A survey on approaches to the protection of personal data gathered by IoT devices

Henry Tranter[1]

[1]**School of Computing, Mathematics & Digital Technology**
[1]**Manchester Metropolitan University**

Corresponding author:
Henry Tranter[1]

Email address: henry.c.tranter@stu.mmu.ac.uk

ABSTRACT

Security is always at the forefront of developing technologies. One can seldom go a week without hearing of a new data breach or hacking attempt from various groups around the world, often taking advantage of a simple flaw in a system's architecture. The Internet of Things (IoT) is one of these developing technologies which may be at risk of such attacks. IoT devices are becoming more and more prevalent in everyday life. From keeping track of an individual's health, to suggesting meals from items available in an individual's fridge, these technologies are taking a much larger role in the personal lives of their users. With this in mind, how is security being considered in the development of these technologies? Are these devices that monitor individual's personal lives just additional vectors for potential data theft? Throughout this survey, various approaches to the development of security systems concerning IoT devices in the home will be discussed, compared, and contrasted in the hope of providing an ideal solution to the problems this technology may produce.

1 INTRODUCTION

The Internet of Things (IoT) is a name that collectively refers to a variety of devices that monitor and react to certain conditions they are presented with, all of which are connected to the Internet. Several examples of this include wearable fitness technology, medical equipment, and smart home technology. Each individual device within the IoT can be uniquely identified but can communicate to other devices via the Internet infrastructure Alsboui et al. (2012); Hammoudeh (2015). It allows various objects to be monitored, controlled, or otherwise interacted with across a network, increasing the efficiency and ease of use of these items without requiring a large amount of human interaction.

This concept has been discussed for decades. An early example of a situation in which IoT devices would have been useful is that of the 'Trojan Room coffee pot'. In 1991, in Cambridge University, a group of university researchers wished to know when a coffee pot was filled. To save an individual time making the trip to check on the machine, they implemented the first webcam to monitor it Boulton (2014). This could have easily become an early example of the use of an IoT device. An earlier example is that of the monitoring of a Coke machine in Carnegie Mellon University. The machine became the first device to connect to an Internet, and was capable of reporting its available inventory, as well as whether or not the drinks available were cold. Whilst these were both simple implementation of the ideas, they aided the proliferation of the discussion of the subject of IoT Hammoudeh et al. (2008); Hammoudeh and Alsbou'i (2011); Hammoudeh et al. (2010).

IoT devices are becoming more and more prevalent in the home, providing convenience for some, and accessibility for others. An example of this is the Amazon Echo, which provides a voice activated interface with the ability to control various other IoT devices around the home, potentially allowing users with mobility issues to carry out their daily tasks with more ease.

Due to the personal nature of this technology, it is understandable that an individual would wish that the data transmitted by these devices remained secure. However, there is a range of security risks to IoT devices which could cause the potential theft of personal data. The OWASP Internet of Things Project identified various issues and vulnerabilities with IoT devices. These include, but are not limited

to, the following areas: username enumeration; weak passwords; account lockout; poorly implemented encryption; denial of service; removal of storage media; lack of two-factor authentication mechanisms; and more Ghafir et al. (2016a); Dibb and Hammoudeh (2013); Carlin et al. (2015a).

Another issue comes with the problem of scalability. As a system grows, so do its security requirements. A system that is too large for its security features to handle becomes vulnerable to attacks. A system can also fault under its own complexity. Smart houses are coming into public discussion, in which a house features several interconnecting IoT devices. The number of devices can be small, or potentially very large depending on the requirements of the user, so a solution to this issue would have to bear this in mind.

There are certain risks present in the home that could cause potential loss of data, or lead to potential theft of data. The first of these is that of burglary. The Crime Prevention Website puts the average risk of being burgled at 2.5%, or 1 in 40 individuals. This number changes depending on demographic, for example, the highest risk group is individuals aged from 16 to 24 years at a 7.2% risk of burglary, or about 1 in 14. The physical security of IoT devices, or lack thereof raises concerns. Should a device be easily disassembled, and the storage is that of an unencrypted memory card, the card could very easily be removed and inserted into a reader, giving potential criminals access to your data Carlin et al. (2015b,b). Another issue is that, should USB ports be present on the device, for example, the fitbit health IoT device, then the data can be accessed should the criminal have physical access to the device. As well as this, custom software can be uploaded to these devices, potentially viruses, or spyware.

On a similar note as above, an IoT device's security could be compromised by other members of a user's household. Whilst this may not be as much of an issue with families, individuals in house sharing or flat sharing agreements would be very vulnerable to these physical attempts to access a device's data.

Another risk to home based IoT devices is that of hackers and hacking. Whilst most home networks come with their own layer of security, weak passwords and out of date security firmware can cause these networks to become compromised. An IoT device operating on this network is therefore at risk, potentially leading to the theft of a user's data as it is broadcast from the IoT device. As well as this, should the hacker already be on the same network as the IoT device, access, or interception, of private data could be potentially much simpler, as a potential hacker would have one less layer of security to get around.

2 CRITICAL ANALYSIS

Throughout this survey, various proposals and solutions to the protection of personal IoT-data will be analysed. These will be organised into three types of solution; Standardization of communication protocol, implementation of authentication and authorization features, and addressing scalability and expansion issues.

2.1 Standardization of IoT communication protocol

One issue the field of IoT is facing at the moment is a lack of standardization, particularly in that of communication protocol. Generally, each IoT device or brand would be built with a company's specific proprietary models in mind. Because of this, there is a large difference between the way each device communicates, making a generalized approach to securing each of these devices difficult. IoT devices also make use of various communication technologies, for example IEEE 802.15.4, WiFi, Bluetooth, etc Newman and Hammoudeh (2008); Hammoudeh et al. (2009); Hammoudeh (2008). Many of these different communication technologies exist within the home. Because of this, the ability to communicate between these devices becomes difficult due to the various physical and link layers.

Keoh et al. Keoh et al. (2014) highlight the lack of standardization of IoT devices must be solved before the further development of the field. They note that because of a very diverse collection of devices that exist together, that will all, at some point, share information, then the issue of lack of interoperability must be solved. Each device has its own proprietary brand of security features, or system architecture, and because of this, direct communication is difficult. Most IoT devices would therefore have to communicate to one another through some sort of middleware. As well as adding another access point in which a system could become compromised, the extra layer in communication is also inefficient, and adds another point of failure in which a system could break, causing communications to fail Aldabbas et al. (2016). Depending on the nature of the IoT devices communicating, this could potentially lead to disaster.

Keoh et al. state there must be a large undertaking between developers to create a security standard across the many communication layers, and by implementing these protocols, they could guarantee a level

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26473v1 | CC BY 4.0 Open Access | rec: 31 Jan 2018, publ: 31 Jan 2018

of security and interoperability. They state that the ideal solution would be that of a security protocol suite which would provide a full security service, from start to finish of communication. Their idea was to consider currently existing security standards which exists in the Internet Engineering Task Force (IETF). They discuss the Constrained Application Protocol, a request and response protocol which is similar to HTTP, and how to adapt current communication security solutions for use with the Constrained Application Protocol.

They proposed the combination of two solutions from the IETF, one concerning the security of the Datagram Transport Layer (DTLS), and its role in authentication and end-to-end security, and the other concerning the avoidance of packet fragmentation through compression. In order to evaluate these two solutions, they considered the memory consumption, energy consumption, percentage of packets lost in communication, and the number of bits sent in a single packet. They note that the DTLS performs poorly over limited network bandwidths, due to the likelihood of a security handshake failing. However, with the implementation of both solutions, the idea is that compression will keep the packet size short, so less time is lost in transfer, also leading to a decrease in likelihood of packet losing data.

Whilst Keoh's proposed solution does increase the security surrounding IoT devices, during the discussion of their solution they only discussed efficiency in both energy and memory consumption. They did not, however, discuss the vulnerabilities of DTLS, such as Plaintext-Recovery Attacks AlFardan and Paterson (2012), one of which a hacker can obtain ciphertexts from plaintexts, and ultimately gain information to lower the security strength of encryption algorithms.

Similarly to Keoh, Tiburski et al. Tiburski et al. (2015) suggest the use of pre-existing models as standards for future IoT developments. However, whilst Keoh highlights the importance of direct communications between IoT devices, and the standardization of this communication, and that middleware could potentially provide another access point for hackers to manipulate, Tiburski et al propose that whilst middleware poses certain security issues, rather than removing this middleware, it is important to instead secure this middleware.

Tiburski, et al, consider various existing solutions to securing middleware in the Internet of Things, as well as potential threats that are posed by middleware, and how to solve these threats. The solutions they discuss include SIRENA middleware, COSMOS middleware, SOCRADES middleware, and HYDRA middleware. Each defines basic architecture to seamlessly connect heterogeneous devices and services offered by such devices. Each different middleware solution focuses on an area of security in order to solve potential issues. These areas include: Authentication, authorization and access control, communication channel protection, data confidentiality, and data integrity. The middleware solutions are compared by how, if at all, they address each of these areas of security.

SIRENA Bohn et al. (2006) middleware makes use of DPWS technology, which is a standard that outlines a set of minimal requirements for implementation of secure web communication on devices with small amounts of resources. It concentrates mostly on communication channel protection, and device and application authentication. COSMOS Kim et al. (2008) middleware contains a module which controls the access for sensor networks within a device. COSMOS focuses mostly on authentication, access control, and confidentiality. SOCRADES Spiess et al. (2009) middleware is focused mostly on access control and authentication. IoT devices are only to be accessed by clients that have specific authorization, and correct credentials. Finally, HYDRA Badii et al. (2010) middleware focuses on authentication, authorization, communication channel protection, and data confidentiality. It makes use of an implementation of the XACML processing model which protects a system from access by unauthorised devices and clients.

Each of these existing solutions cover one area of security and protection. However, Tiburski et al. Tiburski et al. (2015) note that none of the solutions they considered covered every single one of the areas of security. Though this was the case, they then go on to note that each solution highlighted the important requirements for future standardization of IoT systems. These requirements are that of the security areas they compared the various existing solutions from. Whilst no specific solution is proposed, it is important to understand the various areas which must be addressed during the development of new IoT technologies.

It is clear that standardization of communication between IoT devices and networks is required for a consistent model to build future IoT technology from. A consistent model would allow the interoperability of a device, improving the ease in which it can communicate with other IoT devise and systems. From the standardizations we have discussed – middleware standardisation, and data link layer standardization – we can see the importance of secure communication, and a standardized method in which to do this should reduce the risk to potential security breaches.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26473v1 | CC BY 4.0 Open Access | rec: 31 Jan 2018, publ: 31 Jan 2018

2.2 Authentication and Authorization solutions

As mentioned in the introduction of this study, authorization and authentication are two areas of IoT technology in which require more attention and robustness Ghafir et al. (2016b); Atwady and Hammoudeh (2017); Aloraini and Hammoudeh (2017). Often there is a lack of multi-step authentication, and the authentication which does exist is still vulnerable to attack. In the case of IoT systems in the home, a user may not be as aware as to the location of their devices at any moment in time, as they would be with the more traditional computer devices Shahzad and Singh (2017), which would leave these devices open to potential theft. The devices and systems could then either be infiltrated, and manipulated. Because of this, further development is required as to the strength of authentication and authorization features.

Currently, many IoT devices are being built with convenience in mind, rather than security. The example given by Shahzad and Singh is that of the iPhone, Apple Watch, Macbook Pro interactions. They note that a Macbook laptop will unlock should the following conditions be true: The user is wearing the Apple Watch, the apple watch is connected to the users iPhone, the watch is close to the Macbook, and finally, either the phone or the watch have been unlocked recently. This presents a significant physical threat.

They propose multiple solutions to this problem. The first of which makes the use of an Inertial Measurement Unit (IMU). This is a device made up of an accelerometer and a gyroscope. They propose that one of the ways in which to authenticate a user is based on their gait, the patterns in which they move in, which would be calculated using machine learning techniques. Another solution they propose is that of an integrated photoplethysmogram sensor (PPG). This device could be used to measure patterns in blood flow systems, as well as heartbeat rhythms, which are both unique from human to human. Should an attacker attempt to use the device, the IMU or PPG would report an unrecognised pattern and require further authentication.

They go on to propose multiple other solutions all of which take into account biometric measurements. These systems are very strong in the sense that only specific users may be able to log into it, as it takes into account an individual's physical unique patterns that can potentially be difficult to replicate – i.e. an individuals blood flow pattern.

Whilst these solutions are unique, and in some cases secure, there is a large issue in using biometric data for authentication and authorization in that it is inconsistent at times, and can change over time depending on health status, age, and a variety of other factors. This would make it difficult for the actual owner of a device to log in at times. As well as this, certain patterns in the human system are easily monitored by others and there is a chance that these could become replicated and reproduced Xiao (2005).

Halak et al. Halak et al. (2016) propose a solution to authentication and authorization which can be potentially very difficult for an attacker to reproduce. They discuss the implementation of a Physically Unclonable Function (PUF) circuit. They state that the main problem with IoT devices is that of message snooping and interception because of potentially limited energy or memory capacity, leading to smaller and, in some cases, weaker security software/hardware. They propose that the implementation of a PUF circuit as standard would solve these issues.

A PUF circuit is one that is capable of producing different outputs for the same set of inputs. The idea being that this can exploit variability in CMOS technology in order to create a unique digital signature for each device they are integrated into. This can then be used in authentication, encryption, and decryption.

In order to evaluate their solution, and any other solution built from their proposal, they consider two features, the first of which is uniqueness. The measure of uniqueness determines the ability of a PUF device to generate unique IDs. They measure the uniqueness of a PUF device with the Hamming distance, comparing responses generated on one device to the responses generated on another device. This value should be high for a PUF to be considered unique. The second feature is that of reliability. A PUF would only be considered reliable if it were able to generate consistent responses for a challenge set to it. To measure this, they use the intra-chip Hamming Distance; a measure of randomness for a single PUF circuit.

One issue this solution would solve is that of security authentication between two IoT devices. Should both devices be PUF aware, they could authenticate one another for communication, as well as send encrypted communications which could be decrypted and interpreted at the receiver. As well as this, a standardised security measure built into multiple devices would aid in interoperability. This issue with this implementation, however, is the fact that PUF devices have an element of randomness, which can alter depending on slight electronic charges within the hardware of a system. This would mean that outputs of

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26473v1 | CC BY 4.0 Open Access | rec: 31 Jan 2018, publ: 31 Jan 2018

these circuits could become erroneous. This is not aided by the fact that CMOS transistors decay as they age, decreasing the reliability of a PUF circuit Alam et al. (2007), and potentially opening the device it is sat on to attacks.

Whilst not related to IoT systems directly, Nicanfar et al. Nicanfar et al. (2011) propose a solution to secure machine to machine (M2M) communications. This work could, or work similar to this, could then be applied to that of an IoT system.

They propose that a server in their system would contain authoritative duties over devices within a system. This server would compute a device private key by applying a function against a secret value and a counter. From here it selects a device that has previously been authenticated to act as an intermediary between the server and the incoming device. The device would then attempt to authenticate itself against the intermediary device, and the intermediary device would attempt to decrypt and re-encrypt these messages using the servers public key, and then sends the request to the server. The intermediary device also checks to ensure the serial number from the device is consistent with the one received by the server.

A similar solution could be proposed for an IoT system in which a central server similarly to the server in the given solution. Each IoT device could then act as the intermediaries. The only issue then is the fact that generally IoT devices are very sparing with the amount of memory and resources they can allocate. Should this solution be used in future IoT systems, this issue would have to be addressed before this solution could be realised.

Another issue with this system is that should a device which becomes an intermediary become corrupted or compromised in some way, it could open up the system to an attack. As well as this, the fact that it is centralized, and should the server become compromised in some way, the system would fail.

Authentication and authorization are becoming increasingly important as more and more IoT systems make use of personal or otherwise sensitive data. In the case of home devices, or smart homes, a consumer's need for convenience is often one that comes with a security risk. Future solutions should take this in mind as the field develops, as systems containing a user's personal data must be secure.

2.3 Solving Scalability and Growth Issues

A final issue with the growing field of IoT is that of scalability. IoT systems are becoming more and more complex as complicated functionality and interactivity is required for certain tasks. Smart homes a few years ago would feature simple voice activated products, or smart temperature devices. Smart homes now are becoming more and more like their own computer system, with potentially hundreds of small monitoring devices all around. Large systems like this are open to attack as more devices provide more entry points into a system. This scalability issue can become a large problem, and needs to be addressed consistently as the field grows.

Ning et al. Ning et al. (2013) discuss various challenges in the development of secure IoT systems. They define three major issues in reference to securing individual IoT entities within IoT systems. The first of which is the expanding domains of systems. The second, varying activity of the devices. And finally, the interactions of various devices are not limited to just physical and cyber attributes, there is also a social impact of the devices.

They propose the Unit and Ubiquitous IoT (or U2IoT) as standard. Previous solutions consider unit IoT, which are single applications. The U2IoT includes multiple interrelated local, national, and industrial IoTs. This move is proposed in order to deal with the increased growth the IoT sector has made. The U2IoT is made up of three layers: the perception layer, in which technologies exist which are responsible for converting physical objects into cyber entities; the network layer, containing all network components; and the application layer, supporting applications, and including service integration supervision, and coordination. Objects within the U2Iot exist as both physical devices as well as cyberentities.

To evaluate this system, they consider various attacks that could be carried out on the U2IoT, as well as consequences of these attacks, and what countermeasures they will use to prevent a specific attack. These attacks are generalised into four categories: gathering, imitation, blocking, and compromised privacy attacks.

Whilst the system performs well against various attacks, various threats and vulnerabilities of the system still exist. Attackers are able to exploit vulnerabilities related to cybertargets, the data sensed by a cyberentity. The example they used is that of a vehicle battery, in which an attacker can delete the data currently attached to the battery, replace it, or alter it, in order to manipulate a system measuring battery information. Another vulnerability is that related to cybersensors, in which data can be intercepted

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26473v1 | CC BY 4.0 Open Access | rec: 31 Jan 2018, publ: 31 Jan 2018

from, and altered, potentially leading to the trickery of a system into producing a certain response. Also, similar to most IoT systems, the solution proposed by Ning et al is still faced with issues of network vulnerabilities. Cyber targets and cybersensors communicate mostly through wireless means and as such are open to attacks.

They evaluate their system based on four security properties: session freshness, session-sensitive properties serve as access challenges, preventing forward and backward linking of sessions; Mutual authentication; Hierarchical access control; and privacy preservation.

Whilst this system does take into account scalability issues as the field and domain of IoTs grows, it still suffers some of the same issues as current IoT systems, mainly in that wireless communication between various nodes in the system are vulnerable and open to attack. Before systems like this come into prevalence, it is important to address these communication vulnerabilities, as they could lead to major issues in the future.

Another solution of scalability issues comes from the work of Moosavi et al. Moosavi et al. (2015). They consider the slow development of medical based IoT systems, and how healthcare is slowly moving from a highly centralized hospital approach, towards a decentralized home-based approach due to the increasing prevalence of IoT. Their solution builds upon this to create an IoT system making use of distributed e-health gateways.

They consider the main issue in health based IoTs is that of data privacy, as hospitals and medical centres collect a lot of personal information from individuals, and so it is imperative that a robust solution is created to secure this data as IoT healthcare solutions become more and more decentralized in their approaches.

Their proposed system would be comprised of multiple medical sensor nodes, a UT-GATE e-health gateway, a remote server, and their end users. The UT-GATE relays information to and from end-users, collected by the medical sensor nodes, via web browsers to a user's device.

In order to evaluate their system, they first analyse their security systems and compare it to currently existing, centralized systems. Their system shows strength against denial of service attacks due to its decentralized nature. Should one node of their system become compromised, the rest of the system remains intact and working. Another security measure they implement is that of a shared master key, generated by a complex logarithmic algorithm. Because of this, nodes are harder to compromise due to the difficulty of manipulating this algorithm, and so the system is stronger.

One of the main issues of a decentralized system such as this is that of processing power required by each node in the system. Each node will be required to handle additional processing steps in the transfer and collection of this information. Because of these constraints, their nodes can't handle many cryptography techniques which demand heavy computation. This issue would need to be addressed before any sort of implementation goes ahead as it would leave many of the nodes open to potential attack, or manipulation.

Li et al. Li et al. (2013), similarly to Ning et al. (2013), note that mainstream IoT systems tend to be isolated from one another. They state that this limits both the scalability of a solution as well as the efficiency of it, which provides certain challenges in the development of these systems. In order to combat this, they propose an Internet of Things Platform as a Service (IoT PaaS) cloud platform.

They state that the issue is that as systems develop and grow, they need to be maintained. The issue with most IoT systems is that their isolation makes it difficult to adapt a system, or maintain it. This could be particularly problematic in a smart home solution. As more and more machine integration of home appliances occurs, so does the potential threat of fault, and subsequent attacks based upon this fault. The solution proposed Li et al. (2013) allows for the maintenance and repair of a system to be done over cloud based communication by IoT providers.

Whilst this solution solves the issue of scalability, it does not address the various other concerns highlighted in this paper previously. Because of the various communication vectors proposed by this solution, there is a chance that one of these vectors could become compromised, either from an attacker trying to access sensitive information, or that from a malicious party attempting to manipulate the information flowing between two nodes. Should the IoT providers connection to a system be compromised, then malicious code could potentially be uploaded to a user's system. An attacker could then, in effect, spy on a user using the various devices in their home.

Scalability of a system is an important factor in keeping it safe, especially in areas like smart homes, in which not only is the data sensitive, but the systems are growing and changing all the time to suit a

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26473v1 | CC BY 4.0 Open Access | rec: 31 Jan 2018, publ: 31 Jan 2018

user's needs. From the papers we have discussed, the theme with scalable solutions is that of addition of attack vectors. Whilst Ning et al. make use of various cryptographic safety procedures to protect the nodes in their system, the limited resources of each device limits the strength or capabilities of these safety procedures. This issue must be addressed as the field develops, otherwise the solutions run the risk of attack.

3 GAPS AND OPPORTUNITIES

As stated in the discussion of individual solutions, each solution produced its own subset of challenges and/or potential security flaws. Those which produced solutions to these flaws tended to sacrifice functionality and usability. Below we compare each solution based on five yes or no properties. The first of these properties is that of whether the solution introduces its own faults. The second is that of whether the solution introduces reliability issues, for example, in the PUF solution proposed in Halak et al. (2016), PUF circuits have a degree of unreliability, and so may cause issues when implementing these solutions. The third property measures whether the solution places a certain limitation on the devices in the system, for example, in Shahzad and Singh (2017), a limit on the user friendliness of a device was considered, as too much can lead to vulnerabilities. The fourth of these properties measures whether a solution is resource intensive, as this can lead to efficiency issues and potentially increase latency of communications. The final of these is that of whether or not a solution makes use of an existing solution. Table 1 summarises and compares the reviewed approaches.

From what we can observe from the table above, each solution has a certain advantage over the others, and none of the solutions come without their own set of issues, be that relating to security or other areas. Almost all of these solutions introduce their own security risk, minus that of Tiburski et al. (2015). As well as this, only one of the proposed solutions comes without a certain limitation on the IoT device themselves.

It would seem that each solution favours one feature of security over another, and that something is sacrificed in order to secure a certain area of an IoT system. Whilst a complete security solution is very difficult to achieve, a system which combines various aspects from each of these solutions may be ideal. As smart houses, and smart house systems are growing as IoT technology progresses, the ideal system would have to be built with scalability in mind. The use of various devices in the home would also have to offer some level of usability, as well as various functionality. The solution proposed by Ning et al. comes close to this description, but without a solution to its own security flaws, it is not ideal.

4 CONCLUSION

Throughout this study we introduced the Internet of Things, as well as most of the security issues and challenges facing this field. Whilst a lot of the issues presented can be said about other technologies which are related to communication of data, the sensitivity of the data collected by IoT devices makes the threats posed by a potential attack much more harmful. Attacks to these systems could potentially cause the loss or theft of very personal information, either relating to the lives of the users, or sensitive medical information about the users.

We then went on to discuss solutions to the various issues posed by IoT systems; issues relating to scalability, authentication and authorization; and the lack of standardization between the various IoT devices and systems which exist today. Each of these were then compared in order to find a solution that would most ideally suited to a smart house environment.

From our previous discussions, we can conclude that scalability, due to the fact that home based IoT systems are constantly growing and changing as technology progresses, and reliable authentication, as home-based systems usually involve multiple users, seem to be the most prominent areas of security that should be considered. Future systems and solutions would need to take these into mind. As well as this, as home-based systems will receive a lot of user interaction, the system must be user friendly if it were to be implemented, without sacrificing security.

REFERENCES

Alam, M. A., Kufluoglu, H., Varghese, D., and Mahapatra, S. (2007). A comprehensive model for pmos nbti degradation: Recent progress. *Microelectronics Reliability*, 47(6):853–862.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26473v1 | CC BY 4.0 Open Access | rec: 31 Jan 2018, publ: 31 Jan 2018

Table 1. A summary of the reviewed solutions

Solution	Addresses	Introduction of Reliability Issues	Introduction of new attack vectors	Introduction of a limitation of Devices/Device Functionality	Resource Intensive	Use of Existing Solution
Keoh et al. (2014)	Security issues relating to standardization of communication protocol	No	Yes	Yes	No	Yes
Tiburski et al. (2015)		No	No	Yes	No	Yes
Shahzad and Singh (2017)	Security issues relating to Authentication and Authorization	Yes	Yes	Yes	Yes	No
Halak et al. (2016)		Yes	Yes	No	No	Yes
Nicanfar et al. (2011)		No	Yes	Yes	Yes	No
Ning et al. (2013)	Security issues relating to scalability and growth	No	Yes	No	No	No
Moosavi et al. (2015)		No	Yes	Yes	Yes	No
Li et al. (2013)		Yes	Yes (in the case of weak signal)	Yes	Yes	No

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26473v1 | CC BY 4.0 Open Access | rec: 31 Jan 2018, publ: 31 Jan 2018

Aldabbas, O., Abuarqoub, A., Hammoudeh, M., Raza, U., and Bounceur, A. (2016). Unmanned ground vehicle for data collection in wireless sensor networks: mobility-aware sink selection. *The Open Automation and Control Systems Journal*, 8(1).

AlFardan, N. and Paterson, K. G. (2012). Plaintext-recovery attacks against datagram tls. In *Network and Distributed System Security Symposium (NDSS 2012)*.

Aloraini, A. and Hammoudeh, M. (2017). A survey on data confidentiality and privacy in cloud computing. In *Proceedings of the International Conference on Future Networks and Distributed Systems*, ICFNDS '17, pages 10:1–10:7, New York, NY, USA. ACM.

Alsboui, T., Abuarqoub, A., Hammoudeh, M., Bandar, Z., and Nisbet, A. (2012). Information extraction from wireless sensor networks: System and approaches. *Sensors & Transducers*, 14(2):1.

Atwady, Y. and Hammoudeh, M. (2017). A survey on authentication techniques for the internet of things. In *Proceedings of the International Conference on Future Networks and Distributed Systems*, ICFNDS '17, New York, NY, USA. ACM.

Badii, A., Khan, J., Crouch, M., and Zickau, S. (2010). Hydra: Networked embedded system middleware for heterogeneous physical devices in a distributed architecture. In *Final External Developers Workshops Teaching Materials*, page 4.

Bohn, H., Bobek, A., and Golatowski, F. (2006). Sirena-service infrastructure for real-time embedded networked devices: A service oriented framework for different domains. In *Networking, international conference on systems and international conference on mobile communications and learning technologies, 2006. ICN/ICONS/MCL 2006. International conference on*, pages 43–43. IEEE.

Boulton, J. (2014). The first web celebrity was a coffee pot.

Carlin, A., Hammoudeh, M., and Aldabbas, O. (2015a). Defence for distributed denial of service attacks in cloud computing. *Procedia Computer Science*, 73:490–497.

Carlin, A., Hammoudeh, M., and Aldabbas, O. (2015b). Intrusion detection and countermeasure of virtual cloud systems-state of the art and current challenges. *International Journal of Advanced Computer Science and Applications*, 6(6).

Dibb, P. and Hammoudeh, M. (2013). Forensic data recovery from android os devices: an open source toolkit. In *Intelligence and Security Informatics Conference (EISIC), 2013 European*, pages 226–226. IEEE.

Ghafir, I., Prenosil, V., Alhejailan, A., and Hammoudeh, M. (2016a). Social engineering attack strategies and defence approaches. In *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, pages 145–149.

Ghafir, I., Prenosil, V., Svoboda, J., and Hammoudeh, M. (2016b). A survey on network security monitoring systems. In *Future Internet of Things and Cloud Workshops (FiCloudW), IEEE International Conference on*, pages 77–82. IEEE.

Halak, B., Zwolinski, M., and Mispan, M. S. (2016). Overview of puf-based hardware security solutions for the internet of things. In *Circuits and Systems (MWSCAS), 2016 IEEE 59th International Midwest Symposium on*, pages 1–4. IEEE.

Hammoudeh, M. (2008). Modelling clustering of sensor networks with synchronised hyperedge replacement. In *International Conference on Graph Transformation*, pages 490–492. Springer.

Hammoudeh, M. (2015). Applying wireless sensor networks to solve real-world problems. In *Proceedings of the International Conference on Intelligent Information Processing, Security and Advanced Communication*, page 1. ACM.

Hammoudeh, M. and Alsbou'i, T. A. (2011). Building programming abstractions for wireless sensor networks using watershed segmentation. In *Smart Spaces and Next Generation Wired/Wireless Networking*, pages 587–597. Springer.

Hammoudeh, M., Mount, S., Aldabbas, O., and Stanton, M. (2010). Clinic: A service oriented approach for fault tolerance in wireless sensor networks. In *Sensor Technologies and Applications (SENSORCOMM), 2010 Fourth International Conference on*, pages 625–631. IEEE.

Hammoudeh, M., Newman, R., Mount, S., and Dennett, C. (2009). A combined inductive and deductive sense data extraction and visualisation service. In *Proceedings of the 2009 international conference on Pervasive services*, pages 159–168. ACM.

Hammoudeh, M., Shuttleworth, J., Newman, R., and Mount, S. (2008). Experimental applications of hierarchical mapping services in wireless sensor networks. In *Sensor Technologies and Applications, 2008. SENSORCOMM'08. Second International Conference on*, pages 36–43. IEEE.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26473v1 | CC BY 4.0 Open Access | rec: 31 Jan 2018, publ: 31 Jan 2018

Keoh, S. L., Kumar, S. S., and Tschofenig, H. (2014). Securing the internet of things: A standardization perspective. *IEEE Internet of Things Journal*, 1(3):265–275.

Kim, M., Lee, J. W., Lee, Y. J., and Ryou, J.-C. (2008). Cosmos: A middleware for integrated data processing over heterogeneous sensor networks. *ETRI journal*, 30(5):696–706.

Li, F., Vögler, M., Claeßens, M., and Dustdar, S. (2013). Efficient and scalable iot service delivery on cloud. In *Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on*, pages 740–747. IEEE.

Moosavi, S. R., Gia, T. N., Rahmani, A.-M., Nigussie, E., Virtanen, S., Isoaho, J., and Tenhunen, H. (2015). Sea: a secure and efficient authentication and authorization architecture for iot-based healthcare using smart gateways. *Procedia Computer Science*, 52:452–459.

Newman, R. and Hammoudeh, M. (2008). Pennies from heaven: A retrospective on the use of wireless sensor networks for planetary exploration. In *Adaptive Hardware and Systems, 2008. AHS'08. NASA/ESA Conference on*, pages 263–270. IEEE.

Nicanfar, H., Jokar, P., and Leung, V. C. (2011). Smart grid authentication and key management for unicast and multicast communications. In *Innovative Smart Grid Technologies Asia (ISGT), 2011 IEEE PES*, pages 1–8. IEEE.

Ning, H., Liu, H., and Yang, L. T. (2013). Cyberentity security in the internet of things. *Computer*, 46(4):46–53.

Shahzad, M. and Singh, M. P. (2017). Continuous authentication and authorization for the internet of things. *IEEE Internet Computing*, 21(2):86–90.

Spiess, P., Karnouskos, S., Guinard, D., Savio, D., Baecker, O., De Souza, L. M. S., and Trifa, V. (2009). Soa-based integration of the internet of things in enterprise services. In *Web Services, 2009. ICWS 2009. IEEE International Conference on*, pages 968–975. IEEE.

Tiburski, R. T., Amaral, L. A., De Matos, E., and Hessel, F. (2015). The importance of a standard securit y archit ecture for soa-based iot middleware. *IEEE Communications Magazine*, 53(12):20–26.

Xiao, Q. (2005). Security issues in biometric authentication. In *Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC*, pages 8–13. IEEE.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.26473v1 | CC BY 4.0 Open Access | rec: 31 Jan 2018, publ: 31 Jan 2018