Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 3, June 2021: 5034 – 5049

Research Article

Recent Trust Based Models and Security Frameworks for Secure IoT Ecosystem

Kajol Rana[1], Dr. Ajay Vikram Singh[2], Dr. P. Vijaya[3]

Abstract

Internet of Things is an arrangement that provides machine to machine communication with the help of internet where devices can be a physical device's, vehicle's, home appliances or any type of electronic appliances. With the growth of IOT the number of devices connected on the internet is also increasing so, to efficiently implement IOT into the network we need to closely deploy the constraints of IOT. Major challenge in deploying IOT are the security issue since IOT requires an end to end security and any breach can lead to the failure of the entire concept. To overcome this challenge many techniques have been built. In this research paper we are performing a comparative study on different security frameworks along with special focus on different Trust Based Security frameworks developed for IOT.

Index Terms**—**Cryptography, Internet of Things, Near Field Communication, Security and Trust.

I. INTRODUCTION

IoT is a network that contains physical devices, vehicles,electronic appliances, etc. all enclosed with sensors and medium to communicate. It allows the sensors to study the object and enables the object to connect and exchange data without any form of human intervention.

According to a recent survey, it has been predicted that by the year 2020, number of devices connected to Internet will be 2.5 times. With the inclusion of more devices and more data, comes adverse security risks.In 2016, an attack named Mirai Botnet, lead to paralysis of global access to high profile Internet services for a few hours, leaving all forms of data vulnerable and even exposing highly secret documents of the countries.[1]

IoT although very useful, but at times can be disastrous if not dealt with carefully. For instance, if all the devices in a hospital are connected using IoT and some notorious person attacks the system and can access the system, then the life of the patients is at high grade of risk or a burglar is able to crack the security of your house then it can lead to huge financial loss. We have a wide web interface which is highly insecure, leading to major attacks onto the system; we still do not have the right mechanism for authentication of the correct user, we can find so many fake accounts even after so many security aspects; already existing networks, encryption algorithms for transmitting of information are also not strong enough that they can be relied on; cloud services and mobile interfaces are easy to crack; the software's and hardware's are also not able to defend attacks on themselves after an extent and we can also say that the physical security of the device also plays an important role for developing a good IoT; we are still not able to find beforehand if our system is compromised or not, so identifying the various security breaches is also a task, there is no way of predicting the attacks.[2] In this

paper, we are going to review various security frameworks as well as security framework based on trust and try to understand and identify the difference among them.

II. RELATED RESEARCH WORK

The Discrete technologies introduce new forms of designing and working issues. Internet of things has bought an evolution in the field of Artificial Intelligence and is seen to be useful in many areas of interest. However, when working with this kind of huge data, requirement of very high standards of security becomes mandatory. For overcoming this issue various security frameworks have been developed over the years.

LLCPS utilized for Near Field Communication (NFC) provides peer to peer secured transaction by making use of Transport Layer Security. It consists of four layersNear Field Communication Interface and Protocol-1 layer (Works on initialization, target detection and hence forms a data path that avoids this route)[3]; Logical Link Control Protocol layer (Works as a means to encapsulate and secure the packets to be transmitted)[4]; Transport Layer Security layer (Works as an authentication system); Service layer (key is encrypted as per NFC Data Exchange Format to lockdown the target)[5].[6]

Digital Forensics Investigation Framework is used by digital forensics. It forms its base from ISO. Major work is to initialize and investigate material to form modules of digital forensics via reactive and proactive processing.[7]

Software Defined Networking- based security framework forms cluster for IoT devices [8]. It does intrusion detection as well as prevention from malicious attacks.[9] SecIoT provides all forms of basic security features, such as, authentication, authorization, etc. Working with trust as a parameter is still a future scope for this framework.[10] Radio Frequency Identification security framework focuses on novel identification technique to provide security benefits by making use of hash operations and probability evaluations.[11] SAFIR (Secure Access Framework for IoT) provides security for small IoT network by performing access control, authentication, authorization, etc. It also provides secured parameters for the establishment of flexible sharing models.[12]

III. SECURITY FRAMEWORKS

Security is a major hurdle in the growth of IoT. Decisions made prior to a breach in security can result into better functioning of IoT applications. In this section we will be studying in detail about various recently developed security frameworks for IoT.

A. Cisco Framework

This framework (figure1) helps in prevention from physical attacks like Data at Rest and Intrusion detection. To maintain the standards for security it constitutes of four layers of security as given in figure 1. The framework consists of four entities. Firstly, Authentication is Done using Radio Frequency Identification, shared secret key and

X.509 certificates [13] and does not work on IEEE 802.1Xand hence, provides with, lesser credential types, intensive cryptographic constructs and authentication protocols. Secondly, Authorization's job is to only allow access to recognized personnel. It stores the identity information of an entity and hence establishing a trust relationship between the IoT devices. Thirdly, Network Enforced Policyare always some of the protocols applied according to the nature of the work of the devices and to keep the channel secured. Lastly, Secure Analytics: Visibility and Control does threat detections and preventive measures to avoid any foreseen threats are fixed.[14]

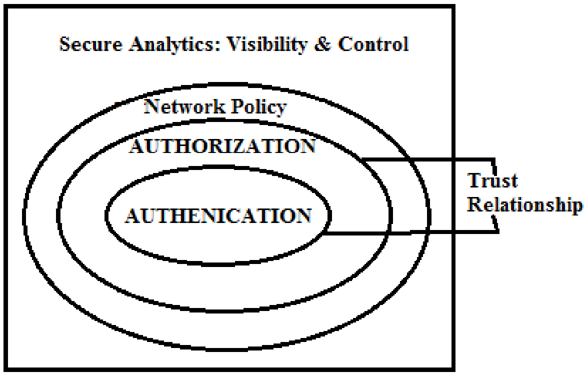

Fig.1. Cisco Framework for IoT

B. Floodgate Framework

This framework works completely according to the ISA/IEC 62443 compliance (cyber security). It allows the entities to prevent from present or upcoming cyber threats and is not favorable for low power devices, as it requires high battery power and storage space and hence it is called as a best fit for Infrastructure security framework. It maintains Internet security, Security for specific applications and security measures are taken at the Run- time for checking the integrity.[15]

C. Intelligent Security Framework

It instruments Asymmetric key Encryption to communicate the session key between nodes and then use this session key for sending the message. Authentication between devices and services is established mutually by using the unique ID of the sensors to generate the key. For the purpose of communication, it makes use of lightweight asymmetric key cryptography (Used for securing the communication between sensors and gateways, by making use of sensor unique ID and gateway unique ID. Using the two above unique ID's and applying Advanced Encryption Standard Algorithm a secret key is created.) and public key encryption – digital signature (Used for securing the communication between device gateway and cloud service). In this framework (figure 2), we can remove most of the fake and faulty packets, as a result, performance improvement is seen and in addition to it, it provides reduced bandwidth consumption and security is established against Quantum Attacks. [16]

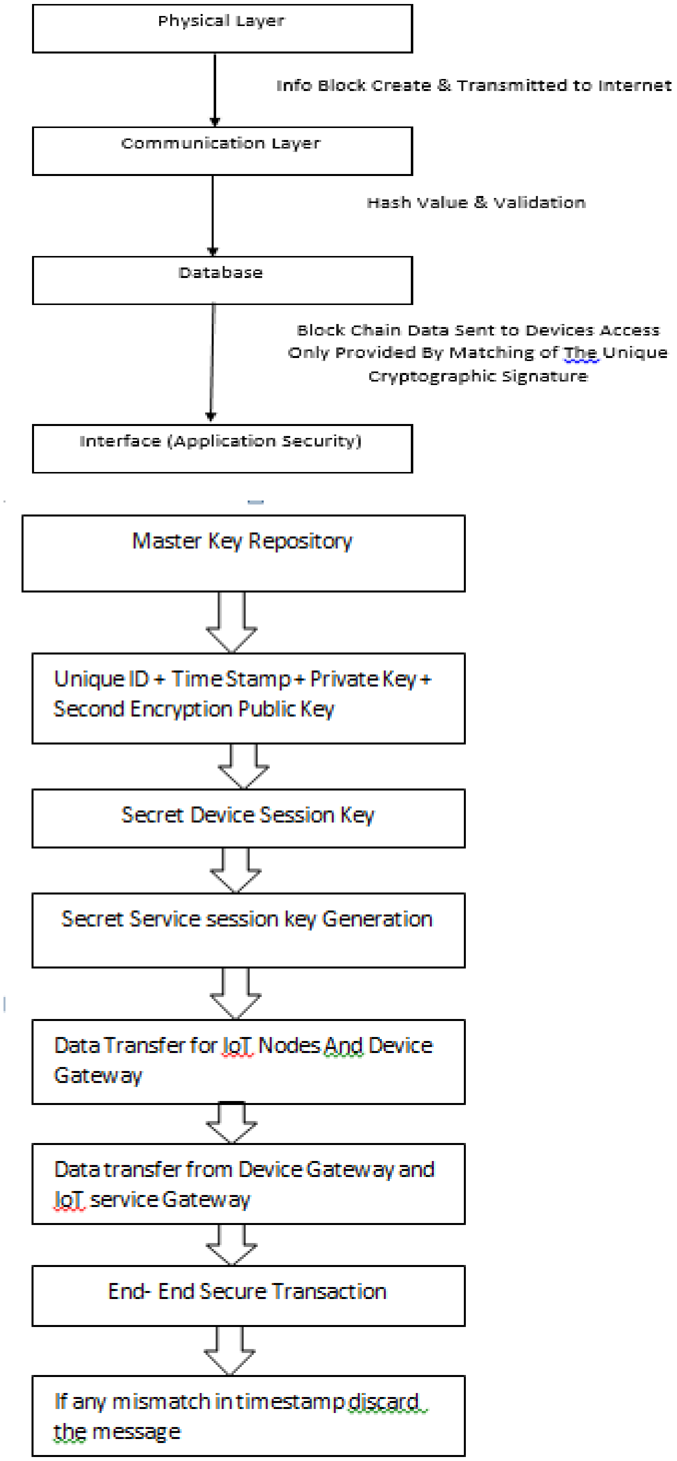
Physical Layer
Info Block Create & Transmitted to Internet
Communication Layer
Hash Value & Validation
Database
Block Chain Data Sent to Devices Access Only Provided By Matching of The Unique Cryptographic Signature
Interface (Application Security)
Master Key Repository
Unique ID + Time Stamp + Private Key + Second Encryption Public Key
Secret Device Session Key
Secret Service session key Generation
Data Transfer for IoT Nodes And Device Gateway
Data transfer from Device Gateway and IoT service Gateway
End- End Secure Transaction
If any mismatch in timestamp discard the message

Fig. 2. Intelligent security framework for IoT

D. Security Framework for IoT against Wireless Threat

For maintaining security against the wireless threats, this framework enables the block chain technique. Block chain technique sustains a database which constitutes of all the data set records, which are, distributed in nature. The benefit of using this technique is that only the nodes whose participation is required are given the copy of the chain and it is very cost effective.

It consists of four layers (figure 3), namely, Physical (Does the encryption work), Communication layer (Follows the Block Chain Protocol) [17], Database (Records are saved here for future use and each record consists of time constraints and unique cryptographic signatures) and Interface layer (It provides with the Application Security). [18] Fig.3. Security Framework for IoT against Wireless Threat

E. IoT Security Model

The IoTSM model is based on end to end security. The model (figure 4) presents a general view of security for any organization working in the area of IoT. It helps the organizations to model an end to end security for its day to day work. Its base is designed by using the Software Assurance maturity model.[19]It constitutes of five layers as shown in the figure 4. The task of the first layer Governance is to create security awareness by educating the employees and designing a soft model of security using the design process and standards. Second layer, Construction wherein, all the risks are identified,and assessment is done to check the level of the risks. Majorly ISO 27001 and OCTAVE are used. Threat modelling is also a part of this layer. Threat modelling is done using two methods: Attack- tree based (identify the possible attacks on the tree structure of the work) and Stochastic model (Analyzed using the state transition metrics). Third layer, Security Requirement and Architecture in which, security measures are implied, such as, Physical security is provided using Encryption, Network security is provided by using privacy and integrity, data security by using authentication and so on. Fourth layer, Verification is done to check the reliability of the system developed. It does artifact review for reviewing the codes and security testing is done for inspection of any vulnerability in the software. Lastly, Operation in which, IoT systems are updated by using a secured as well as verified channel to rule out any threat possibilities.

This model is seen to work better than Software Assurance maturity model, Building Security inMaturity Model [20], Comprehensive Lightweight Application Security Process
[21] and Microsoft Security Development Lifecycle [22], as it involves cloud and data security at every point. [23]

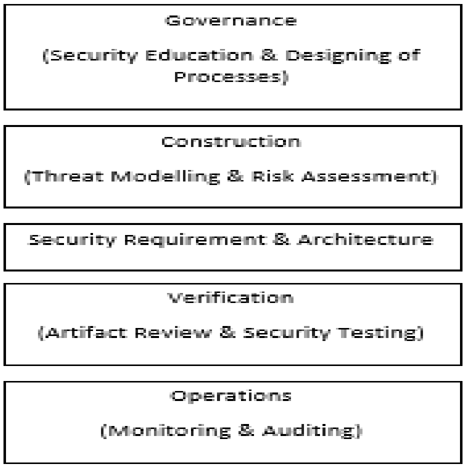
Governance
(Security Education & Designing of Processes)
Construction
(Threat Modelling & Risk Assessment)
Security Requirement & Architecture
Verification
(Artifact Review & Security Testing)
Operations
(Monitoring & Auditing)

Fig.4. IoTSM (IoT Security Model)

F. U-POT A Honeypot Framework

The honeypot framework [24][25][26][27][28][29] is applied on Universal Plug and Play Devices [30], which constitute of Controlled devices (Servers responsible for delivery of service) and control points (Smart phone Application).

Working of the framework is shown in figure 5

a. Target Device: - The use of Belkin WeMo smart switch is done.[31]

b. State scanner: - Its work is to reap the description layer of the target device.

i. Crawling: - If there are multiple descriptions, all the files are creeped through extracted URL's and HTTP Get Method and stored in a local file system. The data collected is searched thoroughly to identify the list of state variables.

ii. Scanning: - It enables the initial handshaking with the control point of the UPnP Device.

c. U-PoT Devices: - Its work is to create mimic devices which can listen to any approaching request on the channel and return/update its state accordingly.

i. Discovery Mode:- All the information of the device and its state are extracted by scanning through the information.

ii. Normal Operations Mode: - Its work is to accept the request and perform update/change according to the request made.

This framework is seen to work better than other algorithms and has low overhead on response time.[32]

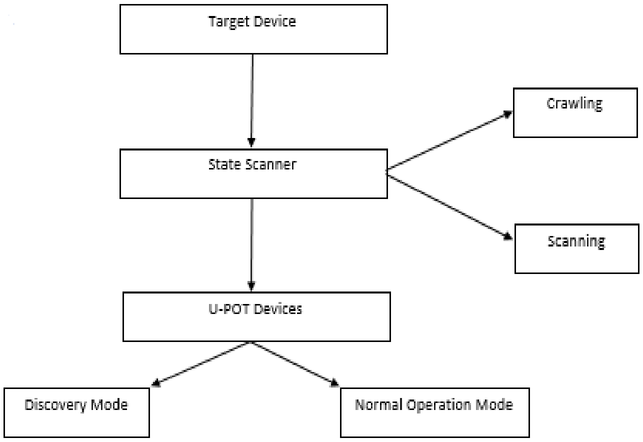

Fig.5. U-PoT: Honeypot Framework for IoT

G. Cloud Computing Framework For Improving IoT Security

This framework is designed specifically for cloud services. It has separated IoT functions from the physical devices and runs confined IoT functions on cloud environment. It applies Dripcast framework [33], [34], [35], [36], as it is a transparent programming framework for IoT Devices.

In which Clientlayer has a small Java library that works on the client's device. Used to send CREATE request to the Relay. All jobs in the library are assigned a unique ID for identification and verification purpose.Relay layer contains a set of servers, known as, Relays. Its job is to accept the request from client and send it to the engine servers. It is protected using strict access controls and authentication is required. Engine layer contains a set of Engine servers, with assigned key space for every server. Its job is to accept the request of the client and process the output for the client. Not connected to any public internet and the only possible way to reach it is relay.Store layer is a Database storing all the information. Information can be only accessed using GET, PUT and REMOVE. This is also not connected to any public internet.[37]

H. PoLIoT (Polytechnic IoT)

It is used for threat identification and management. It is developed by using three frameworks, namely, Power IoT framework (Important features depend upon the risk assessment and security rules, majorly works upon intelligent devices and has 4 layers, namely, application, platform, physical & network) [38], IoT Education Framework (it is used to protect all forms of assets from threats, makes use of SDRAM, FLASH, ROM, etc. and has three layers, namely, Security protocol, software platform and hardware platform.) [39] and Embedded Security Framework (Awareness and education is the main motivation and works majorly on LAN, consists of five layers, namely, Response layer, Control layer, Network layer, Perception layer and Site/base layer) [40]. It is adequate as network systems deployed in polytechnic are of medium size and comprise of basic technology. It consists of three layers: Device layer, Access layer and Data & Application layer. All the layers are used for threat management.

Device layer consists of the information of the device and the description layer of the device. Access layer allows access to only authorized members. Data and Application layer which uses different measures like intrusion prevention, authorization and access control. [41]

IV. TRUST MODELS

Trust is a behavioral pattern of human beings. Usage of trust in the field of IoT has led to the development of security in IoT.

Some of the security framework based on trust for IoT have been studied in detail in this section.

A. Security and Reputation based trust assessment for cloud services for IoT

In this paper, trust evaluation is done on cloud services to safeguard the security of cloud based IoT context through combined services from security and reputation. It develops a security metrics to compute security levels for a cloud service. For the quantification of reputation, feedback is collected. This framework is seen to outperform other trust assessment methods.

It has three main parts: -

a. Security based trust assessment: - Security based trust assessment is done by following three main steps, namely, security metric definition, security metrics quantification and security level evaluation.

i. Security Metric Definition: - Its job is to form security control deliverables which constitutes
of cloud specific security metrics (metrics defines the security requirement of the client).

ii. Security metric quantification: - All the security metrics are quantified, so that, comparison can be done based on security capabilities. Quantification can either be done in Yes/No manner or 0/1 manner.

iii. Security level Evaluation: - Forms its basis from TOPSIS. [42] An ideal decision matrix is developed, and positive/negative solutions are identified. Then the difference is calculated in concordance to the ideal value. Relative closeness can then be identified for each of the CSP's (Cloud service Providers).

b. Reputation based trust assessment: - It is done by following the four main steps given below: -

i. Data Collection and processing: -Data is collected from the feedback ratings and then the required information is normalized to form multi-tuples, which are combined to form a data repository.

ii. Weight factor assignment: - Reputation based Trust Assessment is used to determine the weight factors to be considered.

iii. Local objective reputation: - Calculation of Local Objective Reputation is done by combining feedback rating of each CSC.

iv. Global objective reputation: - Global Objective Reputation can be calculated using the time-based weighted Local Objective Reputation within a specific time window.

c. Integrated Trust Assessment: - It follows the objective weight assignment method to identify the important weights of security and reputation levels and then based on the identified weights trust can be evaluated.[43]

B. *Blockchain based secure and trustworthy IoT*

This paper utilizes trust framework along with block- chain framework for SDN (Software Defined Networks) enabled 5G VANET's (Vehicular Ad-hoc Networks)[44] and provides privacy and avoids malicious attacks. The working of the security model can be majorly divided into two parts, as follows, firstly, blockchain Framework, in which the vehicle is identified by using SIM, which is a unique identification given to the DL number of a vehicle on the network. After the registration symmetric key SKE is used to encrypt the hash value of video. Data transmission is encrypted and message sharing between vehicles is block-chained, so that the records remain immutable as well as the vehicle sending messages can be easily traced. It helps us to avoid any form of malicious attacks. [45] Second comes Trust management which contains Traffic Information collection that does the judgment of road condition tags is done by either +1 or -1. Road Side Unit (RSU) receives messages and classifies it into a set {Ej,1, Ej,2,….Ej,n}. Ej,p is broadcasted to reach all the vehicles.Trust value computation in which, RSU classifies the scores made by forwarding vehicles it has received into {Sj,1, Sj,2, …, Sj,p}. Distance from vehicle is found and RSU finds and tags the vehicle ID's giving high frequency of false positives by using blockchain method.Miner Election in which, Proof-of- stake is used to elect and value of trust is determined and lastly Vehicle Credibility assessment is used in case of any accident, it can use the videos to know the reason of accident and re-route all other vehicles to a free road. [46]

C. *CTRUST (Centric Trust For IoT)*

The performance of the following framework was calculated based on the utility obtained and trust’s accuracy, convergence and resiliency. Parameters involved are communication speed, reliability, rate of work, etc. Weights assignment depends upon the decision of the trustier. In this framework, the nodes required for context criteria are assessed and a partial trust score is obtained, then weights are assigned to the criteria and with the help of previous trust scores the trust database is updated and final decision is then made using the updated trust database. Working of the CTRUST framework is shown in the figure. [47]

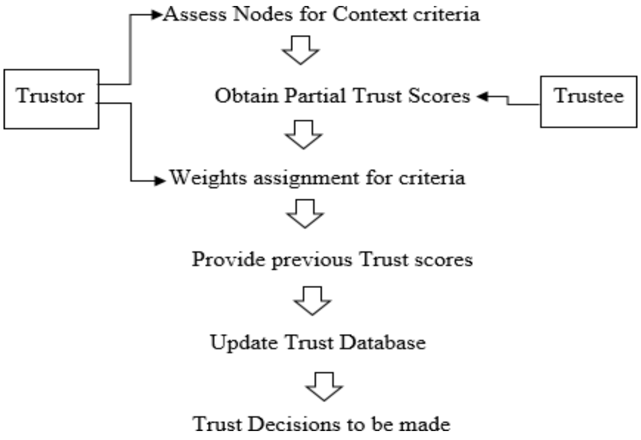
Assess Nodes for Context criteria
Trustor
Obtain Partial Trust Scores
Trustee
Weights assignment for criteria
Provide previous Trust scores
Update Trust Database
Trust Decisions to be made

Fig. 6. CTRUST (Centric Trust) for IoT

V. COMPARISON OF VARIOUS SECURITY FRAMEWORKS AND TRUST BASED SECURITY FRAMEWORKS

In Table 1 comparison of various security frameworks is done, so that a better understanding can be established of the frameworks and their applicability can be underlined. It can be seen that all the frameworks work for different problems certain attacks like intrusion detection and privacy is taken care of in almost all the described frameworks.

TABLE I
COMPARISON BETWEEN VARIOUS SECURITY FRAMEWORKS FOR IOT

S.No.	**Security Framework**	**References**	**Attributes**	**Attacks/ Facilities**
1	Cisco	[14]	RFID X.509 Certificates	Data at Rest Intrusion Detection
2	Floodgate	[15]	ISA/IEC 62443	Cyber Threats

3	OSCAR	[48]	Privacy Coupling content encryption key	Eavesdrop Relay attacks
4	Intelligent Security	[16]	Asymmetric key cryptography Lattice based cryptography	Fake and faulty packets Quantum attacks
5	Security Framework for IoT Against Wireless Threat	[18]	Block chain technique Unique cryptographic signatures	Wireless threats like Rogue access points, denial of service, passive capturing and Eavesdropping
6	IoTSM (IoT Security Model)	[23]	Software Assurance maturity model Threat modelling ISO 27001 OCTAVE	Intrusion detection Eavesdropping Brute Force
7	U-PoT: A Honeypot Framework	[32]	Honeypot Framework	IoT candy Jar [49] Malicious attacks
8	Cloud computing framework for improving IoT security	[37]	Dripcast Framework	Intrusion Detection Privacy
9	PoLIoT (Polytechnic IoT)	[41]	Power IoT Framework IoT Education Framework Embedded Security Framework	Intrusion Detection Authorization Access Control
10	Elliptic curve cryptography-based security framework for IoT	[50]	Elliptic curve cryptography	Unique Authentication Integrity Confidentiality Privacy

In Table 2 comparison of various trust based security framework is done to see how trust as a factor can be included to provide better security and it can be seen that various major attacks are taken care of by making use of different pillars of trust(Reputation, belief, authentication, etc.). Trust can be considered as a good example for security issues as it provides a better understanding for the human brain and with more consideration in this field we can develop a better and secure environment for IoT.

TABLE II
COMPARISON OF SECURITY FRAMEWORK BASED ON TRUST FOR IOT

S.No.	Security Framework based on Trust	References	Attributes	Attacks
1	Security & Reputation based trust assessment for cloud services.	[43]	Security based trust assessment Reputation based trust assessment	Self-promotional attack [51] Slandering attack [52]
2	Block chain based secure and trustworthy IoT	[46]	Trust framework Block chain framework	Privacy preventio n Malicious attack
3	CTRUST	[47]	Trust assessment (Objective and subjective) Decay recommendati o n Aggregation function	Malicious attack
4	Architectur e based trust in M- IoT	[53]	Centralized Framework [54] Distributed Framework [55] Hierarchical Framework [56]	Authenticati on Integrity Confidential ity Access Control Authorizatio n
5	SPTP (Secure, Private & Trustworthy Protocol)	[57]	Platform for Privacy preferences P3P [58] Access control list	Reputation Access control Web cookies

VI. CONCLUSION

After reviewing all the above security frameworks, it can be predicted that working of IoT is more focused on providing services, rather than, securing the existing. The security frameworks designed till date, provide only basic form of security, leading to a highly risky platform. It is observed from the above frameworks that trust based approaches are providing more efficient and secured environment for IoT than the others. The framework IoTSM with certain advances can prove to be a nice approach for industrial operations in the field of IoT . It has also been noticed that majorly cryptographic techniques are used to provide a standard level of security. When talking about Internet of Things and Billions of devices then security standards must go beyond authentication, privacy, integrity and certain predictable attacks. By the above paper, we can conclude that there is a requirement for better security approaches, which are able to provide peer to peer security or device to device security, so that the entire concept of IoT can be established to avoid attacks like CandyJar, Mirai Botnet, Slandering attacks, etc completely.

REFERENCES

[1] Sebastian Bellagamba, “Trust by design: The Internet of things”, ITU, 2018.

[2] Colin Tankard, “The security issues of the IoT”, Elsevier, 2015, p.p:- 11-14.

[3] “Near Field Communication Interface and Protocol”, Standard ECMA- 340, December 2004.

[4] “Logical Link Control Protocol”, Technical Specification, NFC Forum^{TM}, LLCP 1.1, June 2011.

[5] “NFC Data Exchange Format” Technical Specification, NFC Forum^{TM}, NDEF 1.0, July 2006.

[6] Pascal Urien, “LLCPS: A new security framework based on TLS for NFC P2P applications in the Internet of Things”, IEEE, 2013, p.p:-845- 846.

[7] V.R. Kebande, I.Ray, “A generic digital forensics investigation framework for internet of things”. IEEE, 2016, p.p:-356-362.

[8] O.Flauzac, C.Gonzalez, F.Nolot, “SDN based architecture for clustered WSN. Innovative mobile and internet services in ubiquitous computing” 9th International Conference, p.p:-342-347,2015.

[9] C.Gonzalez, S.M. Charfadine, O.Flauzac, F.Nolot, “Sdn-based security framework for the iot in distributed grid”, IEEE, 2014, p.p:- 1-5.

[10] X.Huang, P.Craig, H.Lin, Z.Yan, “Seciot: a security framework for the internet of things”, Security and communication networks, vol.9, no 16, 2016, p.p:-3083-3094.

[11] B.R.Ray, J.Abawajy, M.Chowdhury, “Scalable rfid security framework and protocol supporting internet of things”, Computer networks, vol.67, 2014, p.p:-89-103.

[12] J.L.Hernandez-Ramos, M.V.Moreno, J.B.Barnabe, D.G.Carrillo, A.F. Skarmeta, “Safir: Secure access framework for iot-enabled services on smart buildings”, Journal of Computer and system sciences, vol.81, no.8, 2105, p.p:- 1452-1463.

[13] Zakia El Uahhabi, Hanan El Bakkali, “An approach for evaluating trust in X.509 certificates”, ICITST, IEEE, 2106, p.p:- 196-203.

[14] Z. Bakshi, A. Balador and J.Mustafa, “Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models”, IEEE, 2018, p.p:- 173-178.

[15] Mohammad Irshad, “A systematic review of information security frameworks in Internet of things”, IEEE,2016, p.p:- 1270-1275.

[16] S.Sridhar, S.Syms, “Intelligent security framework for IoT devices”, ICISC, IEEE, 2017, p.p:-1-5.

[17] Konstantinos Christids, and Michael Devetsikiotis,“ Blockchains and Smart Contracts for the Internet of Things”, Special Section on the Plethora of Research in Internet of Things (IoT), 2016.

[18] Himanshu Gupta, Garima Varshney, “A security framework for IoT devices against wireless threat”, TEL-NET, IEEE, 2017.

[19] OWASP, “Software Assurance Maturity Model,” OWASP, 2018. [Online]. Available:https://goo.gl/9cCA4h.

[20] Gary McGraw, S. Migues, and J. West, “Building Security In Maturity Model (BSIMM),” 2018. [Online]. Available: https://goo.gl/JUAtbF.

[21] D. Graham, “Introduction to the CLASP Process,” 2006. [Online]. Available: https://goo.gl/wducjb.

[22] M. Howard and S. Lipner, “The Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software,” *MicrosoftPress*, vol. 8, 2006.

[23] Joseph Bugeja, Bahtijar Vogel, Andreas Jacobsson, “IoTSM: An End- to-end Security Model for IoT Ecosystems”, IEEE, 2019, p.p:- 267-272.

[24] Mitsuaki Akiyama, Makoto Iwamura, Yuhei Kawakoya, Kazufumi Aoki, and Mitsutaka Itoh. Design and implementation of high interaction client honeypot for drive-by-download attacks. IEICE transactions on communications, , 2010 p.p:- :1131–1139.

[25] Yaser Alosefer and Omer Rana “Honeyware: a web-based low interaction client honeypot” (ICSTW), IEEE, 2010, p.p :- 410–417.

[26] Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, and Christian Rossow, “Iotpot: analysing the rise of iot compromises”, 2015.

[27] Adrian Pauna and Victor Valeriu Patriciu “Casshh–case adaptive ssh honeypot. In International Conference on Security in Computer Networks and Distributed Systems”, Springer, 2014, p.p:- 322–333.

[28] Haris ˇSemi´c and Sasa Mrdovic.”Iot honeypot: A multi-component solution for handling manual and mirai-based attacks.”(TELFOR), IEEE, 2017, p.p:- 1–4.

[29] G´erard Wagener, Radu State, Thomas Engel, and Alexandre Dulaunoy.,“Adaptive and self-configurable honeypots” (IM), 2011 IFIP/IEEE International Symposium, IEEE,2011, p.p:-345–352.

[30] UPnP Forum. UPnP upnp device architecture. http://www.upnp.org/specs/arch/UPnP-arch-DeviceArchitecturev1.1.pdf.

[31] Belkin International. belkin wemo. https://www.belkin.com/us/.

[32] Muhammad A. Hakim, Hidayet Aksu, A. Selcuk Uluagac, Kemal Akkaya, “U-PoT: A Honeypot Framework for UPnP-Based IoT Devices”, IEEE, 2018.

[33] Ikuo Nakagawa, Masahiro Hiji, Hiroshi Esaki: “Dripcast - Server-less Java Programming Framework for Billions of IoT Devices”, Proc of IEEE COMPSAC, Jul., 2014. pp:- 186-191,

[34] Ikuo Nakagawa, Masahiro Hiji, Hiroshi Esaki: “Dripcast – architecture and implementation of server-less Java programming framework for
billions of IoT devices”, JIP Journal, 23 (4), 2015.

[35] Ikuo Nakagawa, Masahiro Hiji, Hiroshi Esaki: “Design and Implementation of Global Reference and Indirect Method Invocation Mechanisms
in the Dripcast”, Proc. of IEEE COMPSAC, , Jun, 2016, pp:- 338-343.

[36] Ikuo Nakagawa, Masahiro Hiji, Hiroshi Esaki: “Global reference model and global garbage collection in the Dripcast”, PRAGMA 32, Apr, 2017.

[37] Ikuo Nakagawa, Shinji Shimojo, “IoT Agent Platform mechanismwith Transparent Cloud Computing Framework for improving IoT Security”, IEEE, 2017, p.p:- 684-689.

[38] Zhang Y., Zoun W., Chen X., Yang C., Cao J, “*The Security for Power Internet of Things: Framework, Policies and Countermeasures,* in International Conference on Cyber-EnabledDistributed Computing and Knowledge Discovery”, 2014.

[39] Zhang Tianbo, “*The Internet of Things Promoting Higher Education Revolution”*, Fourth International Conference on
Multimedia Information Networking and Security, 2012, pp:- 790-793.

[40] Babar S., Stango A., Prasad N., Sen J., Prasad R., “Proposed Embedded Security Framework for Internet of Things (IoT)”, IEEE Journal, 2011.

[41] Zulkarnain Md. Ali, Mohamad Azuan Bin Mohamed Arshad, Marini Abu Bakar, “POLIoT : Internet Of Things Framework In Managing Network Threats At Metro Polytechnic Tasek Gelugor” , IEEE, 2018.

[42] M. Behzadian, S. K. Otaghsara, M. Yazdani, and J. Ignatius, ``A state-of the-art survey of TOPSIS applications,'' *Expert Syst. Appl.*, vol. 39, no. 17, , 2012, pp:- 13051_13069.

[43] Xiang li, Gixu wang , Xiao lan, Xingshu chen, Ning zhang , Dajiang chen, “Enhancing Cloud-Based IoT Security Through Trustworthy Cloud Service: An Integration ofSecurity and Reputation Approach”, IEEE, 2019, p.p:- 9368-9383.

[44] I. Yaqoob, I. Ahmad, E. Ahmed, A. Gani, M. Imran, and N. Guizani,
``Overcoming the key challenges to establishing vehicular communication: Is SDN the answer?'' *IEEE Commun. Mag.*, vol. 55, no. 7, Jul. 2017, pp. 128_134,

[45] M. H. Eiza, Q. Ni, and Q. Shi, ``Secure and privacy-aware cloud- assisted video reporting service in 5G-enabled vehicular networks,'' *IEEE Trans.Veh. Technol.*, vol. 65, no. 10, Oct. 2016, pp. 7868_7881.

[46] Lixia xie, Ying ding, Hongyu yang , Xinmu wang, “Blockchain- Based Secure and Trustworthy Internet of Things in SDN-Enabled 5G- VANETs”, IEEE, 2019, p.p:- 56656-56666.

[47] Anuoluwapo A. Adewuyi, Hui Cheng, Qi Shi, Jiannong Cao, Áine MacDermott, Xingwei Wang, “CTRUST: A Dynamic Trust Model for Collaborative Applications in the Internet of Things”, IEEE, 2019, p.p:- 5432-5445.

[48] H. Zhou, et al.,, “*A Cognitive Adopted Framework for IoT Big-Data Management and Knowledge discovery Prospective*,”IEEE.

[49] Tongbo Luo, Zhaoyan Xu, Xing Jin, Yanhui Jia, and Xin Ouyang, “Iotcandyjar: Towards an intelligent-interaction honeypot for iot devices.”, Black Hat, 2017.

[50] T Daisy Premila Bai, K Michael Raj, S Albert Rabara, “Elliptic Curve Cryptography based security framework for Internet of Things Enabled Samrt card ”, WCCCT, 2017, p.p:- 43-46.

[51] K. Hoffman, D. Zage, and C. Nita-Rotaru, ``A survey of attack and defense techniques for

reputation systems," *ACM Comput. Surv.*, vol. 42, no. 1, 2009, Art. no. 1.

[52] P. Chandrasekaran and B. Esfandiari, ``A model for a testbed for evaluating reputation systems," in *Proc. IEEE 10th Int. Conf. Trust, Secur. PrivacyComput. Commun. (TrustCom)*, Nov. 2011, pp. 296_303. [53]Vishal Sharma, Ilsun You, Karl Andersson, Francesco Palmieri, Mubashir Husain Rehmani, "Security, Privacy and Trust for Smart Mobile-Internet of Things (M-IoT): A Survey", IEEE, 2019, p.p:-1-45.

[54] M. D. Alshehri and F. K. Hussain, "A centralized trust management mechanism for the internet of things (ctm-iot)," in International Conference on Broadband and Wireless Computing, Communication and Applications, Springer, 2017 pp. 533–543.

[55] R. Chen, J. Guo, and F. Bao, "Trust management for soa-based iot and its application to service composition," IEEE Transactions on ServicesComputing, vol. 9, no. 3, 2016, pp. 482–495.

[56] X. Wu and F. Li, “A multi-domain trust management model for supporting rfid applications of iot,” PloS one, vol. 12, no. 7, 2017.

[57] Ivor D. Addo, Ji-Jiang Yang, Sheikh I. Ahamed, “SPTP: A Trust Management Protocol for Online and
Ubiquitous Systems” IEEE, 2018, p.p:- 590-595.

[58] R. Wenning, W3C, “Platform for Privacy Preferences Project,” *P3P Public Overview*, October 2007, Retrieved from http://www.w3.org/P3P/.