Hindawi
Complexity
Volume 2020, Article ID 6619498, 9 pages
https://doi.org/10.1155/2020/6619498

WILEY | Hindawi

Research Article

Cyber Security and Key Management Issues for Internet of Things: Techniques, Requirements, and Challenges

Mohammad Faisal[1], **Ikram Ali**[2], **Muhammad Sajjad Khan**[3], **Junsu Kim**[3], **and Su Min Kim**[3]

[1]*Department of CS & IT, University of Malakand, Chakdara 18800, Pakistan*
[2]*School of Automation Engineering, University of Electronic Science and Technology of China, Chengdu, China*
[3]*Department of Electronic Engineering, Korea Polytechnic University, Siheung, Republic of Korea*

Correspondence should be addressed to Su Min Kim; suminkim@kpu.ac.kr

Received 15 October 2020; Revised 24 November 2020; Accepted 30 November 2020; Published 15 December 2020

Academic Editor: M. Irfan Uddin

Internet of Things-based environments pose various challenges due to their anytime/anywhere computing, and the efficient cryptographic based key management is one of the major challenges in Internet of Things. The key management life cycle consists of initialization, key generation, key registration, key backup, key update, key recovery, and key revocation. Our contribution in this paper is to summarize the state-of-the-art key management schemes and techniques in different scenarios, such as mobile ad hoc networks, wireless sensor networks, and the Internet of Things environments. Further different issues related specifically to the Internet of Things environment are discussed and the causes and effects pertaining to the security breach for Internet of Things are identified. Furthermore, in this research work, we develop a novel permutation of threshold and identity-based key management schemes for the Internet of Things environment and have proposed future directions to counteract the attacks on confidentiality, integrity, authentication, and availability of security services in the Internet of Things environment and identified the two key management schemes, that is, identity and threshold schemes for Internet of Things, to resolve Internet of Things key management issues and maximum possible security services effective implementation. We evaluate our scheme with the help of mathematical and statistical techniques.

1. Introduction

In communication technologies, a novel prototype for Internet of Things is grooming rapidly and effectively around the world. The future Internet, designed as an "Internet of Things," is foreseen to be "a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols" [1]. Due to its large scope, Internet of Things covers almost all available wired and wireless networks. The motto of Internet of Things is to connect all objects around us with distinct addressing identities. So that everything (static/dynamic) anytime around us can connect with each other to communicate/exchange information easily and effectively [1]. In Internet of Things, there is always an overriding concern about key management because of the unique characteristics of ad hoc networks, that is, broadcast medium, node mobility, dynamic topology, decentralized architecture, and random join and leaves as shown in Figure 1. Multihop communication provides an opportunity for mischievous nodes to eavesdrop data for the sake of deletion and packet drops and impersonation; later on they can laos launch different attacks like denial of service and replay attacks. such as denial of service attacks.

Due to security concerns, Internet of Things defines a dedicated field named key identifier module to implement key management schemes implicitly. The field is compatible to implement single keys, group keys, pairwise keys, and digital certificate keys as well. The field consists of two parts: key source and key index, respectively. The first part, key source, presents the origin of the key while the second

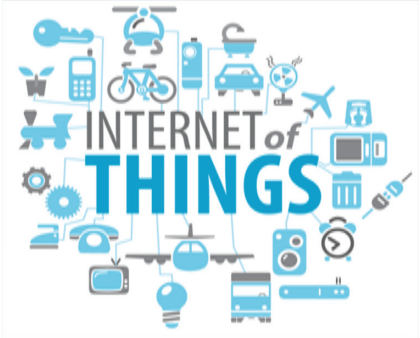

Figure 1: Internet of Things general overview.

part, key index, maintains the record of unique identification of the keys with the same origin [2]. Key management is a set of techniques to initialize, register, update, and recover keys for cryptographic mechanisms in order to ensure privacy, integrity, and authentication among authorized parties. Key management may also be called a process to revoke keys from compromised or detected malicious nodes and update keys for noncompromised ones. The contents of the key may consist of public/private key pairs, secret keys, nonsecret parameters, initialization parameters, and supporting key management in various instances, depending on the nature of the scheme being used, as shown in Figure 2. In Internet of Things, there is not only the issue of dynamic, static, and ad hoc infrastructure but also a challenge of open-source software. This software is available for all consumers for downloading the already available tools and uploading their novel tools without proper authorization and authentication. Hence, proper key management can ensure developers security in open-source environments like Internet of Things [1]. Mobile ad hoc networks (MANETs) consist of self-governing, mobile nodes that act as hosts as well as routers. These nodes are wirelessly interconnected to assist each other via packets' transmission. The internodes' transmission may be single hop (if the sender/receiver lies in the same range) or multihop (if the sender/receiver does not lie in direct range of each other). Since MANETs do not have a centralized control where devices are mobile and resource constraint as well, efficient key management is considered a challenging task for these networks [3, 4]. Wireless Sensor Networks (WSNs) consist of sensing, processing, and communicating data components only with limited capability, due to which, these nodes have constraints in data processing, storage, transmission range, and battery consumption. In addition to these constraints, the broadcast and unrestrained nature of WSN nodes make cryptographic key management a big challenge. Various schemes have been proposed over time; however, due to scalability reasons of WSN, symmetric cryptography is usually not tempting while asymmetric cryptography is also not preferable due to its heavyweight nature, in terms of battery and computational resources [3, 5–8].

The aim of this research work is to propose and evaluate a new key management solution proposed for the networks/platforms, such as MANETs, WSNs, and Internet of Things. These platforms cover a wide area of applications like surveillance, tracking special targets, flood detection, personal area networks, collaborative networks, military communications, disaster management area, and so on, while in Internet of Things, multiplatform software is distributed, which requires proper authorization, authentication, and auditing for which effective key management is mandatory [5, 6]. In this paper, we accumulate multiple key management schemes in Internet of Things area and highlight the pros, cons, and proposed solution. After that, we worked on our hybrid scheme of key management, which will work in both static and dynamic key management environment. We evaluate the efficiency of our scheme with the help of mathematical and statistical techniques and the results are shown in Figures 3 and 4.

The rest of the paper is organized as follows. In Section 2, the background of Internet of Things is argued. In Section 3, key management schemes are classified with respect to their various key distribution methods. Every class is then subclassified and explained with the help of examples. In Section 4, the key management schemes are evaluated with defined parameters. In Section 5, related work is collected since 1976; we identified and presented the security services provided by each and every scheme, attacks successfully encountered by the respective scheme, and the vulnerabilities exploited. In Section 6, differnet challenges are higlighted. In Section 7, the methodology of our proposed scheme is evaluated and discussed. In Section 8, conclusion and future work are discussed.

2. Literature Review

Considerable research has been done on key management in MANET, WSN, and Internet of Things. In this paper, we examined and discussed each and every scheme datewise, starting from 1976. So far, many schemes are based on Hellman; for that reason, it is enlisted here as a beginner/pioneer scheme. This scheme relies on a discreet logic problem which determines an exclusive symmetric key onetime generated between two parties. The scheme ensures intrusion tolerance by avoiding sniffing attack; however, it still vulnerable to man in the middle, impersonation, repudiation, denial of service, Botnets, and Sybil attacks [9, 10]. The name implies ubiquitous network access

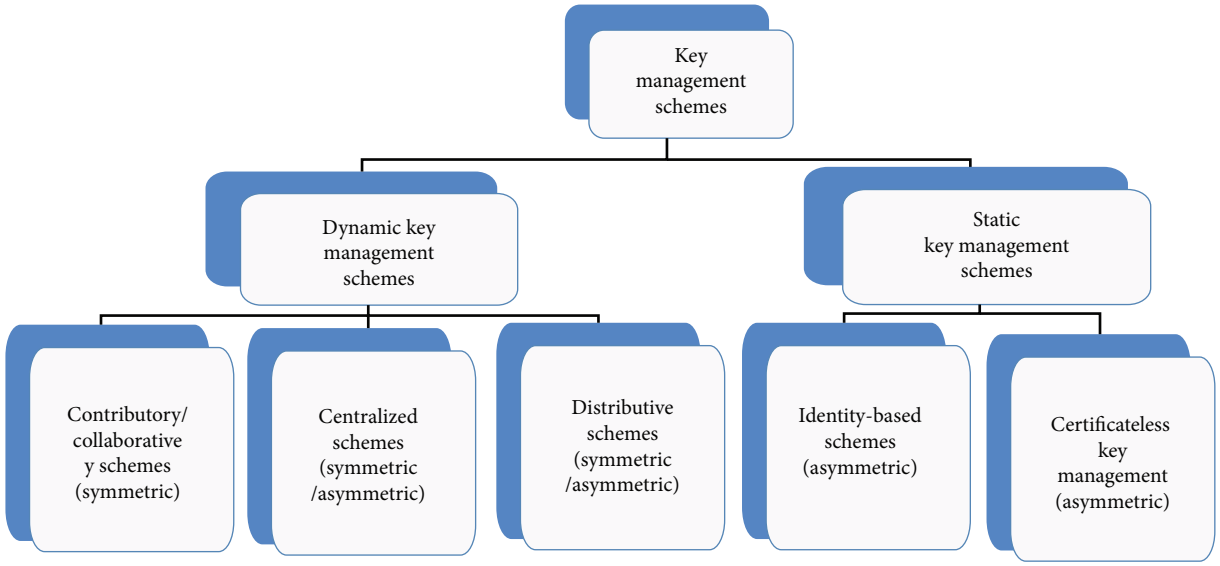

Figure 2: Classification of key management.

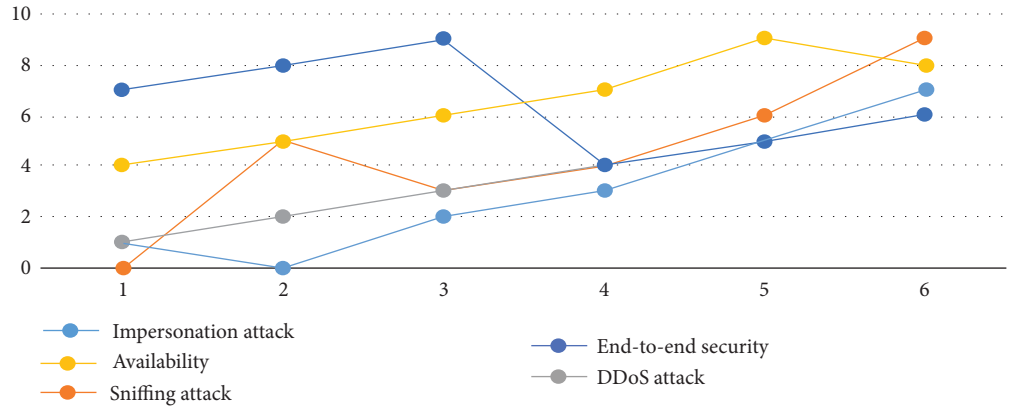

Figure 3: Static key management schemes versus attacks for UDP data.

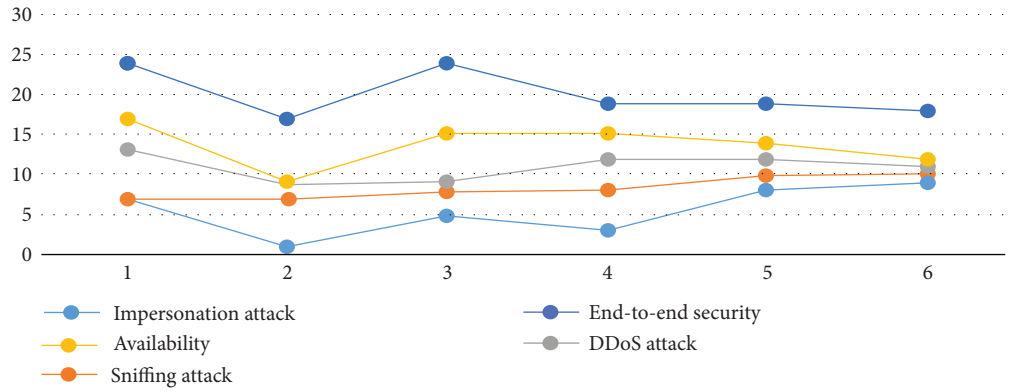

Figure 4: Dynamic key management schemes versus schemes for TCP data.

in Internet of Things computing, offering anytime and anywhere network access for users. This Internet of Things architecture can scale horizontally or vertically as required to either attach or detach the mobile nodes with a little bit change in the topological infrastructure that can make the end users feel as if they are connected to wired network services. However, the utilization of this network infrastructure confidently is still a contentious issue for the service providers in order to prepare its authorization on hardware bases [1, 11–13]. The Internet of Things is assuring availability services of security due to its five main distinct services (like on-demand self-service, ubiquitous network access, location-independent resource pooling, rapid elasticity, and measured service). On-demand self-service means to provide its users the requested/demanded service at its earliest time. Ubiquitous network access means anywhere and anytime available service. Location-independent resource pooling means to provide a pool of resources irrespective of its location anywhere/anytime. Rapid elasticity means extensions of the environment to all users in a short span of time. Measured services mean all the services can be measured by countering their usage and productivity [14]. Internet of Things operation is based on four operational models, that is, public, private, community, and hybrid but it still leaves an open door of vulnerabilities for the security services [12, 15, 16]. Internet of Things on-demand services shares all the possible and available resources for computation. The services might be available either between or within the Internet of Things according to the demand of the users. System resources like servers, network, storage, and applications are provided to users if and when required by the Internet of Things on a lease basis [15]. Internet of Things also offers location freedom for an unrestrained pool of resources in the form of either hardware or software. The client is independent and may not be able to find out the exact location of the resources unless and until the location is requested or required by the service provider to be found out. Its reliability and availability are assured through either multiple distributed sites or fast and quick disaster recovery services. But the user's authorization and authentication are still a blazing issue [12, 13]. The authors pointed out that Internet of Things is swift in flexibility and can accommodate users of heterogeneous nature within the least possible time without any individual interface for computing resources as required. Even in some cases, resources are assigned to users automatically which gives a safe passage for the intruder to enter and seize the system. All these services are measured on the basis of processing time and memory utilization [16–19]. In this paper, we have classified, analyzed, and diagnosed the key management problems in both ad hoc and Internet of Things. To the best of our ability, we have combined the expertise of almost all recent key management schemes implemented in ad hoc networks and suggested the two key management schemes, that is, identity and threshold schemes for Internet of Things, to resolve both Internet of Things key management issues and maximum possible security services implementation.

3. Classification of Key Management Schemes

Before evaluating various key management schemes, we are going to explain some preliminary concepts of key management in cryptography. Symmetric key cryptography also known as shared key ciphers/algorithms is that type of cryptography in which the same key is used by both the sender and receiver for the encryption and decryption of plaintext and ciphertext, respectively. The symmetric algorithms may be stream or block ciphers. In stream ciphers, the encryption/decryption can execute one digit at a time while in block ciphers, the encryption and decryption execute number of bits at a time in a blockwise fashion [17]. Asymmetric key cryptography uses two types in a pair called as public key and private key in a a pair thats why it is also called as public key cryptography. The private key is used to decrypt the cipher text and generate the digital signature, whereas the public key is used to encrypt plaintext and to verify the digital signature [17]. Trusted third party is certification authority that grants a digital certificate. The certificate is usually the public key of that organization to whom this certificate is issued. A third trust party acceptable by both sender and receiver is performing the task of guarantor [18]. Man in the middle attack, MIM, can be shortened as MITM. MITMA is a form of active eavesdropping in which the intruder makes autonomous connection in between the sender and receiver deceiving that they are connected with each other, although in reality, the intruder is sniffing their communication [20]. Session key is a symmetric key assigned for only one single and dedicated communication session between the sender and receiver. The session key must be chosen by both the sender and receiver before the session started. It reduces the intruders prediction if disclosed as the key must be changed for the nest session [21]. In the related literature, key management solutions have been classified in different manner. However, in this paper, key management schemes are mainly classified into two broad classes, that is, static and dynamic. These classes are further catalogued into different subcategories as presented in Figure 2 and explained in the following sections.

3.1. Dynamic Key Management Schemes (DKM). In dynamic key management schemes, different keys are assigned for different sessions. Once the communication session terminated or finished between the sender and receiver, the keys for the next session will be dynamically assigned to nodes without any revocation or updating command. In dynamic key management schemes, it is observed that the keys are created dynamically as the communication is supposed to be

initiated between the sender and receiver in three main fashions, contributory, centralized, and distributive, discussed one by one with the help of an example in the forthcoming sections. In dynamic key management schemes, on the other hand, different keys are assigned for different sessions. Once the communication session terminated or finished between the sender and receiver, the key for the next session will be dynamically assigned without any revocation or updating command.

3.1.1. Contributory/Distributed Key Management Schemes. Contributory/distributive schemes are symmetric cryptographic based solutions characterized by the lack of a trusted third party which is normally responsible for the generation and distribution of the cryptographic keys [3]. All the participating groups have to ascertain or agree upon a secret symmetric key. The keys can be generated in pairs or in a group of more than two for only two parties or for a group, respectively, specifically for an ongoing session. Hence, it is sometimes characterized by a session key as well [9]. Therefore, due to its spontaneous and self-organizing nature, it is most favorable to be used for Internet of Things-based ad hoc networks. Due to the ad hoc and sparse structure of the networks under discussion (Cloud, MANETs, and WSN) and the contributory nature of these schemes, these schemes require costly cryptographic operations [9, 10, 19]. All these schemes are considered asymmetric cryptographic schemes.

3.1.2. Centralized Key Management Schemes. These schemes require centralized trusted authority (TA) which is designated to generate and distribute a unique session key for all concerned group members in the Internet of Things [19]. The key in Internet of Things update is difficult to manage because of its dynamic topology and its connection is varied with multiarchitecture clients/nodes [9, 19]. In these schemes, the user's public key is certified by either semi- or fully distributed certification authority. While using its public key by any user, its validity must be verified by the respective certification authority. For ad hoc networks, the certificate creation, distribution, storage, updates, and revocation are unaffordable due to their resource-constrained nodes [22]. Usually, TA-based cryptographic solutions are considered more efficient than that of decentralized based solutions. However, the distributed dynamic ad hoc nature of MANT, WSN, and Internet of Things makes it unsuitable for these networks.

3.1.3. Distributed/Threshold Key Management Schemes. Distributive schemes involve one or more trusted entities for key distribution; hence, their architecture is not explicitly centralized. These schemes can use both flavors of cryptography, that is, asymmetric and symmetric systems. Internet of Things requires the trusted entity to be established spontaneously during the network initialization. In distribution key management schemes, each TA generates a key and allocates the key to the respective participating nodes [10].

3.2. Static Key Management Schemes (SKM). In static key management schemes, the key is created for the overall lifetime of nodes by either mutual agreement, symmetric cryptography, or centralized certification authority, in asymmetric cryptography. In the static key management approach, keys are assigned for the lifetime of nodes, whereas in dynamic key management, keys are assigned to nodes for each session. In static key management schemes, the key is created either by mutual agreement, such as in symmetric cryptography, or by a certification authority, such as in asymmetric cryptography. The key is created once and then remained applicable until and unless updated or revoked by the certification. In the following subsections, we will discuss different schemes of static key management where the keys are created proactively before the communication is started.

3.2.1. Identity-Based Key Management Schemes. As the name implies, in these schemes, the public key is generated based on the identity of a node, such as e-mail address, IP address, or MAC address, while the private key is generated by a trusted third party called a Private Key Generator (PKG). Nevertheless, there are some common drawbacks in these schemes; for example, there is a lack of privacy and anonymity as their public keys are the node focal identities [10, 22, 23]. These schemes are always using public key cryptography as the pair of keys is created. The public key is its IP/MAC/e-mail address and the private key is generated on the basis of these keys.

3.2.2. Certificateless Key Management Schemes. Until recently, primarily research work in key management is based on identity-based public key cryptography (ID-PKC) [23] and traditional public key infrastructure (PKI). Any key management scheme was based upon these two schemes [9]. Certificateless key management schemes are key management approaches that use certificateless public key cryptography (CLPKC) [22], while for imposing limitations and constraints on the key generation, the threshold cryptography schemes are used [9]. Being an intermediary between PKI and ID-PKI, these schemes do not need certificates and hence do not suffer from key escrow problem (which is also known as fair cryptosystem). In fair cryptosystem, the encryption key is placed in escrow (contractual agreement) for check and balance purposes. The authorized competent authority (e.g., government) can check the makeup of the data under consideration. In

Table 1: Evaluation parameters.

S no.	Security services	Attacks (active or passive) on respective service
1	Confidentiality	Eavesdropping, sniffing, and wiretapping
2	Integrity	Modification and insertion
3	Authentication	Impersonation
4	Nonrepudiation	Repudiation
5	Availability	Denial of service

contrast to identity-based key management schemes, in CLPKC, the public key could not be computed from a user identity only. CLPKC diminishes the computation and improves the efficiency as the scheme does not need authenticated certificates. For effective use of network bandwidth and to prevent a single point of failure, CLPKC is using threshold cryptography in which the key generation attempts are counted and allowed up to some defined threshold [22]. The Key Generation Center (KGC) supplies a user with a partial private key that the KGC computes from the user's identity and a master key. The master key is general for all the nodes while the private partial key is different for each user. The user then combines the partial private key with some secret information to generate the actual private key, and the KGC is just initiating the private key generation process and the final private key is the combination of the KGC generated value with the addition of user secret data/information irrespective of the KGC knowledge and jurisdiction [22].

4. Evaluation Parameters

In this research work, we explored and evaluated various schemes with respect to the achieved services and attacks counteracted in MANETs, WSNs, and Internet of Things. Furthermore, the drawbacks and limitations of the proposed schemes are assessed in terms of vulnerabilities and nontackled attacks. We compiled Table 1, which shows various security services explained here. Confidentiality means unaccessible from intruders. Integrity means unreadable for intruders. Authentication means accessible for the right users only. Nonrepudiation means that either one or both the sender and receiver deny later on after the exchange of data. Availability means to ensure that the service is available around the clock 24/7. Attacks may be either active or passive according to their effects on the data concerned [5, 19]. In a passive attack, the intruders only sniff or analyze the data rather than modifying the data. Passive attacks consist of eavesdropping, sniffing, wiretapping, and so on. All these attacks can be launched to disrupt the confidentiality service [7], while in active attacks, the intruder may change or destroy the contents of the data or source of the data. Types of active attacks are modification, insertion, impersonation, repudiation, and denial of service attacks. All these attacks can be launched to derail integrity, authentication, nonrepudiation, and availability services [7, 23, 24]. To put it briefly, we concluded that confidentiality, integrity, and authentication services are comparatively best controlled by identity-based key management schemes, while the denial of service attacks are resisted effectively by threshold-based key management schemes [9, 10, 22, 23]. In the next section, we present a detailed literature review of various solutions in the area of key management for MANETs, WSNs, and Internet of Things.

5. Discussion

In the previous section, we have analyzed and evaluated various schemes and solutions available for key management. The literature shows that the Internet of Things suffers profoundly from key management problems such as key creation, distribution, updating, and revocation. That is why it is still a challenging issue for these computing environments because of its multiarchitecture latest operating systems platforms with multiple undisclosed vulnerabilities. The abovementioned summarized schemes are proposed for MANETS and WSN but there is no sufficient work done on Internet of Things-based ad hoc networks due to the unique characteristics of Internet of Things infrastructure, which are discussed in the following. In this section, the discussion will point out various issues and challenges specifically pertaining to Internet of Things. In Internet of Things infrastructure, the ideal situation is when the host is executing as a hypervisor, crafting multiple virtual machines which are able to run any operating system platform software for its remote users, whereas hardware like processors and memory is placed at the data centers irrespective of geographical location for all end users. Both of these hardware and software level services are provided by the Internet of Things environment in the abovementioned three models [12]. In infrastructure as a service, the Internet of Things is permitting the consumers the storage, processing, and network services along with deployment of software like operating systems and application software. On these types of deployed software, the customers can also be able to control and manage them with nominal network components [12, 14, 25]. Since consumers are capable of using the storage to save their data, how the issue of time

bombs, worms, viruses, Trojan horses, and rootkits can be contained in such environments? If the infrastructure is shared with the customers, how the users can be authenticated and authorized? How the symmetric/asymmetric key will be shared and distributed? Four deployment models have been identified for Internet of Things architecture which is the main cornerstones of the key management issues. They are private, community, public, and hybrid deployment models [15, 16]. In the private Internet of Things deployment model, the software, infrastructure, and all application resources are dedicated to private (and a single) association. For effective management, it is often governed by a third party while the Internet of Things may be deployed on or off sites. Here, the Internet of Things will be strict enough for its key management policies but it will be isolated from the rest of the world for its communication due to its private nature [25]. In the community Internet of Things deployment model, the applications, software, and infrastructure resources are shared by multiple organizations/communities who must restrain common security concerns and employ the same policy and observance deliberations. The community clouds like its predecessor may be engaged by third guarantor and may be deployed on site or off site locations [14]. Every Internet of Things is looking for its own purposes and business extensions in which key management policies cannot be maintained for an all-in-one package which should be addressed by user to user policy of key management. In the public Internet of Things as the name indicated, all the applications, software, and infrastructure resources are accessible to any user generally for usage. With the increase of users in the Internet of Things, the key management issues increased drastically [11]. The hybrid Internet of Things deployment model is the combination of any two or all of the abovementioned deployment models facilitating the end users with all facilities. The inter-Internet of Things infrastructure is based on specific standard guidelines and policies for data accessibility and protection but also gives the intruders the chances of different possible active and passive attacks.

6. The Identified Issues and Challenges

To the best of our ability, after evaluating multiple schemes in different platforms (MANETS, WSN, and Internet of Things), we identified that, in contrast with Internet of Things, the following recommendation may be considered as open research issues and challenges in Internet of Things. Impersonation: The Internet of Things prime concern is to provide access for data to all users but the question is only the system authorized users can access the data after specific verification which is normally utilized and controlled by usernames passwords or digital certificates, but the issue still does not counteract the attacks like impersonation. Sniffing/tapping: To achieve privacy on both sides for the data of the service provider and the privacy of the user of the data, make the user privileges accountable from sniffing and tapping. End-to-end security: To avoid modification/insertion in the data and assure end-to-end security between the Internet of Things service provider and the user are mandatory for swift and secure communication. Providing a virtual private network between the remote virtual machines is insufficient to provide the required security level. Availability: The access control mechanisms need to be enhanced to ensure the availability service for the users with external users (client/provider of Internet of Things environment) and internal users within the Internet of Things or the multiple Internet of Things domains access and permission policies. Here, due to the dynamic nature, the privacy of Internet of Things nodes and least privileges access control cannot be maintained with passwords and usernames only. Denial of service attack: For a contingency plan, in case of denial of service and distributed denial of service attacks, the Internet of Things needs to either observe the rapid recovery of the servers or execute the distributed computing concepts which are not the only solutions for the said attacks.

7. Methodology

The research work is a part of our ongoing research to identify and develop a novel identity-based key management schemes for Internet of Things environment using mathematical validations and statistical permutation of the threshold value of the secret key, as shown in the following sections. Mathematical validation: The mathematical evaluation is elaborated by means of algorithmic notations and mathematical formulae as shown in Algorithm 1.

Statistical evaluation: based on the literature review conducted, the following analysis has been observed in both static and dynamic key management schemes with respect to the evaluation parameters (confidentiality, integrity, authentication, nonrepudiation, and availability) given in Table 1. Challenges identified in Section 7 are also evaluated in both classes of key management (static/dynamic). In end, all the results are accumulated and their graphical representation is shown here by applying the SPSS tool. Proposed hybrid model (SKM + DKM): in our scheme, we classify the encryption on the basis of the nature of data processing on. For UDP data, symmetric key cryptography will be used, while for TCP communication, asymmetric key cryptography will be used. The proposed scheme is shown in the following figures.

(1) *Step 1: Key Initialization, KI ab initio*ϒ
(2) *Step 2: key Generation, KG* Ш ≥ *0*
(3) *Step 3: key Registration, Kreg V*
(4) *Step 4: key Backup, KB*
(5) *Step 5: key Update, KU*
(6) *Step 6: key Recovery Krec*
(7) *Step 7: key Revocation Krev*
(8) *Threshold value calculation*
(9) *IF 0* ∫^{n} *(KI + KG + K.reg + KB + KU + KREV + KREV) ≤ 1 then Ok*
(10) *ELSE if 0* ∫^{n} *≥ 1, then Ţ!*
(11) *END IF*

Algorithm 1: Algorithmic evaluation (ϒ, Ш, ∫).

8. Conclusion and Future Work

Authentication, authorization, and then verification of the trusted clients/nodes in Internet of Things are the prime concerns in these networks which can only be counteracted through proper and effective devising of key management mechanisms. Currently, the key management schemes are based on either public key management system or trusted third party system like a certification authority; however, there are gaps of multiple user resource access or single-user multiple resource access problems. Here, in this research work, we develop a novel permutation of threshold and identity-based key management schemes for Internet of Things environment, while security services and attacks for Internet of Things environment are identified with its issues and challenges as a future work as well.

Data Availability

The data are available upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest to report regarding the present study.

Acknowledgments

This work was supported in part by the MIST (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) Support Program (IITP-2020-2018-0-01426) supervised by the IITP (Institute for Information and Communication Technology Planning & Evaluation) and in part by the National Research Foundation (NRF) funded by the Korea Government (MIST) (no. 2019R1F1A1059125).

References

[1] J. Li, M. Nazir Jan, and M. Faisal, "Big data, scientific programming, and its role in internet of industrial things: a decision support system," *Scientific Programming*, vol. 2020, Article ID 8850096, 7 pages, 2020.

[2] X. Liao, M. Faisal, Q. Qing Chang, and A. Ali, "Evaluating the role of big data in IIOT-industrial internet of things for executing ranks using the analytic network process approach," *Scientific Programming*, vol. 2020, Article ID 8859454, 7 pages, 2020.

[3] I. Ali, M. Faisal, and S. Abbas, "A survey on lightweight Authentication schemes in vertical handoff," *International Journal of Cooperative Information Systems*, vol. 26, no. 1, Article ID 1630001, 2017.

[4] J. Granjal, E. Monteiro, and J. Silva, "Security for the internet of things: a survey of existing protocols and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015.

[5] M. Faisal, S. Abbas, H. Ur Rahman, M. Zahid Khan, and A. Ur Rahman, "An analysis of DDoS attacks on the instant messengers," *Security and Communication Networks*, vol. 2019, Article ID 1751285, 8 pages, 2019.

[6] F. Ullah, M. Zahid Khan, M. Faisal, H. Ur Rahman, S. Abbas, and F. S. Mubarek, "An energy efficient and reliable routing scheme to enhance the stability period in wireless body area networks," *Computer Communications*, vol. 165, pp. 20–32, 2020.

[7] S. Smaldone, L. Han, P. Shankar, and L. Iftode, "RoadSpeak: enabling voice chat on roadways using vehicular social networks," in *Proceedings of the 1st Workshop on Social Network Systems*, New York, NY, USA, April 2008.

[8] M. Faisal, S. Abbas, and H. Ur Rahman, "Identity attack detection system for 802.11-based ad hoc networks," *EURASIP Journal on Wireless Communications and Networking 2018*, vol. 128, 2018.

[9] A. M. Hegland, E. Winjum, S. F. Mjolsnes, C. Rong, O. Kure, and P. Spilling, "A survey of key management in ad hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 8, no. 3, pp. 48–66, 2006.

[10] K. Gomathi and B. Parvathavarthini, "An efficient cluster based key management scheme for MANET with authentication," in *Proceedings of the Trendz in Information Sciences & Computing*, pp. 202–205, Chennai, India, January 2010.

[11] Z. Jie, "A survey on trust management for VANETs," in *Proceedings of the IEEE International Conference on 2011 Advanced Information Networking and Applications (AINA)*, pp. 105–112, Biopolis, Singapore, March 2011.

[12] A. El-Sayed, "Clustering based group key management for MANET," in *Advances in Security of Information and Communication Networks*, A. Awad, A. Hassanien, and K. Baba, Eds., Springer, Berlin, Germany, pp. 11–26, 2013.

[13] S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure data aggregation in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 1040–1052, 2012.

[14] L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2019.

[15] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583–592, 2012.

[16] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Computer Systems*, vol. 25, no. 6, pp. 599–616, 2009.

[17] H. Takabi, J. B. D. Joshi, and G.-J. Ahn, "Security and privacy challenges in cloud computing environments," *IEEE Security & Privacy Magazine*, vol. 8, no. 6, pp. 24–31, 2010.

[18] N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: a survey," *Future Generation Computer Systems*, vol. 29, no. 1, pp. 84–106, 2013.

[19] F. R. Yu, H. Tang, P. C. Mason, and F. Wang, "A hierarchical identity based key management scheme in tactical mobile ad hoc networks," *IEEE Transactions on Network and Service Management*, vol. 7, no. 4, pp. 258–267, 2010.

[20] G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, "Smart objects as building blocks for the internet of things," *IEEE Internet Computing*, vol. 14, no. 1, pp. 44–51, 2018.

[21] T. Schneider, I. von Maurich, and T. Guneysu, "Efficient implementation of cryptographic primitives on the GA144 multi-core architecture," in *Proceedings of the 2013 IEEE 24th International Conference on Application-Specific Systems, Architectures and Processors*, pp. 67–74, Washington, DC, USA, June, 2013.

[22] L. Junhai, X. Liu, and Y. Danxia, "Research on multicast routing protocols for mobile ad-hoc networks," *Computer Networks*, vol. 52, no. 5, pp. 988–997, 2008.

[23] L. Rongxing, L. Xiaodong, Z. Haojin, and S. Xuemin, "SPARK: a new VANET-based smart parking scheme for large parking lots," in *Proceedings of the IEEE in INFOCOM*, pp. 1413–1421, Rio de Janeiro, Brazil, April 2009.

[24] G. Yan, W. Yang, D. B. Rawat, and S. Olariu, "Smartparking: a secure and intelligent parking system," *IEEE Intelligent Transportation Systems Magazine*, vol. 3, no. 1, pp. 18–30, 2011.

[25] Q.-B. Sun, J. Liu, S. Li, C.-X. FAN, and J.-J. Sun, "Internet of things: summarize on concepts, architecture and key technology problem," *Journal of Beijing University of Posts and Telecommunications*, vol. 3, no. 1, pp. 1–9, 2019.