2018 IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics

An overview of potential authentication threats and attacks on Internet of Things(IoT): A focus on Smart home applications.

Attlee M. Gamundani
Namibia University of Science and Technology
Faculty of Computing & Informatics
Computer Science Department
Windhoek, Namibia
e-mail: agamundani@nust.na

Amelia Phillips
Highline College
CIS and Computer Science Departments Cyber Security and Forensics BAS lead
Seattle , USA.
e-mail: aphillips@highline.edu

Hippolyte N. MUYINGI
Namibia University of Science and Technology
Faculty of Computing & Informatics
Windhoek, Namibia
e-mail: hmuyingi@nust.na

***Abstract*—Internet of things (IoT) are finding their wide use in various domains. IoT implementation in the Smart home domain is one that is complex as the devices that are being used in such platforms are of different sizes and have different computational capacity. The ability to ensure security is enforced on such devices rests on how proper the authentication processes are executed. It is against this background that this paper is formulated, to give a detailed review of the potential authentication threats and attacks on IoT in the Smart home domain in particular. The main ideas on the potential authentication threats and attacks on IoT in Smart home applications, presented in this paper are largely informed by the detailed literature review of related work in the domain of IoT.**

Keywords- *Attacks; Authentication; IoT; Smart home; Security; Threats.*

I. INTRODUCTION

IoT security has become a cause for concern as a result of the increased number of resource constrained smart devices which are not architecturally designed to employ robust security techniques on them [1]. As further summed up by [2] the challenges emanate from existing authentication schemes for IoT devices which include: pre-distributed authentication keys, which are not feasible; manual pairing, which require more user effort especially when dealing with many IoT devices and context-based solutions, which are mostly peer-to-peer instead of being scalable. As clearly summarized by [3], IoT's obstacles to their deployment rest on authentication of different interconnected entities, and exchanged data confidentiality are the top concerns that need to be addressed.

Authentication can be viewed as the first line of security by ensuring enforcement of security measures at level 0 [4]. The process of authenticating the various processes, applications and objects require a handshake that can be done before authorization is granted. The computational limitation[5] and overall capacity nature of IoT devices makes it a challenge to apply conventional security techniques [6]. Another key challenge as highlighted by [7], is that authentication that makes use of the public key system is not pliable under IoT application environments due to some of the reasons cited by [6].

This main contribution of this paper is the classification of autherntication threats based on the key features of IoT devices as they are functionally positioned under various applications scenarios as presented in Table 1, which are Device level; Network level and Application level. These three classifications are based on the 3-layer model for IoT, which correlates to the perception, network and application layers. In the broader sense, such authentication threats, are not confined to one application domain for IoT powered devices, but span almost every domain where IoT devices have their footprints.

To guide the discussion on IoT authentication threats in Smart homes, this paper has four main key segments. Section I, briefly highlight some of the Smart home applications, which paints an idea on the nature of IoT application dimensions in a Smart home setup. Section II, gives an overview of IoT authentication approaches. Section III then builds on Section II by focusing on authentication threats, where a cascading approach is employed by having a more broader approach first, looking into the general then later the specific threats to Smart homes. As the main core section of this paper, it further populates details on classification of threats in Smart home applications. Then Section IV concludes and gives a way forward for the broader perspective of this research.

II. SMART HOME APPLICATIONS

Smart home environments as well defined by [8] can visually be portrayed as an organized and networked collection of heterogeneous components (i.e. be it electronics or appliances) whose defined purpose is to provide smart services seamlessly to the smart home owners. The essence of availing convenience is being underscored, yet attached to that functional specification of Smart home setups is an array

978-1-5386-7975-3/18/$31.00 ©2018 IEEE
DOI 10.1109/Cybermatics_2018.2018.00043

of security loopholes that renders them a ripe haven for different possible attacks of varying magnitudes as they interface directly with personal and sensitive data[9],[10],[11].

The enabling environment for Smart home as a key towards the fundamental industrial and commercial envisaged test bed for IoT, Smart Grids as well as 5G connectivity [12] is being fuelled by IoT [13]. Commercial vendors are introducing health care, home automation and remote monitoring [5],[12]. These key facts about a Smart home, clearly points to the fact that, Smart homes are a delicate and an underdeveloped domain. Due to the infancy nature of the Smart home domain, many of the solutions are on trial and not yet fully developed. On the other hand, the future projections into the growth of Smart cities[14],[15]can be honored if the critical arms to the Smart cities hub are given proper attention; hence Smart homes are a critical component towards the wider Smart cities project.

Some of the key applications highlighted from literature for Smart homes are intrusion and detection systems. As clearly presented in [16] where an Android application for monitoring, configuring and notification remotely is demonstrated. Home owners are notified of any unusual events promptly on their mobile devices, equipping them with the ability to advance instant action despite being physically absent from their own premises, thereby increasing security of their homes by the click of a button [16]. As a result, traditional usage and connectivity of Internet setups will continue to play a significant role [12], hence the continual security challenge for Smart home environments.

Telemedicine is another key application attributable to Smart homes [17], where monitoring of chronic illnesses for homebound patients can be advanced. This offers in home patients monitoring and ubiquitous monitoring as demonstrated by [18] through their personal health system dubbed COMPASS, which empowered by interoperability protocols make use of mobile devices for collection, analysis and subsequent transfer of sensed data to the set observation repository. The architecture of COMPASS is a server-client setting with a publish/ subscribe mechanism, dynamic updates of machine learning models and RESTful services to perform the create, read, update and delete operations [18].

Another key application area for Smart home solutions is home automation and that range from different aspects in the Smart home environment. As highlighted by [19],[20] home based automation powered by smart phones allows control over home electrical devices (e.g. Geysers, TV, Radio, Lights, etc.) in an embedded environment portrayal. As summed up by [20] IoT devices are providing a wide range of services for Smart homes such as surveillance cameras, smart lighting, and door locks. The design thereof is at the backdrop of improving physical security via remote control in a setup that mimics a normal activity based home environment even when the inhabitants are physically absent[19].

A more precise application is highlighted by [21] through the smart wall power outlet which enables intelligent home power metering system, capable of measuring power consumption and transferring the data wirelessly through the low energy integrated Bluetooth transmission. Smart plugs are one of the fast emerging IoT devices finding their way in home automation and making remote monitoring and control of Smart homes easier [22]. As an example demonstrated by [22] one can turn on the heater with their smart phone even before getting home, because of the smart plug capability, however this doesn't come cheap as there are security challenges to some of the available brands on the market which was the main focus of Ling et al in[22].

There are various implementations of Smart home setups such as Qiloc which enables various Smart home applications like calendars, instant messaging and email systems to be setup[23]. This diversity positions Smart home applications at a more vulnerable position as the attack vectors henceforth exponentially grow[24]. Smart homes ultimately have these key requirements once established, mobility management, channel security, consistent data rates and handover support as presented by [9], which hint towards the need to look at security design and requirements for Smart home domains with more rigor.

III. IoT Authentication Overview

Authentication is among the top vital aspects for consideration towards the design of secure IoT communication. Authentication can be rendered as the first phase towards access control, and it can be device authentication or user authentication [25], even more. However, the provision of a lightweight, bulletproof and distributed authentication scheme for total security solutions towards IoT applications remains one of the biggest challenge [26]. Device authentication is critical and a very challenging task for the emerging IoT [27].

There are three security layers for IoT, which can be summarized as perception layer, network layer and application layer [28]. These security layers correspondingly correlate with the three security dimensions of the IoT security architecture, which entail information security, physical security and management security [28]. Authentication should be the initial handshake security level that has to grant access rights to pieces of data around the Smart home environment. This is corroborated by [28], who argues that "IoT should have these characteristics: comprehensive perception, reliable transmission, and intelligent processing (page, 664)."

Detailed review work and the classification of different authentication techniques for IoT was carried out by [29]; building on that work, this section is going to highlight and populate on some of them and highlighting some of the

recent schemes as well. As [29] quoted [30], [31], there is a general agreement that traditional TCP /IP protocols such as HTTP, TCP and IP are not efficient in supporting machine to machine (M2M) communication. This clearly shows that for IoT authentication solutions to work, there has to be specific functional and technical refinement of existing solutions, in a contextual approach as guided by their implementation.

The constrained nature of devices and critical security concerns of IoT applications, sensor-based and wireless systems will demand novel solutions towards system design, network design and data processing procedures [32]. This is further supported by [33] in their REST-ful COAP message authentication scheme whose overarching goal through establishment of a message-oriented security layer for COAP, was to address the specific challenges stemming from the architectural style of REST and the resource constrained nature of IoT networks and devices. For proving trustable services, [32] explored the possibility of developing a node-based identification protocol by striking a balance between energy consumption versus malicious node detection in a heterogeneous IoT setup.

IV. AUTHENTICATION THREATS AND ATTACKS

The main security issues in IoT as highlighted by [34] are interdependent on authentication in one way or the other. Access control requires authentication to grant permission to the required resources or services. To ensure a secure middleware, we need to authenticate how access to the middleware is rendered and what rights can be granted, as part of middleware security. Before trust can be extended between communicating parties, these parties need to be authenticated against the set privileges and access rights. The threats therefore are evident when solutions are advanced and are not being effective, when there are gaps still evident after a solution is rendered, certain changes are effected or certain interactions are propagated and there is concern over security.

Also highlighted by [35], is the fact that, the increase in the number of sensors available and their ability to interconnect and be linked to user personal information, and the need to control personal data calls for the prioritization of data security. This then justifies why in a Smart home environment such IoT sensors need to authenticate themselves in their interaction within their locally created ad hoc networks. This has to be ensured before allowing outsiders to have access to the collected and stored inside information, which may be sensitive to the Smart home owner.

A. Authentication threats and attacks specific to IoT

The motivation behind looking at authentication threats specific to IoT is to prove the fact that, such threats can still be evident as well in smart homes. This will give a wider approach, which makes it easier to design solutions that are holistic in nature, as there is no one size fits, all when it comes to security solutions design.

The device-level IoT security vulnerabilities summarized in figure 1, are a clear indication of the varied nature of worries around IoT devices, hence authentication of such devices is already at risk from various angles. There is no doubt that IoT security incidents based on a varied nature of configurations are susceptible to different risk magnitudes [36]. Henceforth the risk level at device level still has a substantial stake towards the overall security worries for IoT applications.

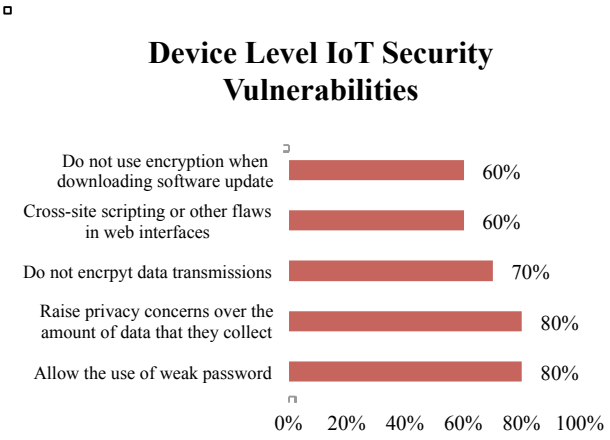

Figure 1: Device-level IoT security vulnerabilities adopted from [37].

The openness nature of IoT devices positions them to suffer potential security threats as poised by [38], when they looked at RFID tags which were noted to suffer the major threats of privacy leakage during the authentication process.

The work of [39] which looked at IoT application systems and security vulnerabilities and attempted to map the various applications, vulnerabilities and their impacts, was a great initiative. However, we strongly feel there is need to relook at the mapping and appreciate the interconnectedness between the three major application domains of IoT, which are Smart home, Smart health and Smart city. What affects the Smart health, can directly affect the Smart home as well as the Smart city. We can therefore represent the Smart health as a subset of the Smart home and of the Smart city at a bigger scale. Health is part of the individual domain of Personal Area Network (PAN). Considering the vulnerabilities presented by [39], it will be ideal not to complicate the representation and trying to singularly map each vulnerability towards a specific application domain, for instance, limited AAA cannot explicitly be attributable to

Smart homes alone but across board where IoT devices have been applied. We can have the same IoT device being used across the three platforms that will entail, the inherent vulnerabilities of that device will have to be dealt with for the same challenge though the magnitude of approach may vary due to other surrounding factors at functional level, even if it was used in a smart city or smart health environment. Finally the impacts mentioned henceforth cut across the different application domains. A re-modification of the mapping initially done by [39], is represented in figure 2.

The authentication solutions proposed by [40] was targeting denial-of service (DoS) attacks in both computation and memory, which are believed to be a direct effect of either deliberate invading behaviors or jammed traffic scenes. The 2FLIP scheme[40] also aimed at achieving non-repudiation as applied to VANETS, where identification of different drivers of the same vehicle is made possible. The premise presented on the basic security goals for wireless communication by[40], as resilience to modification of message and non-repudiation speaks a lot on the key threats that IoT authentication solutions have to embrace.

The work of [41], emphasis the focus on anonymous authentication in wireless networks, pointing to the fact that, privacy protection is key and one of the threats towards authentication solutions. To support the initiative of anonymity [42] presented a lightweight anonymity and mutual authentication protocol for RFID systems to achieve the basic security goals of confidentiality, integrity and authentication. On the contrary, [43] proposed an identity management and key based authentication method to provide single sign-on in IoT, pointing to the fact that the biggest threats to IoT are humans, as they are emphasizing the need to authenticate the technicians who intend to access the appliances from the Internet.

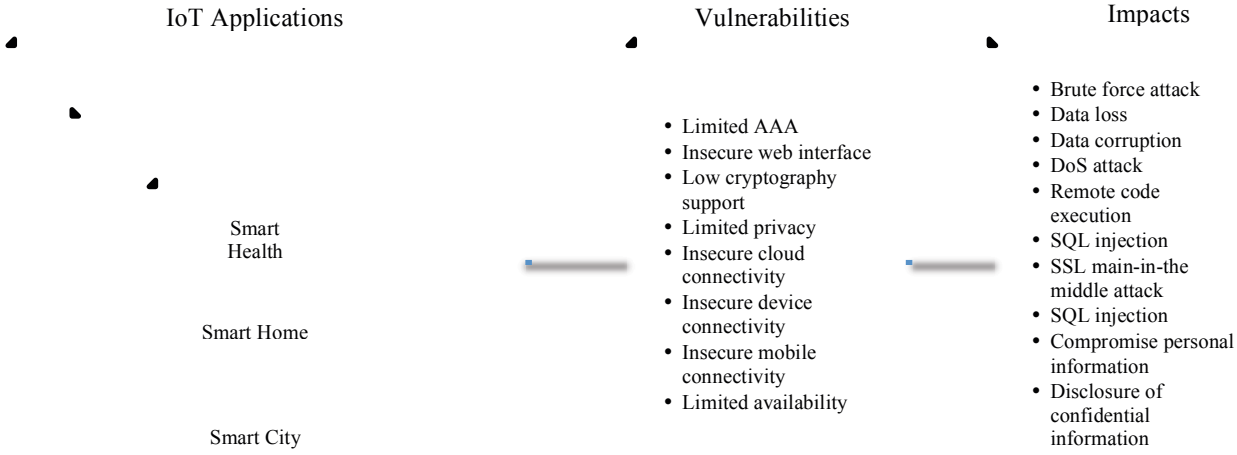

Figure 2: a modification of IoT Application, vulnerabilities and the impacts originally adapted from [39]

As highlighted by [44], loss of basic privacy, tracking, cloning, eavesdropping, physical attacks and denial of service attacks, are some of the surfacing threats for IoT authentication.

A look at the solution presented by [45] tells that the scheme was targeting secure bootstrapping of wireless Home Area Network (HAN) devices by capitalizing on identity based cryptography (IBC); the main argument being that attackers may target the system at setup and network operation stages during HAN setup.

The architectural build of some of the networks that enables IoT, are a threat to authentication in themselves as clearly outlined by [46] that the vulnerable nature of mobile ad hoc networks (MANETS) makes them prone to an adversary's malicious attacks such as dropping data or sending fake data for example. As a result, their work [46] was on an enhancement design of the Ad hoc On-Demand Distance Vector (AODV) digital signature based authentication aimed at preventing potential routing attacks against their protocol from intruders and malicious nodes.

The key known attacks that were put into consideration by [46] were DoS: Sleep deprivation; routing table overflow; replay attack; black hole; Eavesdropping; Sybil; wormhole; byzantine and main–in-the-middle, which proved to be what the scheme can prevent i.e. potential network layer routing attacks. Some of the unique set of security issues are mobile phishing and smishing for mobile application services as presented by [47], where a scenario of an attacker being able to overwrite the Near Field Data Exchange Format (NDEF) message can effectively exchange an authentic tag with a hacked tag, which opens doors for mobile malware for the NFC-enabled device.

The work of [48] proves that some of the authentication schemes can be their own threats in their bid to provide authentication solutions. We witness a demonstration of the

Voltage Over Scaling (VOS), a technique that operates on the basis of a computation process to produce a two-factor authentication scheme after profiling the error signature and gaining information of the underlying procedures whose variation was then combined with security key based authentication protocols. This approach effectively capitalized on the error by methodically profiling it to gain knowledge of the underlying process variation for computation purposes, hence providing a unique key authentication approach that employs hardware process variations.

A cloud based RFID authentication scheme presented by [49] was targeting reader impersonation attack and tag location tracking attack hence was aimed at providing tag location privacy. In a similar research done by [50], it is concluded that identity revelation, information leakage, tracking and spoofing are typical to RFID systems which are defenseless against any varied nature of attacks either active or passive. They suggest that Elliptical Curve Cryptography (ECC) has the ability to establish mutual authentication among the tags and servers, at the same time protecting them against eavesdropping, cloning risks and replay tracking attacks [50].

The work done by [51] investigated the threats of DoS attacks for Software Based Network (SDN) control channel, which proved that, if an authentication mechanism is missing, controlling resources can easily be drained rendering them incapable of offering the intended services. To counter this setup, [51] proposed a mechanism to hide information of the authentication in a lightweight manner.

Advanced persistent threats are the main driver of the solution design presented by [52], where they looked at cloud enabled (security as a service) Internet of controlled things using a contract design approach.

Vehicle-to Grid (V2G) connections are reported vulnerable against security threats like exposing privacy in authenticating Electric Vehicle (EV) [53]. For prevention of various insider and outsider attacks, a mutual authentication and authorization protocol which is efficient and secure is highly recommended on many different devices by [14]. The scheme achieves mitigation of insider and outsider threats every instance a device is accessed by the user through implementing a simultaneously authorization and authentication process of the user [14].

Since most IoT devices are likely to be directly connected to the Internet while being battery powered for some, they are particularly vulnerable to DoS attacks specifically aimed at quickly draining battery and severely reducing device lifetime [54]. The proposed SMACK, offered an early detection mechanism by swiftly picking invalid messages upon reception and validated them against the lightweight message authentication code [54], was an initiative to address the DoS threat of this nature.

Light weight mutual authentication alternatives which also are capable of providing data confidentiality are proposed by [55] which make use of authentication key exchange to defend against phishing and similar attacks. As highlighted by [56] security vulnerabilities of lightweight authentication mechanisms and their inability to tackle memory DoS attacks, motivated the work on an improved scheme derived from the streamlined μTESLA, referred to as X –μTESLA.

Some of the key highlighted potential attacks on user authentication protocols as tested against the RRAM based lightweight user authentication work of [57] are:-

- Password stealing
- Password guessing
- Password collision (false negative) – when different passwords are deemed to be authentic for one user.
- False positive alarm – a case when an authentic password is declined
- Denial of service
- Side channel attack – a group of powerful attacks that targets the vulnerabilities in hardware implementation of the security primitives and protocols

The security attacks identified by [58], when they looked at Vehicle-to-Grid (V2G) networks for security and privacy challenges in which they noted solutions advanced to such networks were costly and failed to provide resistance to known security attacks are:- (replay, man-in-the-middle, redirection, impersonation and repudiation) attacks.

The careful study by [59] of a previous proposed enhanced secure authentication scheme for global mobile roaming services based on ECC, proved that it was vulnerable to attacks such as:- (user impersonation, man-in-the-middle, privileged insider, replay, no login phase, denial-of-service and imperfect mutual authentication phase) attacks [59].

B. Authentication threats and attacks specific to IoT in Smart homes

The reason why we need to zoom further into authentication threats, which are specific to Smart homes, is the unique nature of the domain of application. Generalizing authentication threats to IoT will not give a clear picture as to which ones are more prevalent under certain domains and not other domains. The picture painted in section I, of a Smart home, is one that entails the need to contextualize the threats so that they can effectively be handled. As indicated in Section II, a lot of similarities will be picked too under this section, validating our claim.

Control of Smart homes is being made possible through mobile devices which can access the Internet [13], they can easily be compromised if the very devices are not secured properly causing an extension of the attack vector, hence possible threats to authentication thereof.

By reverse engineering a smart plug and advancing unique set of attacks, [22] proved that they can effectively and efficiently obtain a victim's authentication credentials. By exploiting the communication protocols, device scans attack, brute force attacks, and spoofing attacks and firmware attacks were performed. As presented by [22], where they performed a case study on a smart plug system, a typical gadget in a Smart home environment, the following vulnerabilities were picked:- insecure communication protocols and lack of device authentication.

The Smart home scenario is replete with smart devices that have the capability of interconnecting among themselves, making the whole security design in such an environment equally a challenging task. General security solutions cannot directly be advanced towards IoT application domains as a result of the existing unique standards and communication stacks as well as limited computing power [34]. To ensure that the refrigerator and the TV can interact as they exist in the same space (Smart home), the authentication mechanisms needed for these two typical items would not be equivalent to the security measures that can be enforced on two computers.

Malware is a typical threat that can be directed towards personal data in a Smart home environment if the sensors will present a weak authentication structure. Therefore authentication mechanisms need to be looked at in order to address unauthorized users and devices from accessing data they are not privileged to access [34].

To add on to the list of attacks, [60] highlight the following:- insider attacks, impersonation attacks and man-in-the-middle attacks, reply attacks, unknown key sharing attacks which are presented as some of the prevalent authentication threats that needs serious consideration when designing security solutions. IoT devices are vulnerable to sophisticated security attacks such as man-in-the middle attacks, proffers [61] in their work.

In a Smart home setup, user's privacy information is at risk as a result of low security strength. The magnitude of the risk extend to access of such privacy information by strangers as well as other malicious entities for example eavesdroppers who can gather and aggregate the traffic information to profile a household [62]

Attacks for rolling-code garage door openers simply synchronize the malicious remote with the existing remote control signals, this requires only a few minutes or simply brute forcing the code or physical attack [63]. The approach by most manufactures of having a centralized authentication, authorization and commands is to reduce the demands of the inevitable tech calls [63], which eventually becomes a key threat to authentication. The main reason being that, the cloud platform opens new doors to a range of attack vectors, instead of attackers having one target, they end up having mass attacks of the same model and brand at a go [63] especially during software updates, attackers could gain control of the whole system.

The diversity of the Smart home devices, causes many security and privacy challenges during their usage [13]. Authentication based on fingerprint identification is still dangerous when it is defrauded with the fingerprint film [13].

C. *Classification of IoT Authentication threats and attacks in Smart homes*

Now that this review has allowed us to identify the threats that are specific to IoT in Smart homes, it will be logical to classify them accordingly into the following key classes, device, network, human and environment.

These classifications are based on the key features of IoT devices as they are functionally positioned under various applications scenarios as presented in Table 1 as Device level; Network level and Application level. These three classifications are based on the 3-layer model for IoT, which correlates to the perception, network and application layers. The threats are presented as sources of potential weakness areas that attackers can capitalize on to gain unauthorized access to data or information that is key to the overall security of IoT device in a smart home environment. The classification of attacks is done in two parts, considering data in transit and data at stay, as there is generally an oversight on the different states of data, which can be compromised at varying magnitudes. The examples given for each category on attacks is not an exhaustive list of the various attacks.

Table 1: Classification of Authentication threats and attacks

	Threats	Attacks	
		In transit	*At rest*
Device Level	Limited resources; Architecture; Interfaces; Software.	*Firmware; Brute force; Defraud; DoS;*	*Firmware; Physical; Credentials.*
Network Level	Architecture; Openness; Protocols.	*Eavesdropping; Device scan; Spoofing; Man-in-the middle Reply; Unknown Key sharing.*	*Device Scan; Brute force.*
Application Level	Interactions; Constraints; Environment; Human.	*Impersonation; Malware; Insider.*	

V. CONCLUSION AND WAY FORWARD

This paper gave a detailed summary of the various threats and attacks that can be attributable to Smart home IoT applications. This initial task of identifying such threats then eventually categorizing them is a great milestone in paving the next task on designing solutions that practically can be implemented to address some of these threats. This work is mainly focused on the lightweight solutions that can be applied to low power, low processing capable objects in Smart home things.

ACKNOWLEDGMENT

The support from the Digital Forensics and Information Security Research Cluster, the Faculty of Computing and Informatics and the NUST community's support are highly appreciated for the progress of this research work.

REFERENCES

[1] A. Majeed, "Internet of Things (IoT): A verification framework," *2017 IEEE 7th Annu. Comput. Commun. Work. Conf. CCWC 2017*, pp. 2–4, 2017.

[2] Z. L. Gu and Y. Liu, "Scalable group audio-based authentication scheme for IoT devices," *Proc. - 12th Int. Conf. Comput. Intell. Secur. CIS 2016*, pp. 277–281, 2017.

[3] H. Khemissa and D. Tandjaoui, "A Lightweight Authentication Scheme for E-Health Applications in the Context of Internet of Things," *Proc. - NGMAST 2015 9th Int. Conf. Next Gener. Mob. Appl. Serv. Technol.*, pp. 90–95, 2016.

[4] M. A. Crossman and H. Liu, "Two-factor authentication through near field communication," in *2016 IEEE Symposium on Technologies for Homeland Security, HST 2016*, 2016.

[5] D. Zhang, L. T. Yang, M. Chen, S. Zhao, M. Guo, and Y. Zhang, "Real-Time Locating Systems Using Active RFID for Internet of Things," *IEEE Syst. J.*, vol. 10, no. 3, pp. 1–10, 2014.

[6] Y. Sharaf-Dabbagh and W. Saad, "On the authentication of devices in the Internet of things," *WoWMoM 2016 - 17th Int. Symp. a World Wireless, Mob. Multimed. Networks*, pp. 1–3, 2016.

[7] C. Shen, H. Li, G. Sahin, and H. A. Choi, "Low-complexity Scalable Authentication algorithm with Imperfect Shared Keys for Internet of Things," *2016 IEEE Int. Conf. Commun. Work. ICC 2016*, pp. 116–121, 2016.

[8] J. Iinatti, S. Member, and P. H. Ha, "Smart Home Environments," *Ieee Trans. Inf. Forensics Secur.*, vol. 12, no. 4, pp. 968–979, 2017.

[9] D. Shin, V. Sharma, J. Kim, S. Kwon, and I. You, "Secure and Efficient Protocol for Route Optimization in PMIPv6-based Smart Home IoT Networks," *IEEE Access*, vol. 3536, no. c, 2017.

[10] S. Batool, N. A. Saqib, and M. A. Khan, "Internet of Things Data Analytics for User Authentication and Activity Recognition," pp. 183–187, 2017.

[11] M. Hossain, S. Noor, and R. Hasan, "HSC-IoT: A Hardware and Software Co-Verification Based Authentication Scheme for Internet of Things," *Proc. - 5th IEEE Int. Conf. Mob. Cloud Comput. Serv. Eng. MobileCloud 2017*, pp. 109–116, 2017.

[12] B. Silverajan, J. P. Luoma, M. Vajaranta, and R. Itapuro, "Collaborative cloud-based management of home networks," *Proc. 2015 IFIP/IEEE Int. Symp. Integr. Netw. Manag. IM 2015*, pp. 786–789, 2015.

[13] H. Ren, Y. Song, S. Yang, and F. Situ, "Secure smart home: A voiceprint and internet based authentication system for remote accessing," *ICCSE 2016 - 11th Int. Conf. Comput. Sci. Educ.*, no. Iccse, pp. 247–251, 2016.

[14] N. Saxena, B. J. Choi, and R. Lu, "Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 5, pp. 907–921, 2016.

[15] J. Paek, "Fast and Adaptive Mesh Access Control in Low-Power and Lossy Networks," *IEEE Internet Things J.*, vol. 2, no. 5, pp. 435–444, 2015.

[16] A. Daramas, S. Pattarakitsophon, K. Eiumtrakul, T. Tantidham, and N. Tamkittikhun, "HIVE: Home Automation System for Intrusion Detection," *Proc. 2016 5th ICT Int. Student Proj. Conf. ICT-ISPC 2016*, pp. 101–104, 2016.

[17] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, S. Kumari, and M. Jo, "Chaotic Map-based Anonymous User Authentication Scheme with User Biometrics and Fuzzy Extractor for Crowdsourcing Internet of Things," *IEEE Internet Things J.*, vol. 4662, no. c, pp. 1–1, 2017.

[18] T. Hofer, M. Schumacher, and S. Bromuri, "COMPASS: an Interoperable Personal Health System to Monitor and Compress Signals in Chronic Obstructive Pulmonary Disease," *Proc. 9th Int. Conf. Pervasive Comput. Technol. Healthc.*, 2015.

[19] J. P. Pienaar, R. M. Fisher, and G. P. Hancke, "Smartphone: The key to your connected smart home," *Proceeding - 2015 IEEE Int. Conf. Ind. Informatics, INDIN 2015*, pp. 999–1004, 2015.

[20] Y. Ashibani, D. Kauling, and Q. H. Mahmoud, "A Context-Aware Authentication Framework for Smart Homes," 2017.

[21] J. Brenkus, V. Stopjakova, R. Zalusky, J. Mihalov, and L. Majer, "Power-efficient smart metering plug for intelligent households," *Proc. 25th Int. Conf. Radioelektronika, RADIOELEKTRONIKA 2015*, no. 296131, pp. 110–113, 2015.

[22] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, and X. Fu, "Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System," *IEEE Internet Things J.*, vol. 4662, no. c, pp. 1–1, 2017.

[23] Y. Li, Y. Wang, Y. Cheng, X. Li, and G. Xing, "QiLoc: A Qi wireless charging based system for robust user-initiated indoor location services," *2015 12th Annu. IEEE Int. Conf. Sensing, Commun. Networking, SECON 2015*, pp. 480–488, 2015.

[24] A. M. Gamundani, "An impact review on internet of things attacks," in *Proceedings of 2015 International Conference on Emerging Trends in Networks and Computer Communications, ETNCC 2015*, 2015.

[25] S. Shaju, "BISC Authentication Algorithm : An Efficient New Authentication Algorithm Using Three Factor Authentication for Mobile Banking," 2016.

[26] P. Mahalle, "Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things," *J. Cyber ...*, vol. 1, pp. 309–348, 2013.

[27] D. Chen *et al.*, "S2M: A Lightweight Acoustic Fingerprints-Based Wireless Device Authentication Protocol," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 88–100, 2017.

[28] K. Zhao and L. Ge, "A survey on the internet of things security," in *Proceedings - 9th International Conference on Computational Intelligence and Security, CIS 2013*, 2013, pp. 663–667.

[29] M. Saadeh, A. Sleit, M. Qatawneh, and W. Almobaideen, "Authentication techniques for the internet of things: A survey," *Proc. - 2016 Cybersecurity Cyberforensics Conf. CCC 2016*, pp. 28–34, 2016.

[30] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," *Inf. Syst. Front.*, vol. 17, no. 2, pp. 243–259, 2015.

[31] J. Granjal, E. Monteiro, and J. Sa Silva, "Security for the Internet

of Things: A Survey of Existing Protocols and Open Research Issues," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015.

[32] S. C. Lin and C. Y. Wen, "Energy-efficient device-based node authentication protocol for the Internet of Things," *2016 IEEE Int. Conf. Consum. Electron. ICCE-TW 2016*, no. 1, pp. 1–2, 2016.

[33] H. V. Nguyen and L. Lo Iacono, "REST-ful CoAP Message Authentication," *Proc. - 2015 Int. Work. Secur. Internet Things, SIoT 2015*, pp. 35–43, 2016.

[34] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Networks*, vol. 76, pp. 146–164, 2015.

[35] X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute-based encryption scheme for the Internet of Things," *Futur. Gener. Comput. Syst.*, vol. 49, pp. 104–112, 2014.

[36] M. Mohsin, M. U. Sardar, O. Hasan, and Z. Anwar, "IoTRiskAnalyzer: A Probabilistic Model Checking Based Framework for Formal Risk Analytics of the Internet of Things," *IEEE Access*, vol. 5, pp. 5494–5505, 2017.

[37] C. Tankard, "The security issues of the Internet of Things," *Comput. Fraud Secur.*, vol. 2015, no. 9, pp. 11–14, 2015.

[38] P. Ghosh, "A Privacy Preserving Mutual Authentication Protocol for RFID based Automated Toll Collection System," 2016.

[39] J. Ahamed and A. V Rajan, "Internet of Things (IoT): Application Systems and Security Vulnerabilities," 2016.

[40] F. Wang, Y. Xu, H. Zhang, Y. Zhang, and L. Zhu, "2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET," *IEEE Trans. Veh. Technol.*, vol. 65, no. 2, pp. 896–911, 2016.

[41] X. Li, H. Liu, F. Wei, J. Ma, and W. Yang, "A lightweight anonymous authentication protocol using k-pseudonym set in wireless networks," *2015 IEEE Glob. Commun. Conf. GLOBECOM 2015*, 2015.

[42] M. Rahman, R. V. Sampangi, and S. Sampalli, "Lightweight protocol for anonymity and mutual authentication in RFID systems," *2015 12th Annu. IEEE Consum. Commun. Netw. Conf. CCNC 2015*, pp. 910–915, 2015.

[43] A. Witkovski, A. Santin, V. Abreu, and J. Marynowski, "An IdM and key-based authentication method for providing single sign-on in IoT," *2015 IEEE Glob. Commun. Conf. GLOBECOM 2015*, no. IdM, 2015.

[44] L. Cheng, L. Shenwen, L. Yingbo, L. Na, and W. Xuren, "A secure and lightweight authentication protocol for RFID," *ICEIEC 2015 - Proc. 2015 IEEE 5th Int. Conf. Electron. Inf. Emerg. Commun.*, no. 2012, pp. 317–320, 2015.

[45] R. H. Jacobsen, S. A. Mikkelsen, and N. H. Rasmussen, "Towards the use of pairing-based cryptography for resource-constrained home area networks," *Proc. - 18th Euromicro Conf. Digit. Syst. Des. DSD 2015*, pp. 233–240, 2015.

[46] N. Nissar and N. Naja, "Lightweight Authentication-based Scheme for AODV in Ad-hoc Networks," 2017.

[47] J. Baek and H. Y. Youm, "Secure and lightweight authentication protocol for NFC tag based services," *Proc. - 2015 10th Asia Jt. Conf. Inf. Secur. AsiaJCIS 2015*, pp. 63–68, 2015.

[48] M. T. Arafin, M. Gao, and G. Qu, "VOLtA: Voltage over-scaling based lightweight authentication for IoT applications," *Proc. Asia South Pacific Des. Autom. Conf. ASP-DAC*, pp. 336–341, 2017.

[49] M. Karthi and P. Harris, "A Realistic Lightweight Authentication Protocol for Securing Cloud based RFID System Surekha," pp. 168–171, 2016.

[50] K. Kaur, N. Kumar, M. Singh, and M. S. Obaidat, "Lightweight authentication protocol for RFID-enabled systems based on ECC," *2016 IEEE Glob. Commun. Conf. GLOBECOM 2016 - Proc.*, no. Id, 2016.

[51] O. I. Abdullaziz, Y. J. Chen, and L. C. Wang, "Lightweight authentication mechanism for software defined network using information hiding," *2016 IEEE Glob. Commun. Conf. GLOBECOM 2016 - Proc.*, pp. 0–5, 2016.

[52] J. Chen and Q. Zhu, "Security as a Service for Cloud-Enabled Internet of Controlled Things under Advanced Persistent Threats: A Contract Design Approach," *IEEE Trans. Inf. Forensics Secur.*, vol. 6013, no. c, 2017.

[53] A. Abdallah and X. Shen, "Lightweight Authentication and Privacy-Preserving Scheme for V2G Connections," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2615–2629, 2017.

[54] C. Gehrmann, M. Tiloca, and R. Hoglund, "SMACK: Short message authentication check against battery exhaustion in the Internet of Things," *2015 12th Annu. IEEE Int. Conf. Sensing, Commun. Networking, SECON 2015*, pp. 274–282, 2015.

[55] P. H. Griffin, "Security for ambient assisted living: Multi-factor authentication in the internet of things," *2015 IEEE Globecom Work. GC Wkshps 2015 - Proc.*, 2015.

[56] B. Mbarek, A. Meddeb, W. Ben Jaballah, and M. Mosbah, "A broadcast authentication scheme in IoT environments," *Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl. AICCSA*, 2017.

[57] M. T. Arafin and G. Qu, "RRAM based lightweight user authentication," *2015 IEEE/ACM Int. Conf. Comput. Des. ICCAD 2015*, pp. 139–145, 2016.

[58] N. Saxena, B. J. Choi, and S. Cho, "Lightweight privacy-preserving authentication scheme for V2G networks in the smart grid," *Proc. - 14th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2015*, vol. 1, pp. 604–611, 2015.

[59] E.-J. Yoon, A. K. Das, K.-Y. Yoo, and A. Goutham Reddy, "Lightweight authentication with key-agreement protocol for mobile network environment using smart cards," *IET Inf. Secur.*, vol. 10, no. 5, pp. 272–282, 2016.

[60] T. Shen, "Home Area Networks in Smart Grids," pp. 2444–2447, 2016.

[61] Y. P. Kim, S. Yoo, and C. Yoo, "DAoT: Dynamic and energy-aware authentication for smart home appliances in Internet of Things," in *2015 IEEE International Conference on Consumer Electronics, ICCE 2015*, 2015.

[62] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes," *IEEE Internet Things J.*, vol. 4662, no. c, pp. 1–1, 2017.

[63] J. Margulies, "Garage Door Openers: An Internet of Things Case Study," *IEEE Secur. Priv.*, vol. 13, no. 4, pp. 80–83, 2015.