ISSN: 2181-4341, IMPACT FACTOR (RESEARCH BIB) – 7,245, SJIF – 5,431

Madina Rustamqulova Ihtiyor qizi
rustamqulovamadina200@gmail.com
Muhammad Al-Xorazmiy nomidagi TATU universiteti Kiberxavfsizlik fakulteti talabasi

INTERNET BUYUMLARIDA TURLI AUTENTIFIKATSIYA MEHANIZMLARINI TADQIQI

ANNOTATSIYA: Mazkur maqolada IoT(Internet of Things) qurilmalari,axborotni kriptografik himoyalash,identifikatsiya va autentifikatsiya, axborotni himoyalashda autentifikatsiyaning ahamiyati, sog'liqni saqlash tizimida IoT qurilmalarining zaruriyati va autentifikatsiya mehanizmlarining afzalliklari haqida ma'lumot berilgan.

Kalit so'zlar: raqamli texnalogiya, IoT(Internet of Things) qurilmalari ,parolga asoslangan autentifikatsiya, sertifikatga asoslangan autentifikatsiya, biometrik autentifikatsiya, ikki faktorli autentifikatsiya, O'zaro autentifikatsiya (Mutual Authentication), HMAC (Hash-based Message Authentication Code)

АННОТАЦИЯ: В статье представлена информация об устройствах IoT (Интернета вещей), криптографической защите информации, идентификации и аутентификации, важности аутентификации в защите информации, необходимости использования устройств IoT в системе здравоохранения и преимуществах механизмов аутентификации.

Ключевые слова: цифровые технологии, устройства IoT (Интернет вещей), аутентификация на основе пароля, аутентификация на основе сертификатов, биометрическая аутентификация, двухфакторная аутентификация, взаимная аутентификация, HMAC (код аутентификации сообщения на основе хэша).

ABSTRACT: This article provides information about IoT (Internet of Things) devices, cryptographic protection of information, identification and authentication, the importance of authentication in the protection of information, the need for IoT devices in the health care system, and the advantages of authentication mechanisms..

Keywords: digital technologies, IoT (Internet of Things) devices, password-based authentication, certificate-based authentication, biometric authentication, two-factor authentication, mutual authentication, HMAC (hash-based message authentication code).

KIRISH

Raqamli texnalogiyalar tobora rivojlanib ketayotgan bir davrda IT hodimlari umuman insonlar orasida IoT(Internet of Things) qurilmalari atamasi ham tez tez takrorlanyapti.

IoT(Internet of Things) qurilmalari – bu internet tarmog'iga ulangan va ma'lumot almashish imkoniyatiga ega bo'lgan,turli maqsadlar uchun foydalanish mumkin bo'lgan elektron qurilmalar hisoblanadi.Ushbu qurilmalar har xil sanoatlar,uylar va korxonalar uchun avtomatlashtirgan funksiyalarni bajarish va samaradorlikni oshirish uchun yaratilgan.IoT qurilmalari odatda sensorlar,tarmoqqa ulanish imkoniyatlari va ma'lumotlarni qayta ishlash texnalogiyalari bilan jihozlangan bo'ladi. Internet tarmoqlari buyumlaridan biz kundalik davomida o'zimiz bilgan va bilmagan holatlarimizda foydalanamiz.Masalan:Sog'liqni saqlash IoT qurilmalari,Turar joy IoT

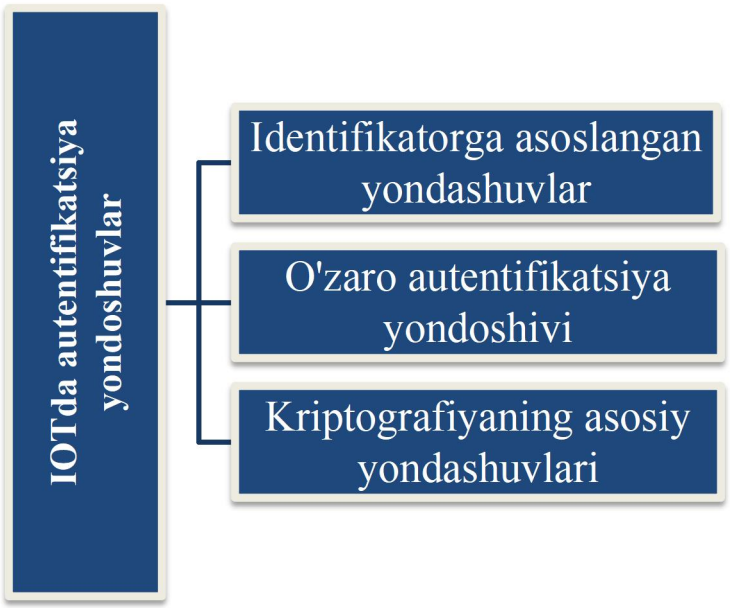
qurilmalari, Avtomobillar va transport vositalari IoT qurilmalari, Aqlli shahar(Smart City) IoT qurilmalari va x.k.

Turar joy IoT qurilmalari,xususan Aqlli eshik qo'ng'iroqlari va xavfsizlik kameralar eshik oldida kim bolrigini kuzatish va masofadan turib video monitoring qilish imkonini beradi.Bunday hollarda IoT tarmoqlarida xavfsiz autentifikatsiya usullari qurilmalarni noqonuniy kirishdan himoya qilish,ma'lumotlarning maxfiyligi va butunligini saqlashda katta ahamiyat kasb etadi. Ya'ni Autentifikatsiya – ma'lum qilingan foydalanuvchi,jarayon yoki qurilmaning haqiqiy ekanligini tekshirish uchun foydalaniladi.Bu tekshirish foydalanuvchi (jarayon yoki qurilma) haqiqatdan aynan o'zi ekanligiga ishonch hosil qilish imkonini beradi. Autentifikatsiya o'tqazishda tekshiruvchi taraf tekshiriluvchi tarafning haqiqiy ekanligiga ishonch hosil qilishi bilan bir qatorda tekshiriluvchi taraf ham axborot almashinuvi jarayonida faol qatnashadi.Odatda foydalanuvchi tizimga o'zi xususidagi noyob,boshqalarga ma'lum bo'lmagan axborotni(masalan,parol yoki sertifikat) kiritishi orqali o'zinig shaxsi(nomi,(identifikatsiya jarayoni))ni tasdiqlaydi.

IoT ning masofaviy foydalanuvchilari sensorli elemant yoki sensor tugunini IoT muhitiga ulash orqali aqlli qurilmalar yordamida tarmoq resurslariga osongina kirishlari mumkin.Ya'ni ulanish o'rnatilgandan so'ng qonuniy foydalanuvchi autentifikatsiya jarayoni orqali IoT resurslariga bog'lana oladi.IoT mahsulotlarida autentifikatsiya uchta muhim jihatga ega.Ayniqsa Xavfsizlik sanoati IoT ilovalari uchun muhimdir.Avtomatlashtirish va monitoring jarayaoni kabi ilovalar sensor tarmoqlari yordamida autentifikatsiya qilingan va shifrlangan ma'lumotlar almashinuvini qo'llab quvvatlash uchun end- autentifikatsiyani talab qiladi.

Cheklangan dastur protokoli (COAP) energiya yoki cheklangan xotira qurilmalari yordamida IoT qurilmalaring dasturiy qatlamida qo'llaniladi.Bu haqida ma'lumotlar havolasi darajasi kriptografik kengaytmalar Elektr va elektronika muhandislari institute (IEEE) 802.15.9 standartlariga kiritilgan.Aqlli shahar ishlanmalari odatda bir nechta IoT qurilmalarini o'z ichiga oladi va zararli hujumlarga qarshi turish uchun tegishli xavfsizlik tizimiga tayanishikerak bo'ladi.Qurilmaning kengayishi ierarxik termoq strukturasidan foydalanish orqali erishiladi.

IoT xavfsizligining eng muhim talabi to'g'ri autentifikatsiyadir.IoT qurilmalari o'rtasida xavfsiz seansni o'rnatishning dastlabki bosqichi autentifikatsiya mexanizmini aniqlashdan iborat. Autentifikatsiya jarayoni qurilma xotirasiga maxfiy ma'lumotlarni saqlamasdan samarali va xavfsiz tarzda amalga oshirilishi zarurdir. Ushbu xavfsizlik muammolari yengil yondashuv,o'zaro autentifikatsiya,identifikatsiyaga asoslangan autentifikatsiya va asosiy kelishuvga kirishni boshqarish mehanizmi kabi autentifikatsiyaning turli usullarini joriy etish orqali muammoning yechimi hal qilinmoqda.IoT ilovalarida xizmat ko'rsatuvchi provayderlar,sensor tugunlari va qayta ishlash tizimlari kabi obyektlar ishonchli tarmoqni yaratish uchun tugunlarni bir-biriga nisbatan autentifikatsiya qilishlari nazarda tutiladi. Autentifikatsiya protokoli nafaqat zararli hujumlarga qarshilik ko'rsatishi,balki u yomon ishlaydigan holatlarda qo'llanilishi uchunmos ravishda bo'lishi talab etiladi.Quyida IoT da Autentikatsiya usullarining tahminiy toifalari ko'rsatilgan:



1-rasm. Autentifikatsiya yondoshuvlari

Autentifikatsiya vositalarini aqlli qurilmalardagi o’rnini Sog'liqni saqlash IoT qurilmalari misolida olib qarasak, ular shaxsiy tibbiy ma'lumotlarni himoya qilish, xakerlik hujumlarining oldini olish va tarmoq xavfsizligini ta'minlash uchun ishlatiladi. Bu qurilmalar bemorlarning sog'lig'ini kuzatadi, shaxsiy ma'lumotlarni yig'adi va tibbiyot xodimlariga yuboradi, shuning uchun autentifikatsiya vositalari juda kuchli va ishonchli bo'lishi kerak.

IoT tarmoqlarida asosan Parolga asoslangan autentifikatsiya, Sertifikatga asoslangan autentifikatsiya, Biometrik autentifikatsiya, O'zaro autentifikatsiya (Mutual Authentication),HMAC (Hash-based Message Authentication Code) kabi xavfsiz autentifikatsiya mexanizmlaridan foydalaniladi.

Parolga asoslangan autentifikatsiya - an’anaviy ko’p martali parollarni ishlatishga asoslangan bo’lib,u autentifikatsiyaning keng tarqalgan sxemalaridan biridir.Biroq bu eng oddiy usullardan biri bo’lganligi sababli sog'liqni saqlash tizimlari uchun kamchiliklarga ega bo'lishi mumkin. Ya’ni parollarni oson buzish mumkin va ularni qayta ishlatish xavfli. Tibbiy IoT qurilmalari kam resursga ega bo'lganligi sababli kuchli parolni boshqarish qiyin bo'lishi mumkin.

Sertifikatga asoslangan autentifikatsiya – kriptografik kalitlar yordamida amalga oshiriladi.Sertifikat olish uchun foydalanuvchi sertifikatsiya markaziga shaxsini tasdiqlovchi ma’lumotni va ochiq kalitni taqdim etilishi zarur bo’ladi. Har bir qurilma yoki foydalanuvchi shaxsiy va jamoatchilik kalitlariga ega bo'ladi, va ulardan foydalanib autentifikatsiya qilinadi. Sertifikatga asoslangan autentifikatsiyaning Afzal tomoni shundaki, sertifikatlar yuqori darajadagi xavfsizlikni ta'minlaydi va sog'liqni saqlash tizimida ma'lumotlar maxfiyligini himoya qilishda ishonchli.Biroq bu usulda sertifikatlarni boshqarish va o‘rnatish qiyin bo‘lishi va turli resurslar talab etilishi mumkin.

Identifikatsiyaga asoslangan autentifikatsiya yondashuvlari. Salman va uning jamoasi (2016) IoT qurilmalari uchun identifikatsiyaga asoslangan autentifikatsiya yondashuvini ishlab chiqdi.U shlyuzlar, autentifikatsiya qurilmalari va manzillar yordamida aniq identifikatorlarni umumiy identifikatsiyaga tarjima qilish uchun autentifikatsiya va identifikatsiya modelidan foydalangan.

Mishra va uning jamoasi esa 2018 – yilda IoT xizmatlarida maxfiylik va xavfsizlikni ta'minlash uchun samarali autentifikatsiya mehanizmini ishlab chiqdi. U bulutli xizmatlarni taklif qildi va sensorli tugun,foydalanuvchiga taqlid qilish hujumlari kabi xavfsizlik hujumlariga qarshi turdi.

Biometrik autentifikatsiya - sog'liqni saqlash sohasida keng qo'llaniladigan xavfsizlik vositalaridan biri. Bu usulda foydalanuvchi yoki tibbiyot xodimining barmoq izi, yuzni tanib olish, ko'z qopqog'i (iris), ovoz yoki hatto yurak urishi kabi biometrik xususiyatlari yordamida autentifikatsiya amalga oshiriladi.

Biometrik autentifikatsiyalash usullari an'anaviy usullarga nisbatan quyidagi afzalliklarga ege:

- Biometrik alomatlarning noyobligi tufayli autentifikatsiyalashning ishonchlilik darajasi yuqori;
- Biometrik alomatlarning sog'lom shaxsdan ajratib bo'lmasligi;
- Biometrik ma'lumotlarni soxtalashtirishning qiyinligi.

Foydalanuvchilarni autentifikatsiyalashda faol ishlatiladigan biometrik alomatlar quyidagilar:

- Barmoq izlari;
- Qo'l panjasining geometrik shakli;
- Yuzning shakli va o'lchamlari;
- Shaxsning ovoz xususiyatlari;
- Ko'z yoyi va to'r pardasining naqshi .

Yuqoridagi biometrik autentifikatsiyalar orasida aniqligi eng yuqori Qo'l panjasining geometrik shakli bo'yicha autentifikatsiyalash tizimlaridir. Bu tizimlarda qo'l panjasi shaklini o'quvchi qurilmalar barmoqlar uzunligini,qo'l panja qalinligi va yuzasini o'lchash orqali qo'l panjasining hajmiy tasvirini yaratadi.Masalan,Recognition Systems kompaniyasining mahsulotlari 90 dan ortiq o'lchamlarni amalga oshiradi.Natijada keying taqqoslash uchun 9 xonali namuna shakllantiriladi. Qo'l panjasini skanerlovchi qurilmalar narxining yuqoriligi va o'lchamlarining kattaligi sababli tarmoq muhitida kamdan kam ishlatilsada, ular qat'iy xavfsizlik rejimiga va shiddatli trafikga ega bo'lgan hisoblash muhiti uchun qulay hisoblanadi.Ularning aniqligi yuqori va inkor koeffitsenti,ya'ni inkor etiladigan qonuniy foydalanuvchilarning foizi juda kichik.

Biometrik autentifikatsiyalashda yuzning tuzilishi va ovoz bo'yicha autentifikatsiyalovchi tizimlar arzonligi tufayli eg foydalanuvchan hisoblanadilar,chunki aksariyat zamonaviy kompyuterlar video va audio vositalariga ega.Yuz tuzilishini skanerlash texnalogiyasi boshqa biometric texnologiyalar yaroqsiz bo'lgan ilovalar uchun to'g'ri keladi.Bu holda shaxsni dentifikatsiyalash uchun ko'z,burun va lab xususiyatlari ishlatiladi.Yuz tuzilishini skanerlash-biometrik autentifikatsiyalash usulari ichida yagona,tekshirishga ruhsatni talab qilmaydigan(yashiringan kamera yordamida amalga oshirilishi mumkin)usul hisoblanadi.

Ta'kidlash joizki yuz tuzilishini aniqlash texnologiyasi hozirgi kunda yanada takomillashtirishni talab etadi.Yuz tuzilishini aniqlovchi aksariyat quyosh yorug'ligi jadalligining kun bo'yicha tebranishi natijasidagi yorug'lik o'zgarishiga o'ta ta'sirchan bo'ladi.Yuz holatining 45 gradus o'zgarishi aniqlashni samarasiz bo'lishiga olib keladi.

Ikki faktorli autentifikatsiya (2FA) - Ikki faktorli autentifikatsiya foydalanuvchining paroliga qo'shimcha himoya qatlamini qo'shadi. Foydalanuvchi parolni kiritgandan keyin, ikkinchi darajali tasdiqlash talab qilinadi, masalan:

- SMS orqali yuborilgan bir martalik kod.

- E-mail orqali yuborilgan havola.
- Maxsus autentifikatsiya ilovasi orqali yaratilgan vaqtga bog'liq kod.

Ikki faktorli autentifikatsiya usuli birlamchi parol buzilgan taqdirda ham qo'shimcha himoya qatlamini ta'minlaydi.

Qat'iy autentifikatsiyalash – asosan kriptografik protokollarda amalga oshiruvchi g'oya hisoblanadi.Tekshiriluvchi taraf qandaydir sirni bilishini namoyon etgan holda tekshiruvchiga o'zining haqiqiy ekanligini isbotlaydi.Masalan,bu sir autentifikatsion almashinish taraflari o'rtasida oldindan xavfsiz usul bilan taqsimlangan bo'lishi mumkin.Sirni bilishlik isboti kriptografik usul va vositalardan foydalanilgan holda so'rov va javob ketma-ketligi yordamida amalga oshiriladi.Aksariyat hollarda qat'iy autentifikatsiyalashga bionan har bir foydalanuvchi o'zining maxfiy kalitiga egaligi alomati bo'yicha autentifikatsiyalanadi. Boshqacha aytganda,foydalanuvchi uning aloqa bo'yicha sherigining tegishli maxfiy kalitga egeligini va u bu kalitni axborot almashinuvi bo'yicha haqiqiy sherik ekanligini isbotlash imkoniyatiga ega.

Token asosida autentifikatsiya - Token asosida autentifikatsiya xavfsiz kirish uchun tibbiyot xodimlariga yoki bemorlarga o'ziga xos tokenlar yaratadi. Bu tokenlar har safar qurilmaga kirishda foydalaniladi va vaqtga bog'liq ravishda yangilanadi. Token asosidagi autentifikatsiya sog'liqni saqlash tizimlarida kirishni osonlashtiradi va xavfsizlikni oshiradi. Bir marta foydalanilgan tokenlar qayta foydalanilmaydi va qisqa muddatli. Biroq bu usulda tokenlarni yo'qotish xavfi bor yoki foydalanuvchilar bu tizimni notanish deb his qilishlari mumkin.

O'zaro autentifikatsiya (Mutual Authentication) - Bu usulda IoT qurilmasi va server o'zaro autentifikatsiya qilinadi. Qurilma serverni va server qurilmani autentifikatsiya qilishi kerak bo'ladi. Bu, ayniqsa, sog'liqni saqlash ma'lumotlarini xavfsiz tarmoqlarda uzatishda muhim. Ushbu usulda har ikkala tomonning ishonchliligi tasdiqlanadi, bu hujumlarga qarshi qo'shimcha himoya ta'minlaydi. Bu texnologiya murakkab va kuchli kriptografik protokollarni talab qiladi.

Saxena, Grijalva and Chaudhari (2016) IoT ni qo'llab quvvatlaydigan tarmoq xiamatlari uchun autentifikatsiya va o'zaro kelishuv protokolini taqdim etdi.Bu IoT qurilmalari va foydalanuvchilari o'rtasida samaraliva xavfsiz aloqa o'rnatish imkonini berdi.Bu takrorlash,qayta yo'naltirish,o'zni o'zi taqlid qilish va obyektlarni o'g'irlash hujumlaridan xavfsizroq edi.Ushbu protokol IoT qurilmalariga maxfiylik va anonimlikni taklif etdi.

Li va uning jamoasi (2017) tarmoq aloqasidagi umumiy kanallar ustidan kafolatni taklif qilish uchun samarali foydalanuvchi autentifikatsiya modelini taklif etdi.U ba'zi xavfsizlik modellariga qarshi turdi va IoT qurilmalariga asosiy xavfsizlik anonimligini ta'minladi.Ushbu yondashuvdagi autentifikatsiya xavfsizlik talablariga to'liq mos keldi va past hisoblash harajatlariga erishdi.Bu yondashuv Tibbiy yordamga asoslangan IoT tizimida aloqa narxi yuqori deb tasdiqlandi.

HMAC (Hash-based Message Authentication Code) - IoT qurilmalari orqali uzatiladigan ma'lumotlarning haqiqiyligini va butligini tasdiqlash uchun ishlatiladi. Bu usul hash-funksiyalar va maxfiy kalitlar yordamida autentifikatsiya qilish imkonini beradi. HMAC tibbiy ma'lumotlar xavfsizligini ta'minlashda oddiy va samarali bo'lgan autentifikatsiya vositasi hisoblanadi.Biroq bu usul murakkab autentifikatsiya mexanizmlariga qaraganda kamroq xavfsizlik darajasiga ega bo'lishi mumkin.

Quyidagi jadval olimlarning turli yillarda autentifikatsiya qurilmalari ustida olib brogan tadqiqotlarining natijasiga asoslangan.

Mualliflar	Uslublar	Afzallik jihati	Ishlash ko'rsatkichlari	Dasturiy vositalar
Aman, Chua & Sik- dar (2017)	O'zaro foydalanish uchun qulay autentifikatsiya protokoli	Samarali yondashuv	Hisoblash,aloqa muammlari, xotira va energiyaga munosabatlar	Xavfsizlik protokollari tekshiruvi
Li, Liu & Nepal (2017)	Umumiy autentifikatsiya protokoli	Samarali yondashuv	Autentifikatiya vaqti va konfedensiallik	Sky mote In Cooja Simulator
Porambage et al. (2014a)	Ikki fazali autentifikatsiya protokoli	Boshqalar	Samaradorlik,xavf-sizlik, xotira istemoli	-
Yao et al. (2013)	Foydalanish uchun qulay autentifikatsiya Mehanizmi	Samarali yondashuv	Hisoblash uchun Qo'shimcha xarajatlar, paketlarni yo'qotish, aloqa xarajatlari, Xabar entropiyasi	-
Kalra & Sood (2015)	Xavfsiz ECC O'zaro autentifikatsiya protokoliga asoslangan	O'zaro autentifikatsiya usuli	Aloqa harajatlari	Automated Validation of Internet Security Protocols and Ap-plications (AVISPA) Tool
Alcaide et al. (2013)	To'liq markazlashmagan Anonim autentifikatsiya Protokoli	Kriptografiyaga asoslangan yondashuv	Hisoblash harajatlari va aloqa narxi	-
Punithavathi et al. (2019)	Lightweight Framework	Oson yondashuv	Aniqlik va xavfsizlik	Python
Alshahrani, Traore & Woungang (2019)	Anonim tekshirish sxemasi	Kriptografiyaga asoslangan yondashuv	Efficiency, com-Munication overhead	AVISPA Tool
Zhou et al. (2019)	Oson autentifikatsiya yondashuvi	Samarali yondashuv	Samaradorlik, xavfsizlik	Proverif Tool

Xulosa qilib aytganda Sog'liqni saqlash IoT qurilmalarida autentifikatsiya juda muhim rol o'ynaydi, chunki bu tizimlar shaxsiy va sezgir tibbiy ma'lumotlarni boshqaradi. Har bir autentifikatsiya usulining afzalliklari va kamchiliklari mavjud bo'lib, sog'liqni saqlash tizimlarida xavfsizlik, foydalanish qulayligi va tizim talablariga qarab tanlanadi. Xavfsizlikni oshirish uchun ko'p faktorli autentifikatsiya va sertifikatga asoslangan autentifikatsiya keng qo'llaniladi. Autentifikatsiya usullari, baholash ko'rsatkichlari va asboblar to'plamining toifalari yordamida oddiy statistik tahlil amalga oshirish mumkin. yengil vaznga asoslangan autentifikatsiya usuli IoT autentifikatsiya qilishning eng keng tarqalgan usulidek ko'rinadi. Keyinchalik, AVISPA ko'rib chiqilayotgan tadqiqot ishlarining eng ko'p ishlatiladigani bu asboblar to'plamidir ya'ni foydalanilgan ko'rsatkichlar orasida autentifikatsiya mexanizmlarining sifatini baholashda eng ko'p ishlatiladigan aloqa narxi, xavfsizlik va hisoblash narxi hisoblanadi. IoT texnologiyasi oldida bir qancha muhim muammolar mavjud bo'lib, ularni kelgusi ishlarda to'g'ri hal qilish kerak. Ushbu muammolar muvaffaqiyatli hal etilgach, IoT ilovalari elektron sog'liqni saqlash, aqlli transport, aqlli shaharlar va uylarni avtomatlashtirish kabi muhim sohalarda yanada rivojlanishi mumkin.

Foydalanilgan adabiyotlar

1. Aman, Chua & Sikdar (2017)
Aman, M., Chua, S., & Sikdar, B. (2017). An Efficient Network Coding Scheme for Wireless Networks. In Proceedings of the 16th International Symposium on Wireless Communication Systems (ISWCS) (pp. 1-6).

2 Li, Liu & Nepal (2017)
Li, W., Liu, L., & Nepal, S. (2017). Big Data Processing in Cloud Computing Systems: A Survey. International Journal of Cloud Computing and Services Science (IJ-CLOSER), 6(3), 123-136.

3 Porambage et al. (2014a)
Porambage, P., et al. (2014). A Survey on Cloud Computing Security Issues and Challenges. Journal of Cloud Computing: Advances, Systems and Applications, 3(1), 1-16.

4 Punithavathi et al. (2019)
Punithavathi, P., et al. (2019). Design and Analysis of Secure Cloud Storage: A Survey. International Journal of Engineering and Technology (IJET), 7(4), 192-198.

5 Alshahrani, Traore & Woungang (2019)
Alshahrani, M., Traore, I., & Woungang, I. (2019). Security and Privacy in Cloud Computing: A Survey. International Journal of Computer Science and Network Security (IJCSNS), 19(12), 18-26.

6 Zhou et al. (2019)
Zhou, Z., et al. (2019). Blockchain-Based Secure Cloud Storage Systems: A Survey. Journal of Cloud Computing: Advances, Systems and Applications, 8(1), 1-15.