A Novel Cognitive Security Approach for Internet of Things

Kushal Kumar B. N. [1], Panduranga Rao M. V. [2]
[1] Research scholar, Department of CSE KSIT, VTU, Belagavi, India
[1] bn.kushalkumar@gmail.com
[2] Professor, Department of CSE, BTLIT Bengaluru, India
[2] raomvp@yahoo.com

***Abstract* --The Internet of Things (IoT) defined as an extremely interlinked network of heterogeneous devices where all kinds of communications are possible. Therefore, the security essential for such network becomes critical because the typical Internet security protocols identified as unusable in this type of networks, due to some classes of IoT devices with constrained resources. The IoT requires multifunctional security systems, which is protected with integrity, confidentiality, authentication and the network is protected against invasions, ructions and the data inside a sensor node. The cognitively it can learn from interactions with people and from experiences with their environment. It helps in reducing the complexity of the Internet of things is discovering data corrigibility. Cognitive security can drive the Internet of Things to heightened levels. This paper proposes cognitive security approach for internet of things network. The cognitive approach to improve the services provided to the user.**

Keyword- Internet of Things, Cognitive Security, Attacks**.**

I. INTRODUCTION

The Internet of Things (IoT) [1] is the network of physical objects or things entrenched with sensors software, and network connectivity. Kevin Ashton coined the term IOT. IoT observed as a technology and monetary wave in the global information industry after the Internet. The IoT is an intellectual network, which associates all things to the Internet for the perseverance of communicating and exchanging information through the information sensing devices in accordance with agreed protocols. IoT regarded as an extension of existing interaction between people and applications are by a new aspect of Things for communication. The IoT development process is a multifaceted large-scale technological innovation process.

The interconnection and communication, in the IoT model, empowers many applications in many domains. The development of Internet instigates with involving two computers together, later created the World Wide Web by connecting huge number of computers together. Mobile-Internet appeared when mobile devices were associated to the Internet. The Internet of Things developed, encompassed of everyday objects added to the Internet. IoT devices are accessed from anywhere via un trusted network like the internet so IoT networks are vulnerable against an extensive variety of malevolent attacks, thus, the security problems must be addressed. The attacks can be internal and external, the external attack, the attacker is not a part of the network while in an internal attack, can be originated by malevolent nodes that are part of the network.

The following are the potential attacks on IoT applications. In the Sinkhole Attack, malicious node attracts network transportation towards it. In these types of attack, a malicious node attracts all neighbouring nodes to headlong their packets through the malicious node by displaying its routing cost minutest. The attacker generates an attack by hosting deceitful node inside a network. In the Wormhole Attack, the adversary node produces a virtual channel between two ends. An adversary node deeds as an advancing node between two actual nodes. The malicious nodes prerogatives that, they are one hop from the base station. The wormhole attack used to persuade two divergent nodes that they are the neighbours by relaying packets between two of them. The hello flood attack occurs in the sensor network, the routing protocol transmits the hello message to proclaim its existence to its neighbours. A node, which obtains the hello message, may adopt that the source node is within its communication range and add this source node to its neighbour list.

Denial of Service (DOS) Attack can damage the availability of resources. When this attack occurred, the resources are not accessible to authentic users. In Selective Forwarding Attack, malicious node acts as a normal node but it selectively drops some packets. The numerous trends have emerged over the past several years that are functioning organized to outline the evolving IoT market. There is rapid growth of data and analytics capabilities enabled by cloud computing and rapid growth in smart mobile devices, growing interconnectivity among the smart mobile devices. The enterprise networks allows applications such as video surveillance, smart meters, asset tracking, digital health monitoring.

The data is generated in the IoT are by numerous categories of devices, managed in different methods. The IoT Orientation model is comprised of six levels. The IoT Orientation Model does not bind the opportunity or vicinity of its components. The IoT Orientation Model permits the dispensation happening at each, contingent on the condition. The model defines handing of the jobs at each level to preserve effortlessness, tolerate high scalability, and confirm supportability. It defines the functions required for an IoT figure 1 illustrates the IoT Orientation model. In the IoT, the data moves in both directions. The governor information flows from the top of the model to the bottom and the monitoring information flows in the reverse. In many systems, the movement will be bidirectional.

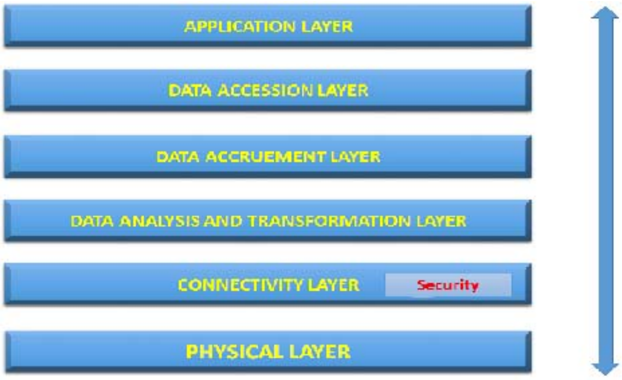

Figure 1: IoT Orientation model

The IoT Orientation Model starts with physical layer that might control multiple devices. They are the things in the IoT, and they comprise an extensive variety of endpoint devices that can send and receive information. Connectivity layer, its most important function is trustworthy, well-timed transmission of information and it includes transmissions between devices and the network across networks, between the network and low-level information processing occurring in the next layer.

The functions of data analysis and transformation layer is driven by the need to convert the network data drifts into information which is appropriate for storage and higher level processing at data accruement layer. This means that data analysis and transformation layer activities focus on high-volume data analysis and transformation. The Networking systems, designed for reliably transfer data. The data is moving through the network at the rate and organization determined by the devices generating the data. The model is event driven. As defined earlier, the devices do not include computing capabilities themselves. However, some computational activities could occur at connectivity layer, such as protocol transformation and application of network security strategy. Further, the tasks performed at data analysis and transformation layer, such as packet assessment. Driving computational tasks as close to the edge of the IoT as possible, with heterogeneous systems

IoT systems will need to scale to a corporate—or even global—level and will require multiple storage systems to accommodate IoT device data and data from traditional enterprise ERP, HRMS, CRM, and other systems. The data abstraction functions of data accession layer focuses on rendering data and its storage. It will allow developing simpler, improved performance application. In the application layer, the information interpretation occurs. Software at this level interacts with data accession layer and data at rest, so it does not have to operate at network speeds.

The cognitive architectural model for the IoT [2] is to obscure the technological heterogeneity and deliver services to diverse applications. The model involves of three levels of facilitators, as shown in figure 2, which are reusable to various-diverse applications. The every layer offers apparatuses for the registration, look-up and finding of objects, and the configuration of services, the virtual demonstrations of the real world objects created. The VOs are liable for keeping the means of communication to the RWOs, checking the eminence and apprehending the data from the objects. A cognitive mash-up of the VOs together forms the CVOs that render services based on the application requests. The arrangement of CVOs accelerates the salvage of the VOs in extensive variety of contexts. Cognitive technologies help to improve the resource usage by intelligent choice mechanisms, which optimizes to system requirements such as energy conservation, computational performance.

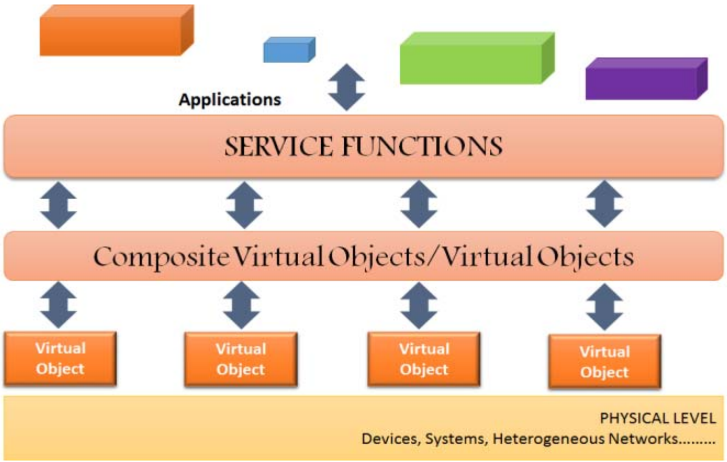

Figure 2: IoT cognitive architectural model

The service level is accountable for interaction and elicitation of requirements from service petitioners and users. This level comprises the functionalities of conversion of service requests, constructing real world knowledge and offers the necessary information down to the CVO level in order to make meaningful mash ups to assist the request. It also holds the acceptance criteria for the services thereby confirming the quality of the extracted services. One method of building the real world knowledge is to record the user's needs and requirements by accumulating and studying the user profiles, stakeholders contracts and eventually acting on behalf of the users. The real world knowledge model embraces the logic accountable for distinguishing and cognitive on the appropriate information and conducting associated knowledge driven decision-making.

II. MOTIVATION

IoT will create enormous network of billions or trillions of ―Things‖ interactive with one another are facing many practical and application challenges. There are enormous numbers of devices poised to go online in the coming years. The CISCO forecasting that, there will be a projected 50 billion by 2020.

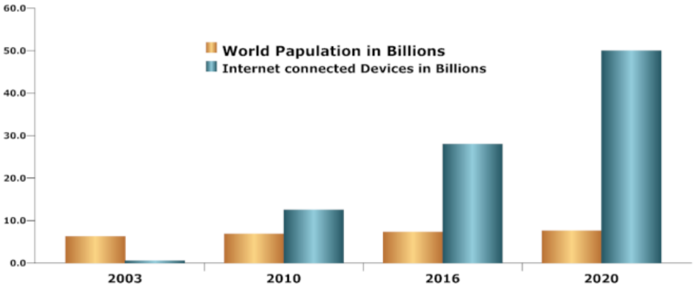

Figure 3: The Development in Internet Connected Objects by 2020

The Internet is associated with devices worldwide, consisting of computers, smart phones, and tablets. As showed in the figure 3, the number of things associated to the Internet surpassed the number of people on Earth. According to CISCO, each individual on globe will have more than six devices linked to the Internet by 2020. Therefore, the IoT will likely be one of the most imperative technological improvements of this decade. The Internet of Things is part of a greater evolving phenomenon that brings the newly associated devices with the existing connections of people, process and data. The growth of IoT must be, accompanied by robust security for things based resolutions. This demands that to find pioneering security mechanisms for the IoT.

III. LITERATURE SURVEY

The Internet of Things is a hybrid network of minute devices, WSNs, and the conformist Internet. Unlike, typical WSN where devices are resource constrained and unlike in the Internet where devices are powerful, the nodes or things in the IoT are heterogeneous devices. There are many scholars have been functioning on IoT to provide the better security mechanism. The following are the various approaches proposed in the recent years.

G. Chavan, et al., [3] proposed novel IDS to detect wormhole attack and in which implemented in Contiki OS with Cooja simulator. The proposed system uses centralized and distributed architecture for placement of IDS. In this approach, wormhole attack detected by using location information and attacker node identified by using neighbor information.

Diego Poplade et al., [4] proposed IDS to detect sinkhole attacks for IoT, executed in Cooja simulator. The proposed scheme describes four units. The first unit is Cluster configuration unit. It is responsible for categorizing a node like members, leaders and associated based on their network functions. The second one is observing of routing module. Observer node monitors the number of transmissions is accomplished. The third one is attacker detection module, which identifies the sinkhole attack. The fourth module is the separation of attacker module, which segregates the wicked node from the cluster and it notifies an alarm to inform its neighboring nodes. The simulation result illustrations that 92% detection rate is attained.

N. Dharini et al., [5] proposed a distributed detection approach to identify flooding and gray whole attacks in WSN and implemented with MANNASIM framework in NS2 simulator. In this approach, a lightweight energy prediction algorithm detects the anomalies of the nodes activities. In this system cluster head is responsible for energy prognostication for every nodes in the cluster. The attack can be, detected by irregularities between prognostication and actual energy. The detection accuracy achieved by obtaining high prediction accuracy.

Byung Gyu Kim et al., [6] proposed a method of improving proxy preparation reducing service connection deferral by implementing the provision of shared authentication of data and session key. Through experiments on a test bed, it confirmed that connection delay time could be, reduced by about 2.6 times in proportion to the message sizes.

Youngseok Chung et al., [7] proposed an anonymous authentication scheme for intercommunication between the things in the Internet of Things surroundings. The proposed system offers not only secrecy and security, but also intractability for the things.

Chen Jun et al., [8] proposed event processing IDS to decipher the problem of real time of IDS in IoT network. In this approach, they introduced the IDS architecture on the foundation of event handling model. It is also rule-based IDS where the rules are stored in rule pattern repository.

A. Babu Karuppiah et al., [9] proposed an energy efficient IDS to detect Sybil node in WSN. The proposed system describes two circumstances. The first case is centralized approach, implemented to send and reception of the request of data packets. The Cluster head preserves a table for accumulation of identified locations of every node. In the second case, all genuine nodes answer to the cluster head with their personalities and current location coordinates. Sybil node also sends their identities and current location coordinates so the cluster head compares those data in a table with legitimate nodes data. Sybil node, if any difference arises. The simulation result shows that proposed system improves energy efficiency and it detects the Sybil node accurately.

Yousef EL Mourabit et al., [10] proposed an intrusion detection system in WSN based on mobile agent. It uses multi-agent and a taxonomy based approach for detection of intrusions. It includes three mobile agents to detect the intrusions. The first agent is accumulator agent, which collects the data from the wireless environment and provides response to the misuse detection agent. The second agent is misuse detection agent, which detects the identified attacks using misuse detection technique. The third agent is anomaly detection agent, which detects the unknown attacks by using SVM classification algorithm. The system has less parameter to distinguish the attacks and work improved by making additional composite detection parameters by means of statistical anomalies detection and allowing the formation of attack signatures.

Sandhya G et al., [11] proposed IDS in wireless sensor network using genetic k-means algorithm. This algorithm is more suitable for dynamic topologies. The false positive rate is abridged and high detection rate attained. It acts as intellectual IDS that can investigate produced intrusion alerts and it detects new attacks deprived of any predefined patterns or signatures.

S. Razaa et al., [12] proposed a real-time intrusion detection system in IoT named as SVELTE and implemented in Contiki OS. There are three main centralized components, in 6LoWPAN Border Router. The first component is 6LoWPAN Mapper, which gathers information about the RPL protocol and reconstructs the networks in 6BR. The second component is intrusion detection, which perceives the intrusion by examining the recorded data. The third component is a distributed mini firewall, which screens the malicious transportation before it spreads to the network.

Ms. T. Eswari et al., [13] proposed a rule based intrusion detection system for wireless sensor network. There are three main stages of this approach. The first stage is native reviewing phase, which authenticates the packets to confirm that packet is incoming from a valid adjacent node, or not. The second stage is rule application phase, which works, in licentious mode. The third stage is intrusion detection stage, which perceives routing bouts by endorsing the data gathered from satisfied suppression thing. This security mechanism can be able to detect only routing attacks.

Abdulaziz Alsadhan et al., [14] proposed an optimized intrusion detection system by soft computing method. The main objective is to increase the performance of the system and recognize each action in a racy way. They applied soft computing techniques like LDA, PSO, PCA, LBP, Greedy Search, SVM and MLP. In this methodology, the number of features abridged with the accumulative of detection rates.

Kasinathan et al., [15] proposed network IDS architecture on empowering the internet of things for business-based application. In this approach, IDS can listen or monitor 6LoWPAN traffic by using IDS probe. They used hybrid approach for placement of IDS. DOS protection manager is core component of proposed system, which raised an alert by using information available on network manager component.

Samir Athmani et al., [16] proposed a categorized energy proficient IDS to detect black hole attacks in WSN. It is executed using NS2 network simulator. This method has sensor node and base station are exchanging control packets with each other. Each control packet includes the node_id and number of packets directed to the head of the cluster. The base station is functioning on monitor mode to sense black hole attacks. This approach will chomp the less energy for intrusion recognition. It will not detect all black hole attacks, but it can reduce the impact of attacks.

IV. PROPOSED METHODOLOGY

The Security is one of the most important parameter has to be considered in designing the IoT, for its predisposition and connectivity of the data composed. The literature survey reviews that there are some limitations in the existing method in terms of computational overhead and they are heavyweight so it is not suitable for IoT environment. There is no centralized approach available to detect attacks in IoT network, so security is the key topic that disturbs the growth of IoT. It required strengthening the security of the IoT. Therefore the Intrusion detection systems for the IoT networks which is necessary to sense mischievous activities in the networks.

In the proposed methodology the IoT components interacts with the Intrusion detection systems where it includes the data acquisition module which collects the data from the IoT and it is delivers the data to the central monitoring system. The proposed framework of a cognitive intrusion detection system for internet of things demonstrated in the figure 4. The central monitoring system consists of detection module and cognitive module. The Access control and associated accounting schemes, which are processed by the central monitoring system. The detection module used to detect the attack, diagnose the attack.

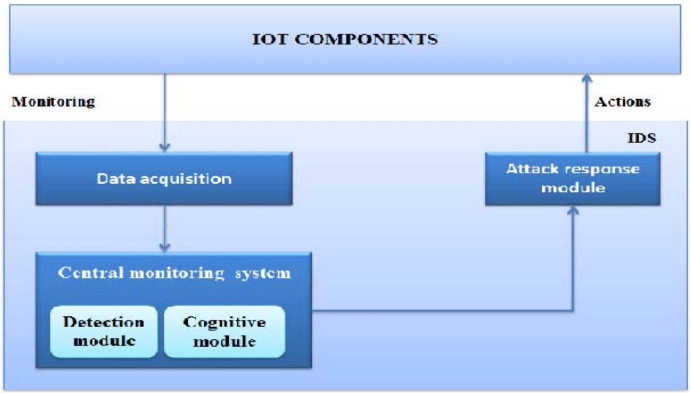

Figure 4: The proposed framework of a cognitive approach for IoT.

V. CONCLUSION AND FUTURE WORK

The security in Internet of Things is a important possessions for the mass acceptance of the technology. The cognitive approach should provide the secure exchange of data between IoT devices. There should be security protection during integration and interaction adaptation. In the future work, the implementation of the proposed methodology performed to validate it. The performance of the scheme evaluated to verify that the proposed procedure has better results.

REFERENCES

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

[2] P. Vlacheas, R. Giaffreda, V. Stavroulaki, D. Kelaidonis, V. Foteinos, G. Poulios, P. Demestichas, A. Somov, A. Biswas, and K. Moessner, ―Enabling smart cities through a cognitive management framework for the internet of things,‖ IEEE Communications Magazine, vol. 51, no. 6, 2013.

[3] G. Chavan, P. Pongle , ―Real Time Intrusion and Wormhole Attack Detection in Internet of Things‖, International Journal of Computer Applications (0975 - 8887), Volume 121 No. 9, July 2015.

[4] Diego Poplade, Christian Cervantes, Michele Nogueira and AldriSantos, ―Detection of Sinkhole Attacks for Supporting Secure Routing on 6LoWPAN for Internet of Things‖, International Federation for Information Processing /IEEE International Symposium on Integrated Network Management 2015.

[5] N. Dharini, Ranjith Balakrishnan and A. PravinRenold, ―Distributed Detection of Flooding and Gray Hole Attacks in Wireless Sensor Network‖, International Conference on Smart Technologies and Management for Computing, Communication, Controls Energy and Materials IEEE 2015.

[6] Byung Gyu Kim, Sung-Ki Kim, and Byoung Joon Min ―Reducing Security Overhead to Enhance Service Delivery in JiniIoT‖, International Journal of Distributed Sensor NetworksJanuary 2015.

[7] Youngseok Chung, Seokjin Choi, and Dongho Won ―Anonymous Authentication Scheme for Intercommunication in the Internet of Things Environments‖, International Journal of Distributed Sensor NetworksJuly 2015.

[8] Chen Jun, Chen Chi, ―Design of Complex Event Processing IDS in Internet of Things‖, Sixth International Conference on Measuring Technology and Mechatronics Automation, IEEE DOI: 10.1109/ICMTMA.2014.57, 2014.

[9] A. BabuKaruppiah, J. Dalfiah, K. Yuvashri, S. Rajaram, Al-Sakib Khan Pathan, ―A Novel Energy Efficient Sybil Node Detection Algorithm for Intrusion Detection System in Wireless Sensor Networks‖ 3rd International Conference on Eco-friendly Computing and Communication Systems, 2014.

[10] Yousef EL Mourabit, Ahmed Toumanari, AnouarBouirden, Hichamzougagh, Rachid Latif, ―Intrusion Detection System In wireless Sensor network Based On Mobile Agent‖, Second World Conference on Complex Systems (WCCS), IEEE 2014.

[11] Sandhya G, Anitha Julian, ―Intrusion Detection in Wireless Sensor Network Using Genetic K-Means Algorithm‖, IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT),2014.

[12] S. Razaa and L. Wallgrena, ―SVELTE: Real-time Intrusion Detection in the Internet of Things‖, Ad HocNetworks (Elsevier), vol. 11, no. 8, pp. 2661-2674, 2013.

[13] Ms. T. Eswari, Dr. V. Vanitha, ―A novel Rule Based Intrusion Detection Framework For Wireless Sensor Networks‖, International Conference on Information Communication and Embedded Systems (ICICES), IEEE 2013.

[14] Abdulaziz Alsadhan, Naveed Khan, ―A Proposed Optimized and Efficient Intrusion Detection System for Wireless Sensor Network‖, World Academy of Science, Engineering and Technology, International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, Vol: 7, No: 12, 2013.

[15] Kasinathan, Prabhakaran, et al. ―Denial-of-Service detection in 6LoWPAN based internet of things‖ Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE2013.

[16] Samir Athmani, DjallelEddine Boubiche and Azeddine Bilami, ―Hierarchical Energy Efficient IntrusionDetection System for Black Hole Attacks in WSNs‖, Published in Computer and Information Technology (WCCIT), 2013.

AUTHOR PROFILE

Kushal Kumar B. N. obtained his Master of Technology in Digital Communication and Networking and Bachelor’s Degree in Information Science. He is currently pursuing his Ph.D in Computer Science and Engineering from VTU. He is working as an Assistant Professor in the Department of computer science at KSIT. His research interests are in the field of networking, communication and Internet of Things. He is the Life member of Indian Society for Technical Education and IAENG.

Dr. Panduranga Rao M. V. obtained his PhD degree from National Institute of Technology Karnataka, Mangalore, India. He has completed Master of Technology in computer science and Bachelor of Engineering in electronics and communication. He is currently working as Professor and Head in the Department of computer science at BTLIT. His research interests are in the field of Real-Time and Embedded Systems on Linux platform. He has published various research papers in journal and conferences across India, Also in the IEEE international conference in Okinawa, Japan. He has authored two reference books on Linux Internals. He is the Life member of Indian Society for Technical Education and IAENG.