, and remote channels. Besides, by trading off a solitary control unit, a skilled assailant may access different units by means of inside interchanges, for example, the supervisory control and information procurement (SCADA) framework also, assault basic subsystems [3]. As SCADA gets interconnected with IoT assets and administrations, it moves toward becoming simple focuses to digital enemies, particularly since it was never intended to deal with digital dangers. This makes SI information defenseless against distortion assaults that prompt off base data conveyance to clients, and therefore making them take wrong and risky activities or to be unconscious of a continuous assault similar to the case in Stuxnet assault [4]. It likewise permits foes to conceivably execute pernicious charges on SI's control frameworks, causing unsafe activities (e.g. open security valves) [4][5].

In this work, we center in digital assaults focusing on savvy urban communities' water conveyance framework that is incorporated to the IoT; we call it Smart Water System. We initially present our IoT various leveled engineering that can be utilized to convey IoT applications. We at that point stretch out that design to our IoT System. The principle goal of presenting our structure is to empower engineers to address security issues in a efficient way while outlining and building up each IoT layer. In our approach, IoT pecking order comprises of four layers: Application, Service, Communications, and End-Devices layers. By protecting for each layer that all current vulnerabilities and dangers can be distinguished and moderation arrangements will be connected, our system will give the compositional help to convey reliable

IoT administrations that can: 1) Protect IoT administrations against pestilence assaults; 2) Guarantee that basic IoT frameworks can survive issues and ruinous assaults; and 3) Ensure IoT security and protection.

## II. BACKGROUND

### A. Shrewd Infrastructures (SI)

The idea of a SI is picking up consideration driven by objectives of manageability and productivity. SI are getting to be self-checked, self-conveyed, and in particular self-administrated. Numerous variables have empowered this change, including supportability, asset administration, economy, fast improvement of data advances, and the advances in computational and correspondence frameworks [6]. While order and control issues are natural in any perplexing framework, the fundamental worry in SI is the need to convey solid benefits even under obliged assets.

### B. IoT Cyber Security

IoT can be seen as a pervasive system that empowers checking and controlling countless gadgets that are topographically scattered by gathering, handling, and following up on the information created by brilliant items[10]. It speaks to canny end-to-end frameworks that empower keen arrangements and spreads a various scope of innovations counting detecting, correspondences, and systems administration. [11].This various and dynamic utilization of assets has made security a significant test. Conventional IT security arrangements are most certainly not specifically appropriate to IoT because of the accompanying issues [10][11]: 1) The IoT expands the "web" through the conventional web, portable system, non IP systems, sensor arrange, distributed computing, and haze registering; 2) Computing stages, compelled in memory and preparing ability what's more, therefore may not bolster complex security calculations; 3) All "things" will speak with each other. This prompts numerous entrance indicates that can be utilized endeavor existing vulnerabilities; and 4) Some IoT gadgets and administrations might be shared and could have diverse proprietorship, strategy, and network areas. These difficulties should be tended to manufacture a safe and flexible IoT framework, where Secrecy, Integrity, and Availability (CIA) must be guaranteed. Subsequently, there is a solid research enthusiasm for securing and ensuring IoT and their administrations utilizing strong systems.

### C. Peculiarity Behavior Analysis

Current digital security arrangements are a long way from being attractive to stop the exponential development in number and intricacy of digital assaults [5]. What's more, the exertion furthermore, information required to dispatch advanced assaults is diminishing while their proliferation has been decreased from days in the mid-80s to a small amount of seconds in 2000s [6]. There are two fundamental interruption recognition systems to recognize cyber-attacks: signature based and peculiarity based Intrusion Discovery Systems (IDS). Mark based IDS fabricates a database of known assault marks or characters. In any case, these frameworks can't recognize new kinds of assaults or even a known assault with a slight change on its mark. The fundamental highlight of the oddity discovery approach is their ability in distinguishing novel and new assaults. The inconsistency based IDS characterizes a benchmark show for typical conduct of the framework through disconnected preparing and consider any action which lies outside of this ordinary model as irregularity [7]. Any assault, misconfiguration or abuse will prompt a deviation from the ordinary conduct; we name it as anomalous conduct. The principle confinement of this approach is the huge number of false alerts that can be delivered. To overcome this restriction, our approach performs fine-grain peculiarity conduct investigation as will be examined in additionally itemized when we present our ABA-IDS approach.

### D. Risk demonstrate

Enhancing security and diminishing dangers in keen frameworks vigorously relies upon investigating dangers, dangers, and vulnerabilities to build up the proper countermeasures and alleviate their misuses [8]. To better comprehend the IoT security scene, a general IoT danger display should be produced. A danger demonstrates characterizes risk situations with related hazard conveyances, probability of event, and effect. It helps in investigating security issues, outline moderation techniques, and assess alleviation arrangements. At the point when made in the outline stage, a risk show recognizes changes that should be made to the outline to relieve potential dangers.

At the point when a danger show is made for a conveyed framework, it can be utilized to organize the moderation activities. By and large, the ventures to make a general danger display are: 1) Identify assailants, resources, and dangers, 2) Rank the dangers, 3) Choose alleviation techniques, and 4) Build moderation arrangements based on these techniques. We will take after the previously mentioned ventures to make the danger demonstrate for our IoT structure and after that we will demonstrate to utilize it to secure and ensure our IoT passage.

## III. IoT ARCHITECTURE FOR SMART WATER SYSTEM

There are a few designs that can be connected to construct dependable administrations for brilliant foundations [6][8]. The IoT administrations for brilliant water can be produced utilizing our progressive design as appeared in Figure. The engineering comprises of four layers: IoT end gadgets, interchanges, administrations, and end clients/applications.

In figure 1: IoT progressive engineering for shrewd water administrations. In the main layer (end hubs), the data passes through physical gadgets to recognize or alter the physical world. This data incorporates protest properties, ecological conditions, and information. The key parts in this layer are the sensors for catching and speaking to the physical world in the computerized world, the actuators to change the condition to a coveted state, and a neighborhood controller to take quick activities when required [6][8].

The interchanges layer is in charge of the dependable transmission of data from/to end hubs [8][9]. The advancements utilized as a part of this incorporate the Internet, portable correspondence systems, arrange frameworks, and correspondence conventions. A key part in this layer is the secure portal, which is the purpose of access (locally) to the framework, to screen sensors or issue orders to the actuators.

The administrations layer goes about as an interface between the application layer in the best level and the system layer in the bring down level [7][8][9]. At this layer, all the required computational power is for the most part given as a cloud and additionally mists administrations. This layer is utilized for remotely observing and controlling the framework, and additionally to store information and dissect expansive measure of data. The application layer gives the customized administrations as indicated by the requirements of the client [7][8]. The entrance to the IoT administrations is through this layer and it can be by means of portable innovation, for example, cellphone, portable applications, or a brilliant apparatus or gadget. In this layer, information sharing is a critical trademark and therefore application security must address information protection and access control.

Aggressors may utilize any current powerlessness to get entrance to the framework and dispatch an assault; subsequently, is it vital to distinguish the potential vulnerabilities and the proper relief components. For example, an IP water stream sensor situated in a remote place can be effectively traded off to get unlawful data and to dispatch an assault (e.g. replay assault).

Since sensors ordinarily have low (or no) computational power, it is implausible to apply encryption systems which is a more appropriate approach is to verify every sensor and its information.

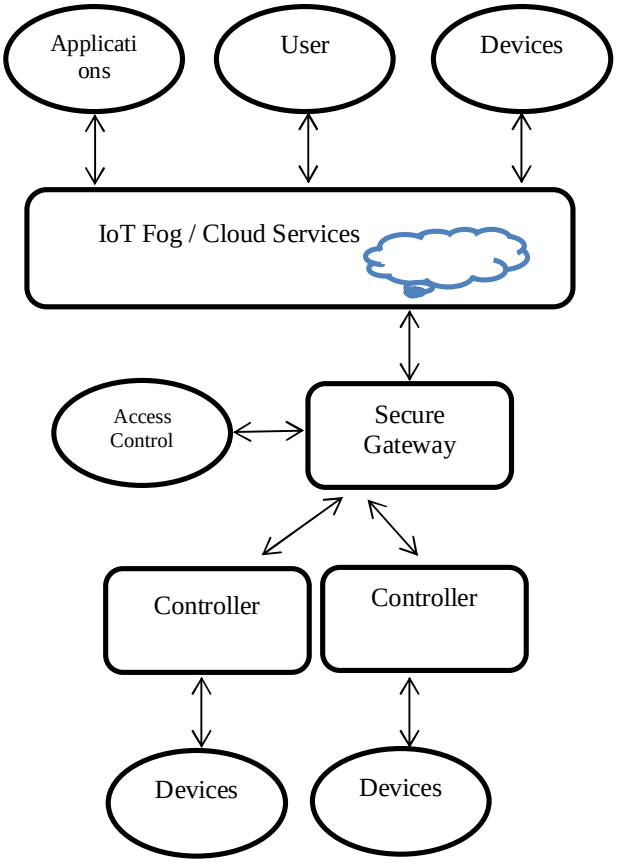


Figure 1: IoT hierarchical architecture for smart water services.

## SMART WATER SECURITY DEVELOPMENT FRAMEWORK (SWSDF)

The principle objective of the SWSDF is to give the building support to grow exceptionally secure and dependable SW administrations that can proactively distinguish and endure pernicious practices that can be because of assaults, shortcomings (malevolent or regular), or mishaps. To secure against a wide range of assaults, we require an all-encompassing way to deal with the plan and improvement of the SWS that will prompt the conveyance of put stock in applications and administrations [9]. We characterize a dependable administration to be the one that can secure and ensure the framework against cyber-attack (self-ensure), that

can keep on operating typically by meeting its execution prerequisites in spite of deficiencies and ruinous assaults (self-mending, and self-upgrading), and can refresh its design and security approaches to keep up security, protection, flexibility to issues and mischances, and quality of administration necessities (self-arrangement). The auto data security that should be kept up at all layers can be characterized utilizing [9]: 1) Authentication - It speaks to the implies by which principals safely recognize themselves to a framework, 2) Authorization (get to control) - It gives a component for restricting access by principals in view of their personality to esteemed assets, 3) Integrity - To distinguish whether a message or protest was altered or supplanted in an unlawful way, 4) Non-revocation - To demonstrate that specific principals have sent/gotten a specific message, and 5) Auditing - To find the succession of occasions that prompted an anomaly.

The SWSDF coordinates the advancement of savvy water administrations with security system at the plan and improvement arrange as appeared in Figure 2. Figure 2: SWSDF structure. The SWSDF is composed as 2-D design with four layers and each layer is actualized into five planes: Capacity Specification (demonstrate), Attack Surface, Impact, Relief, and Priority planes. For each layer, we first distinguish the Attack Surface (AS) that describes the section focuses that can be abused by assailants to infuse malevolent occasions or practices in the SWS condition, trailed by distinguishing potential effect of detonating the vulnerabilities.

At that point we distinguish the relief components that can be executed to reduce these assaults lastly we organize the administration as indicated by the potential effect to the framework. By following this design, we can guarantee the advancement of profoundly secure and reliable SWS administrations. In what tails, we depict the assault surface, affect, and moderation and need planes for each layer in our SWSDF system.

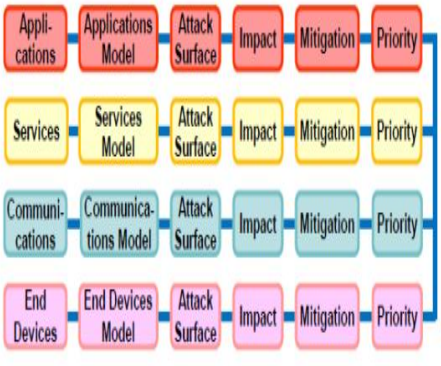


Figure 2: SWSDF framework

**Keen WATER SYSTEM TESTBED**

The SWS testbed contains all the required equipment (e.g, funnels, sensors, valves, and so on.) and programming to copy the primary water conveyance in a shrewd office (e.g., a keen building).

Water stream sensors are utilized to peruse the water utilization in constant. The data from the sensors is procured by an Arduino board [6] each millisecond however refreshed in memory each 5 milliseconds. The fundamental errands of the Arduino board are: 1) gather data from sensors, 2) investigate water utilization searching for variations from the norm, for example, spills or intemperate utilization, 3) trigger cautions in the event that a variation from the norm is identified, and 4) send the gathered data to the safe door (counting the cautions). A manual valve connected to a auxiliary pipe is utilized to reenact water spills, and an electric valve is utilized to begin the water stream in the fundamental pipe. On the off chance that a variation from the norm is recognized in the water stream, the Arduino actuates a visual caution (a red light), and sends the data to the safe passage. The protected passage is fabricated in a Raspberry PI framework. The fundamental errands of the Raspberry are: 1) get the data from the Arduino board, 2) Publish the data in the site facilitated in the same Raspberry, 3) empower Wi-Fi correspondence for neighborhood control/screen of the testbed, and 4) send all the data to the cloud. A perceptible normal for the protected door is simply the capacity of performing insurance by utilizing Anomaly Conduct Analysis. Keen Infrastructures coordinate self-governance and versatile control that can be utilized to better oversee assets in a city, building, or at home. SI interface controllers, robotization, data innovation, supportable advancement, security, what's more, correspondences (among different frameworks) to accomplish propelled data benefits that fundamentally decrease operational cost, enhance human solace, and diminish vitality utilization [6][7]. On account of the extensive variety of clients, interconnected frameworks, and ecological elements, the computational power expected to work SI is like that required in substantial scale server farms. One answer for satisfy the needs is Cloud Computing, which goes for giving computational power, stockpiling, and system administrations to end gadgets [8][9].

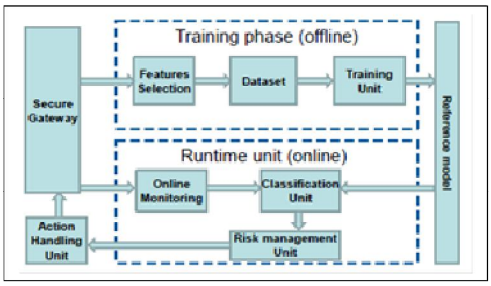


Figure 3: Anomaly Behavior Analysis Methodology

## IV. CONCLUSION

In this paper we have presented an IoT security system to coordinate a Smart Water Systems to the IoT security. The system comprises of four layers: gadgets, correspondence, administration, and application layers. We moreover displayed a philosophy to build up a risk demonstrate that can be used to distinguish potential assaults against each layer, their effects and how to relieve and recoup from these assaults. We demonstrated to utilize the risk model to secure and ensure our safe door which is a piece of the correspondence layer. Our inconsistency conduct investigation philosophy incorporates the utilization a profile that is produced to precisely describe the ordinary tasks of our entryway. We demonstrated that our ABA- IDS approach can recognize both known and obscure assaults with high identification rates and low false positive cautions (less than 3.4%), additionally having irrelevant overhead as far as memory and CPU use. Emphasize that our proposed procedure is expected to ensure the ordinary task of our safe entryway guaranteeing accessibility. As future work we are right now broadening our ABA procedure to alternate layers of the IoT security system.

## ACKNOWLEDGEMENT

We would like to take this opportunity to thank our guide Dr. P. Bindhu Madhavi (Professor and Head Dept. of Information Science & Engineering) for her inspiration and guidance on paper.

## REFERENCES

[1] Z. Andrea , B. Nicola, C. Angelo, V. Lorenzo, and Z. Michele, “Internet of Things for Smart Cities”, IEEE Internet of Things journal, vol. 1, no. 1, February 2014.

[2] Verizon (2017, April, 03). Internet of Things (IoT) solutions.Retrievedfrom:http://www.verizonenterprise.com/solutions/connected-machines/

[3] B., Ayan, K. Krishna, T. Mukherjee, and S. Gupta. “Ensuring safety, security, and sustainability of mission-critical cyber-physical systems.” Proceedings of the IEEE 100, no. 1 (2012): 283-299.

[4] D. Kushner, “The Real Story of Stuxnet, How Kaspersky Lab tracked down the malware that stymied Iran’s nuclear-fuel enrichment program”, IEEE Spectrum, February 2013.

[5] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, T. Kohno, “Comprehensive experimental analyses of automotive attack surfaces” USENIX Conference on Security, 2011.

[6] J. Jin, J. Gubbi, S. Marusic, and M. Palaniswami. “An information framework for creating a smart city through internet of things.” IEEE Internet of Things Journal 1,no. 2 (2014): 112-121.

[7] H. Ferreira, G. Cerqueira, E. Dias, and R. de Sousa. “IoT architecture to enable intercommunication through REST API and UPnP using IP, ZigBee and arduino.” In Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on, pp. 53-60. IEEE, 2013.

[8] M. Soliman, T. Abiodun, T. Hamouda, J. Zhou1, C.Lung, “Smart Home: Integrating Internet of Things with Web Services and Cloud Computing”, IEEE 5th International Conference on Cloud Computing Technology and Science, 2013.

[9] J. Pacheco and S. Hariri. IoT Security Framework for Smart Cyber Infrastructures. In Foundations and Applications of Self* Systems, IEEE International Workshops on, pp. 242-247. IEEE, 2016.

[10] P.B. Nassar, Badr Y., Barbar K., and Biennier F. “Risk management and security in service-based architectures.” In Advances in Computational Tools for Engineering Applications, 2009. ACTEA'09. International Conference on, pp. 214-218. IEEE, 2015.

[11] Shostack, Adam. Threat modeling: Designing for security. John Wiley & Sons, 2016.

[12] Y.A. Badamasi, “The working principle of an Arduino.” In Electronics, Computer and Computation (ICECCO), 2014 11th International Conference on, pp. 1-4. IEEE, 2016.